Intra2net
Administrator Handbuch



Intra2net Business Server
Intra2net Security Gateway
Intra2net Network Security

www.intra2net.com

Intra2net Administrator Handbuch

Intra2net AG

Veröffentlicht 20. Mai 2025

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 Intra2net Systeme finden Sie im Internet unter https://www.intra2net.com

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

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

Copyright © 1999-2025 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 Intra2net Software Version 7.0.0

Gültig für Intra2net Groupware Client Version 5.0.2

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 3
2.5. RAID 5
2.6. Installation des Betriebssystems 5
2.6.1. Installation von einem USB-Speicherstick 5
2.6.2. Installation von DVD 6
2.6.3. Start der Installation 6
2.6.4. Serielle Konsole 6
2.6.5. Lösen von Kompatibilitätsproblemen 7
3. Installation der Appliance 8
3.1. Lieferumfang 8
3.1.1. Intra2net Appliance Micro 8
3.1.2. Intra2net Appliance Eco 8
3.1.3. Intra2net Appliance Pro 8
3.2. Standort 9
3.3. Reinigung und Pflege 9
3.4. Anschlüsse 10
3.4.1. Übersicht 10
3.4.2. Netzteile 10
3.4.3. Erdung (nur Appliance Eco) 11
3.4.4. Kabelhalter (nur Appliance Eco) 11
3.5. LED-Anzeige 11
3.5.1. Start des Geräts 11
3.5.2. Normaler Betrieb 12
3.5.3. Update läuft 12
3.5.4. Fehler 12
3.6. Software 13
4. Installation als virtuelle Maschine 14
4.1. Vergleich mit echter Hardware 14
4.1.1. Ungleichmäßige Ausführungsgeschwindigkeit 14
4.1.2. Geringere I/O-Performance 14
4.1.3. Kontakt mit ungefilterten Netzwerkpaketen 14
5. Installation auf VMware vSphere Hypervisor 4 (ESXi) 17
5.1. Konfiguration der virtuellen Maschine 17
5.2. Virtuelle Maschine mit direktem Internetzugang 22
5.3. Installation des Intra2net Systems 25
6. Installation auf Microsoft Hyper-V unter Windows Server 2012 R2 27
6.1. Konfiguration der virtuellen Maschine 27
6.2. Installation des Intra2net Systems 34
7. Die Konsole 36
7.1. Intra2net Appliance Micro 36
7.2. Netzwerkkarten 36
7.3. DNS und DHCP 37
7.4. Firewall-Notmodus 37
7.5. In Auslieferungszustand zurücksetzen 38
7.6. Das root-Passwort 38

7.7. Die Linux-Shell 38
8. Die Weboberfläche 40
8.1. Zugriff auf die Weboberfläche 40
8.2. Lizenzcode 40
8.3. Die Hauptseite 40
8.4. Die Warteschlange 41
8.5. Die Konfigurationsprüfung 42
8.6. Herunterfahren notwendig 42
2. Allgemeine Funktionen 43
9. Intranet 44
9.1. IPs und Netze 44
9.2. VLAN-Tagging 44
9.3. Zugriffsrechte eines Netzwerkobjekts 45
9.4. Domain und DNS 45
9.4.1. Das Intra2net System als lokaler DNS-Server 45
9.4.2. Anderen DNS-Server im LAN anbinden 46
9.4.3. DNS für andere Domains weiterleiten 47
9.4.4. DNS-Rebind verhindern 47
9.5. Clients eintragen 49
9.5.1. Wake-On-LAN 50
9.5.2. DHCP 50
9.6. DHCP-Server 50
9.7. Bereiche eintragen 51
9.8. Import/Export von Rechnerprofilen 51
9.8.1. Import von Rechnern 51
9.8.2. Export von Rechnern 51
9.9. Routing im Intranet 51
10. SSL-Verschlüsselung und Zertifikate 53
10.1. Prinzip und Gefahren der SSL-Verschlüsselung 53
10.2. Zertifikate richtig erstellen 53
10.2.1. Der Rechnername 53
10.2.2. Konfiguration 54
10.3. Zertifikate auf Clients installieren 54
10.3.1. Installation unter Windows 54
10.3.2. Verteilen von Zertifikaten über Active Directory 58
10.4. Benutzer sensibilisieren 59
10.5. Verwenden einer externen Zertifizierungsstelle 59
10.5.1. Zertifikate von Let's Encrypt 59
10.5.2. Zertifikate von klassischen Zertifizierungsstellen 60
10.6. Schlüsselimport 61
10.7. Verschlüsselungsstärke 61
11. Internet 63
11.1. Einwahl mit DSL (PPPoE) 63
11.2. Einwahl mit DSL (PPTP) 63
11.3. Router mit fester IP 63
11.4. Router mit DHCP oder Kabelmodem 64
11.5. Router im lokalen Netz 64
11.6. Router vs. Modem 65
11.7. Offizielle IPs und DMZ 66
11.7.1. Klassisches Routing 66
11.7.2. Statische NAT 67
11.7.3. Proxy-ARP 68
11.8. Verbindungsautomatik 69

11.9. Verbindungsüberwachung 70
11.10. Ausweichen auf andere Provider im Fehlerfall (Fallback) 70
11.11. Bandbreitenmanagement und VoIP-Priorisierung 70
11.11.1. Bandbreitenmanagement 70
11.11.2. VoIP- und Echtzeitdaten priorisieren 72
11.12. Masquerading / NAT 73
11.13. DynDNS 73
11.13.1. Anbieter 73
11.13.2. Aktualisierung und verwendete IP 74
11.14. Zugriff von außen 74
12. Proxy 75
12.1. Überblick 75
12.2. Zugang zum Proxy 75
12.3. Proxykonfiguration 76
12.4. URL-Filter 76
12.4.1. Proxy-Profile 76
12.4.2. Proxy-Zugriffslisten 76
12.4.3. Zeitsteuerung 77
12.5. Web-Content Filter 77
12.6. Proxy-Virenscanner 78
13. Statistik und Datenschutz 79
13.1. Proxy-Statistik 79
13.1.1. Proxy-Protokollierung 79
13.1.2. Auswertung 79
13.1.3. Methodik 79
13.2. Internet-Zugriffsstatistik 80
13.2.1. Methodik 80
13.3. Tachometer 81
13.3.1. Methodik 81
13.3.2. Seiten 82
13.3.3. Datenschutz 83
13.4. Speicherverbrauchsstatistik 84
13.5. Datenschutz 84
14. Benutzermanager 85
14.1. Benutzergruppen 85
14.1.1. Zugriffsrechte 85
14.1.2. Administrationsrechte 86
14.2. Benutzer 86
14.2.1. Einstellungen für E-Mail und Groupware 86
14.3. Import/Export von Benutzerprofilen 87
14.3.1. Import von Benutzern 87
14.3.2. Export von Benutzern 87
15. E-Mail 88
15.1. E-Mail-Versand 88
15.1.1. Rechte 88
15.1.2. SMTP-Submission 88
15.1.3. Versandmethoden 88
15.1.4. Versand über Relayserver 88
15.1.5. Direkter Versand 89
15.1.6. Auswahl der Versandmethode 89
15.2. E-Mail-Empfang auf dem Client (POP oder IMAP) 90
15.3. E-Mail-Empfang auf dem Intra2net System 91
15.3.1. Konzepte 91

15.3.2. Abruf einzelner POP-Konten 93
15.3.3. Direkte Zustellung per SMTP 93
15.3.4. Abruf von POP-Sammelkonten (Multidrop) 93
15.4. Weiterleitung von gesamten Domains 95
15.4.1. Konzept 95
15.4.2. Empfängeradressprüfung 95
15.4.3. Weiterleitung einzelner POP-Konten 98
15.5. E-Mail-Adressierung 99
15.5.1. Adresseinstellungen 99
15.5.2. E-Mail-Adressen und Aliases 99
15.6. E-Mail-Verarbeitung 99
15.6.1. Weiterleitung 99
15.6.2. Automatische Antwort 100
15.6.3. Sortierung 100
15.6.4. Automatisch Löschen 101
15.7. E-Mail-Filter 101
15.7.1. Spamfilter 101
15.7.2. Virenscanner 106
15.7.3. Anhangfilter 106
15.8. DKIM 108
15.8.1. Grundlagen 108
15.8.2. Umsetzung 109
15.8.3. Weitere Standards 109
15.8.4. Voraussetzungen zur Nutzung 109
15.8.5. Konfiguration 110
15.8.6. Filterung und Quarantäne 113
15.8.7. Headerlisten und Ausnahmen 114
15.8.8. Schlüssel rotieren 115
15.9. Archivierung 116
15.9.1. Schnittstelle 116
15.9.2. Anbindung des MailStore Servers 117
15.10. Automatischer Transfer 124
15.11. Verteiler 124
15.12. Weitere Einstellungen 125
15.13. Warteschlange 125
15.14. Aufbau des Mailsystems 126
15.15. Unterschiede zwischen den Lizenzen 126
16. Dienste 128
16.1. Zeitserver 128
16.2. Überwachung per SNMP 128
17. Systemfunktionen 130
17.1. Lizenz 130
17.1.1. Demomodus 130
17.1.2. Lizenzcode 130
17.1.3. Updatezeitraum 130
17.2. Updates 131
17.2.1. Update-Fernsteuerung via Partnerweb 131
17.2.2. Rettungssystem 132
17.3. Backup 132
17.3.1. Schutz der Backups 133
17.3.2. Aufbewahrungsdauer 133
17.3.3. Auslagern 134
17.3.4. Rücksichern 134

17.3.5. Vorgehen bei Festplattenschaden oder Hardwaretausch 134
17.3.6. Hardwareumzug mit Unterstützung von Intra2net 136
17.3.7. Standby-Systeme 136
17.4. Betrieb hinter einer Firewall 138
17.5. Logdateien 140
17.6. Logcheck Reports 140
17.7. Zeitgesteuertes Herunterfahren 140
17.8. Prüfung und Reparatur der Dateisysteme 140
3. Groupware Client 142
18. Einführung 143
18.1. Systemvoraussetzungen 143
18.2. Übersicht der Funktionen 144
18.3. Bekannte Einschränkungen 144
19. Installation 147
19.1. Installation des Programms 147
19.2. Verteilung des Programms über Active Directory 148
19.3. Umstieg von 32 Bit auf 64 Bit 149
20. Profil einrichten 150
21. Konten konfigurieren 153
21.1. Groupware-Konto 153
21.1.1. Zertifikatsüberprüfung aktivieren 153
21.1.2. Deaktivieren des Searchindexers 154
21.2. Bestehende Daten übernehmen 156
21.2.1. Übernehmen per Outlook-Import 156
21.2.2. Übernehmen größerer Mengen an E-Mails 159
21.3. Einrichten mehrerer Konten und E-Mail-Adressen 160
21.3.1. Mehrere Serverkonten 161
21.3.2. Mehrere Absenderadressen 163
21.4. Umwandeln bisheriger Installationen des Groupware Clients 166
22. Ordner verbinden 170
22.1. Eigene Ordner verbinden 170
22.1.1. Automatisch verbinden 170
22.1.2. Ordner von der Synchronisation ausschließen 171
22.1.3. Ordnerliste aktualisieren 172
22.2. Gemeinsame Ordner verbinden 173
23. Ordner freigeben 175
23.1. Rechte 176
23.2. Gelesen-Status gemeinsam/individuell 176
24. Expertenmodus für Ordnerverbindungen 178
24.1. Gemeinsame Ordner verbinden 178
24.2. Ordner manuell verbinden 181
24.2.1. Umstellen auf Manuelles Verbinden 181
24.2.2. Einen einzelnen Ordner verbinden 182
24.2.3. Verbindung eines Ordners aufheben 184
25. Erweiterte Funktionen 185
25.1. Ordnerhierarchie und ibx_sub 185
25.2. Ordneroptionen 185
25.3. Serverseitige Einstellungen bearbeiten 186
25.4. Kategorien und Farbzuordnung 187
25.4.1. Vorschlag gemeinsame Farbzuordnung 188
25.4.2. Lokale Farbzuordnung zurücksetzen 188
25.4.3. Ändern einer vorhandenen Farbzuordnung 189
25.5. Frei-/Gebucht-Informationen verwenden 191

25.5.1. Outlook 2010 bis 2021 ... 191
25.5.2. Outlook 2007 ... 192
25.6. Kennzeichnung als Privat ... 193
25.7. Erinnerungen in gemeinsam genutzten Ordnern ... 194
25.8. Benutzerdefinierte Felder in Kontakten ... 195
25.9. Anzeige des Quelltexts von Objekten ... 195
25.10. Sicherungsordner ... 195
25.10.1. Gesicherte Daten nach Wiederherstellung ... 196
25.10.2. Sicherung lokaler Daten beim Zurückstellen auf Automatik ... 196
25.11. Hinweise an den Benutzer ... 197
25.12. Logdateien ... 198
25.12.1. Übermitteln von Logdateien an den Support ... 198
26. Erweiterte E-Mail-Konfiguration ... 199
26.1. E-Mails komplett oder nur Kopfzeilen abrufen ... 199
26.2. Benachrichtigung über neue E-Mails ... 199
26.3. Gelesen-Markierung bei verschobenen E-Mails ... 200
26.4. Erinnerungen und Nachverfolgen von E-Mails ... 201
26.5. Lesebestätigungen ... 203
27. Kompatibilität und Zusammenarbeit ... 204
27.1. Personal-Firewalls auf dem Client ... 204
27.2. Virenscanner auf dem Client ... 204
27.3. Kompatibilität mit PDAs und Mobiltelefonen ... 205
27.4. Sonstige Programme ... 205
27.4.1. Inkompatible Add-Ins ... 205
27.5. Automatische Erkennung von Kompatibilitätsproblemen ... 206
28. Konzept für öffentliche Ordner ... 207
28.1. Einrichtung ... 207
28.2. E-Mails ... 208
29. Migration von E-Mails mit IMAPCopy ... 209
30. Migration von Microsoft Exchange ... 211
30.1. Offline-Migration ... 211
30.1.1. Die Migration in einzelnen Schritten ... 211
30.2. Migration im laufenden Betrieb ... 212
30.2.1. Vorbereitung der Migration ... 213
30.2.2. Die Migration der einzelnen Benutzer ... 214
30.2.3. Öffentliche Ordner ... 215
30.2.4. Abschließende Schritte ... 215
31. Referenzinformationen ... 216
31.1. Synchronisierbare Daten ... 216
31.1.1. Aufgaben ... 216
31.1.2. Termine ... 217
31.1.3. Notizen ... 218
31.1.4. Kontakte ... 218
31.1.5. Kontaktgruppen ... 221
31.1.6. E-Mails ... 221
31.1.7. Alle Objekte ... 222
31.2. Erweiterte Einstellungen in der Registrierung ... 222
31.2.1. Einstellungen für den Store ... 223
31.2.2. Einstellungen für das Add-In ... 231
31.3. Datenformate ... 233
4. Web-Groupware und ActiveSync ... 234
32. Einführung in die Web-Groupware ... 235

32.1. Die Anzeigemodi 235
33. E-Mail 236
33.1. E-Mails lesen und bearbeiten 236
33.1.1. E-Mails anzeigen 236
33.1.2. Gelöschte E-Mails 236
33.1.3. E-Mails exportieren 237
33.2. E-Mails senden 238
33.2.1. Neue Nachricht 238
33.2.2. Signaturen anhängen 239
33.3. Ordner verwalten 239
33.3.1. Ordnerhierarchie 239
33.3.2. Ordner organisieren 240
33.3.3. Ordner abonnieren 240
33.3.4. Ordner freigeben 241
34. Adressbuch 243
35. Mobile Geräte per ActiveSync anbinden 244
35.1. Einführung 244
35.2. Einstellungen auf dem Server 244
35.3. Besonderheiten und Tipps 245
35.3.1. Löschen von E-Mails auf dem Server 245
35.3.2. Synchronisationsschritte 245
35.3.3. Geräte verwalten und neu synchronisieren 246
35.3.4. Synchronisieren von mehreren Kalendern oder Kontakteordnern 246
36. ActiveSync mit Android-Geräten 247
37. ActiveSync mit Apple iOS-Geräten 252
38. Referenzinformationen 257
5. Firewall 258
39. Auswahl der Firewall-Regellisten 259
39.1. Regellisten im LAN 259
39.2. Regellisten fürs Internet 259
39.3. Weg der Pakete durch die Firewall 260
39.3.1. Paketwege im LAN und Internet 260
39.3.2. Paketwege bei VPN-Verbindungen 260
40. Firewall-Profile 262
40.1. Basis-LAN Grundregeln 262
40.2. Rechnerprofile 262
40.3. Providerprofile 263
41. Vollständige Regellisten 264
41.1. Komponenten 264
41.1.1. Dienste 264
41.1.2. Netzgruppen 264
41.1.3. Netzgruppen mit DNS-Rechnernamen 265
41.1.4. Automatische Objekte 265
41.2. Regellisten 265
41.2.1. Grundeinstellungen 265
41.2.2. Durchlaufen der Regelliste 266
41.2.3. Verknüpfung der Regel-Kriterien 266
41.2.4. Die Aktionen 267
41.2.5. Extra-Optionen 268
41.2.6. Besonderheiten bei Provider-Regellisten 269
42. Weitere Funktionen 270
42.1. MAC-Adressen überprüfen 270

42.2. Spoofing im LAN verhindern 270
42.3. Blockieren von IPs nach zu vielen Loginfehlern 270
42.4. Firewall-Notmodus 270
43. Fallbeispiele und Aufgaben 271
43.1. Aufgabe 1: Erweitern eines einfachen Rechnerprofils 271
43.1.1. Musterlösung 271
43.2. Aufgabe 2: Portforwarding nur von einer externen IP erreichbar 272
43.3. Aufgabe 3: Separiertes Gästenetz 272
43.3.1. Musterlösung 273
43.4. Aufgabe 4: Beschränkter Zugang aus dem VPN 274
43.5. Aufgabe 5: Webserver in der DMZ 274
43.5.1. Musterlösung 275
6. IPSec VPN 276
44. IPSec Grundlagen 277
44.1. IPSec 277
44.2. Public-Key Kryptographie 277
44.3. Zertifikate 277
44.4. IPSec Verbindungen 278
44.5. Algorithmen 278
44.6. Einschränkungen 279
44.7. Kompatibilität mit anderen IPSec-Gegenstellen 279
45. Schlüsselmanagement 280
45.1. Eigene Schlüssel 280
45.1.1. Zertifizierungsstellen (CAs) 280
45.2. Fremde Schlüssel 281
46. Anbinden von einzelnen PCs 282
46.1. Konzept 282
46.2. Vorbereiten der Konfiguration auf dem Intra2net System 282
46.2.1. Zertifikat erstellen 282
46.2.2. Standardeinstellungen für neue Verbindungen 285
46.3. Automatische Konfiguration für Clients auf dem Intra2net System 285
46.4. Manuelle Konfiguration auf dem Intra2net System 287
46.4.1. Voraussetzungen 287
46.4.2. Grundeinstellungen 287
46.4.3. Authentifizierung 288
46.4.4. Tunnel konfigurieren 289
46.4.5. Rechte 290
46.4.6. Aktivierung 290
47. VPN mit dem NCP Secure Entry Windows Client 291
47.1. Import 291
47.2. Verbindung aufbauen 293
47.3. Verbindungsprotokolle 293
48. VPN mit dem Shrew Soft VPN Client 295
48.1. Import 295
48.2. Verbindung aufbauen 295
48.3. Verbindungsprotokolle 296
49. VPN mit Mac OS X 298
49.1. Installation 298
49.2. Zertifikate erzeugen 298
49.3. Zertifikate importieren 299
49.4. Verbindungen konfigurieren 301

49.5. Intra2net System 304
50. VPN mit dem NCP Secure Entry macOS Client 305
51. VPN mit Apple iOS-Geräten 308
52. VPN mit Android 310
52.1. Gerät vorbereiten 310
52.2. Verbindung auf dem Intra2net System 311
52.3. Zertifikate 311
52.4. Verbindung auf Android 313
52.5. Verbindungsaufbau vereinfachen 315
53. VPN mit dem NCP Secure Android Client Premium 318
54. Anbinden von kompletten Netzen 322
54.1. Konzept 322
54.2. Konfiguration auf dem Intra2net System 323
54.2.1. Voraussetzungen 323
54.2.2. Grundeinstellungen 323
54.2.3. Authentifizierung 323
54.2.4. Tunnel konfigurieren 324
54.2.5. Rechte 324
54.2.6. Aktivierung 324
55. VPN mit ZyXEL ZyWALL USG 325
55.1. Überblick 325
55.2. Vorbereitung 325
55.3. Zertifikate 326
55.4. Verbindung 329
55.4.1. IKE / Phase 1 329
55.4.2. IPSec / Phase 2 330
55.5. Intra2net System 334
55.6. Logs 334
56. VPN mit Lancom Routern 335
56.1. Überblick 335
56.2. Zertifikat für das Lancom-Gerät 335
56.3. Zertifikat für das Intra2net System 337
56.4. Verbindung 338
56.5. Intra2net System 344
56.6. Zertifikate löschen 344
57. VPN mit Linux 345
57.1. Überblick 345
57.2. Zertifikate erzeugen 345
57.3. Verbindungen konfigurieren 346
57.4. Intra2net System 348
58. Lösen von IP-Adresskonflikten in VPNs durch NAT 349
58.1. Das Problem 349
58.2. Konfiguration 349
58.3. Gleiche IPs in LAN und auf der Gegenseite 350
58.3.1. Umsetzung 351
58.4. Mehrere Gegenstellen mit gleichen IPs 351
58.4.1. Umsetzung 352
58.5. Lokale IPs festgelegt durch Fernwartungs-Dienstleister 352
58.5.1. Umsetzung 353
59. Fehlerdiagnose 354
59.1. Logs lesen 354
59.2. Das Protokollformat des Intra2net Systems 354
59.3. Fehler in Phase 1 354

59.4. Fehler in Phase 2 356
7. WireGuard VPN 357
60. WireGuard Grundlagen 358
60.1. Das WireGuard Protokoll 358
60.2. Anpassungen durch Intra2net 359
60.3. Vergleich mit IPSec 360
61. Vorbereiten der Konfiguration auf dem Intra2net System 363
61.1. Eigener Schlüssel und Schnittstelle 363
61.2. Externe Adresse und Firewall 363
61.3. Standardeinstellungen für neue Verbindungen 364
62. Anbinden von einzelnen PCs 365
62.1. Konzept 365
62.2. Automatische Konfiguration für Clients auf dem Intra2net System 365
63. WireGuard Clients 367
63.1. Installation 367
63.2. Konfiguration 367
63.3. Bedienung des Clients 367
63.3.1. Logdateien 368
63.3.2. DNS-Namensauflösung 368
63.4. Besonderheiten des Clients für Windows 369
63.4.1. Schutz der privaten Schlüssel 369
63.4.2. Nutzung ohne Administratorrechte 369
63.4.3. Routing für das Netz Alles (0.0.0.0/0.0.0.0) 370
64. Verbindung mit anderen Intra2net Systemen 371
65. Verbindung mit anderen Routern und Firewalls 372
65.1. Gegenseite ohne eigenen Schlüssel 372
65.2. Gegenseite mit vorhandenem eigenen Schlüssel 373
66. Verbindung mit AVM FRITZ!Boxen 375
66.1. AVM FRITZ!Box ohne bisherige Verbindung 375
66.2. AVM FRITZ!Box mit anderer VPN-Verbindung 377
67. Zustands- und Fehlerdiagnose 381
67.1. Hauptseite 381
67.2. VPN-Status 381
67.3. Logs 382
8. Anhang 383
A. Lizenzen 384
A.1. Intra2net Software Lizenzvertrag 384
A.2. Lizenzierte Software 390
A.3. Hinweise zur Rücknahme und Entsorgung 391
A.3.1. Getrennte Erfassung von Altgeräten 391
A.3.2. Batterien und Akkus sowie Lampen 391
A.3.3. Möglichkeiten der Rückgabe von Altgeräten 391
A.3.4. Datenschutzhinweis 391
A.3.5. Bedeutung des Symbols der durchgestrichenen Mülltonne 391
A.3.6. Unentgeltliche Rücknahme von Altbatterien 392
A.3.7. Bedeutung der Batteriesymbole 392
B. Lizenz 393
B.1. Intra2net Groupware Client Lizenzvertrag (EULA) 393
B.2. Lizenzierte Software 397
B.2.1. Info-ZIP 397
B.2.2. JsonCpp 398

Index 400

Teil 1. Installation

1. Kapitel - Willkommen

Willkommen zu der anwenderfreundlichen Lösung von Intra2net, um Ihr Netzwerk mit geringem Aufwand und maximaler Sicherheit an das Internet anzubinden. Die Intra2net Software regelt die Zugriffsrechte Ihrer einzelnen Arbeitsplätze, verschickt und verwaltet die E-Mail des Teams (abhängig von der gewählten Lizenz) und ermöglicht es, den Internetzugang jederzeit frei zu wählen, ohne fest an einen Zugangsprovider gebunden zu sein.

1.1. Über dieses Handbuch

Dieses Handbuch beschreibt die komplette Administration des Intra2net Systems 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	intra
Domain	net.lan
DHCP	aktiviert
DHCP IP-Pool	192.168.1.200 bis 192.168.1.250
HTTP-Proxy (nur wenn in der Lizenz enthalten)	Port 3128
Oberfläche nur über SSL erreichbar	aktiviert
Administrator Login	admin
Administrator Passwort	admin
Backup erstellen	täglich differenzielles Backup um 06:30, 12:30 und 19:00 Uhr, Vollbackup Samstag 22:00 Uhr
Backup-Zugriffsschutz	aktiv, setzen Sie das Passwort unter System > Backup > Einstellungen
E-Mail-Virenscanner (nur wenn in der Lizenz enthalten)	aktiv
E-Mail-Anhangfilter (nur wenn in der Lizenz enthalten)	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 der Intra2net Software an die Hardware sind wie folgt:

- x86 Prozessor mit 64 Bit und mindestens 2 GHz Taktfrequenz
- Mindestens 2 GB Arbeitsspeicher
- Festplatte mit mindestens 40 GB Speicherkapazität
- Zwei Netzwerkkarten
- Einen USB-Speicherstick oder CD-ROM Laufwerk (nur während der Installation benötigt)

Genauere Details zur unterstützten Hardware finden Sie im Internet unter https://www.intra2net.com/de/support/hardware-compatibility.php.



Wir empfehlen, nur Komponenten bzw. Komplettgeräte zu verwenden, die dort als "zertifiziert" gelistet sind. Intra2net garantiert für diese sowohl mit der aktuellen, als auch mit zukünftigen Versionen der Software, eine optimale Kompatibilität.

2.2. Installation als virtuelle Maschine

Das Intra2net System 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 https://www.intra2net.com/de/support/virtualization-platforms.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 die Hardware in einen Bereich mit kontrollierbarem Zugang (z.B. abschließbarer Raum), da es bei physischem Zugriff mit ausreichenden Systemkenntnissen und etwas Zeit möglich ist, das System zu kompromittieren.

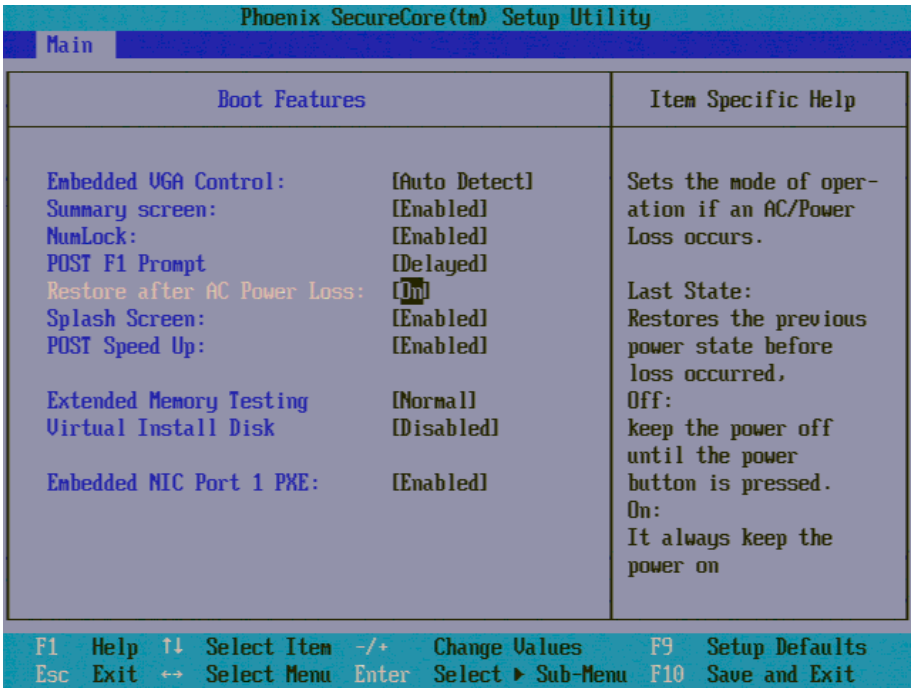
Beachten Sie unbedingt die Vorgaben des Hardwareherstellers bezüglich maximaler Umgebungstemperatur und Luftzufuhr. Die meisten Geräte dürfen nicht bei einer Umgebungstemperatur von mehr als 30 °C oder 35 °C betrieben werden.

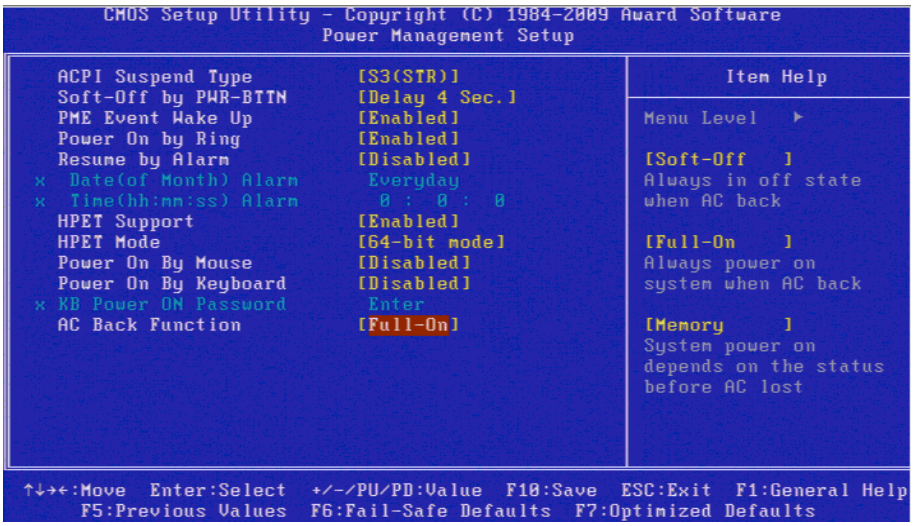
2.4. BIOS

Im BIOS-Setup sollten vor der Installation der Intra2net Software 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 die Intra2net Software auf einem zertifizierten Server von HPE, so finden Sie Hinweise auf die nötigen BIOS-Einstellungen auf dieser Webseite: https://www.intra2net.com/de/support/server-systems.php.

Datum und Uhrzeit	Sollte in etwa stimmen (ca. +-10 Min.), da das Intra2net System bei der Installation ein zeitabhängiges Zertifikat anlegt. Sobald eine Internetverbindung besteht, wird die Zeit über NTP genau gestellt.
"Restore on AC Power Loss" oder "AC Back Function"	Auf "On" oder "Full-On". Damit startet das Intra2net System 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.
"CSM", "Legacy BIOS" oder "UEFI"	Das Intra2net System kann sowohl mit klassischem BIOS, als auch mit UEFI betrieben werden. Ein Wechsel ist auch nach der Installation noch möglich.
"UEFI Secure Boot"	Deaktivieren
"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 Intra2net Systems 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 (evtl. 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 das Intra2net System 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 das Intra2net System die einzelnen Platten separat ansprechen kann. Diese Konfiguration wird häufig auch JBOD genannt. Nach der Installation des Intra2net Systems auf die erste Festplatte können Sie in der Weboberfläche über das Menü System > Hardware > RAID einen RAID-Verbund mit der zweiten Platte anlegen.

2.6. Installation des Betriebssystems

Die Intra2net Software bringt ein vollständiges Betriebssystem auf Linux-Basis mit. Diese 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.

2.6.1. Installation von einem USB-Speicherstick

Um einen bootfähigen USB-Speicherstick zu erstellen, benötigen Sie einen USB-Stick mit mindestens 8 GB Kapazität. Die ZIP-Datei, mit der das Intra2net System ausgeliefert wird, enthält das Programm rufus.exe zum Erstellen von bootfähigen USB-Sticks unter Windows.

Auf einem PC mit Windows entpacken Sie das ZIP-Archiv und starten rufus.exe. Verwenden Sie Rufus aus dem ZIP-Archiv und keine andere Version, da es einige notwenige Anpassungen enthält. Wählen Sie die ISO-Datei aus und den USB-Stick. Alle anderen Voreinstellungen sind bereits korrekt. Beim Schreibvorgang werden alle Daten auf dem Stick gelöscht.

Unter Linux können Sie das Programm Fedora Media Writer zum Erstellen eines bootfähigen USB-Sticks verwenden. Dies ist entweder im Paketmanager Ihrer Distribution erhältlich oder kann als Flatpak von Flathub [https://flathub.org] bezogen werden. Wählen Sie "Custom Image" und dann die ISO-Datei aus. Beim Schreibvorgang werden alle Daten auf dem Stick gelöscht.

Starten Sie den Rechner, auf dem Sie das Intra2net System installieren möchten, von dem vorbereiteten USB-Stick.

2.6.2. Installation von DVD

Brennen Sie die ISO-Datei auf eine DVD und booten den Rechner von dieser. Sie können sowohl ein fest eingebautes DVD-Laufwerk, als auch ein per USB angeschlossenes dafür verwenden.

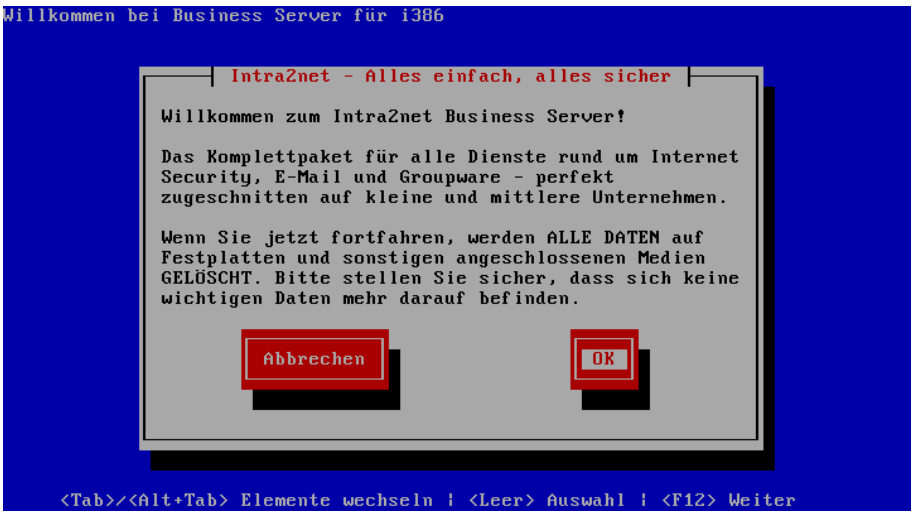
2.6.3. Start der Installation

Nach dem erfolgreichen Start des Installationsprogramms werden Sie aufgefordert, die Installation des Intra2net Systems 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. Entfernen Sie DVD oder USB-Stick, um von der Festplatte zu starten. Der Rechner startet in die Installationskonsole, beschrieben im 7. Kapitel, „Die Konsole“.

2.6.4. Serielle Konsole

Verfügt die Hardware über keinen normalen Monitoranschluss, sondern nur über eine serielle Konsole, so verwenden Sie ein Null-Modem-Kabel oder -Adapter und verbinden sich mit den Parametern 115200 Baud, 8 Bit, No Parity, 1 Stoppbit. Die serielle Konsole muss über die erste serielle Schnittstelle des Systems (COM1 oder ttyS0) angesprochen werden. Evtl. muss dies im BIOS angepasst werden.

Starten Sie das System vom Installationsmedium. Bei klassischem BIOS geben Sie im Bootmanager den Text **`serial`** ein und drücken Enter. Bei UEFI wählen Sie die mit "serial console" gekennzeichnete Option im Bootmenü.

2.6.5. Lösen von Kompatibilitätsproblemen

Sollte das Installationsprogramm eine Fehlermeldung anzeigen, dass nicht genügend Speicherplatz auf der Festplatte zur Verfügung steht, so ist entweder eine kleinere Festplatte als die minimal mögliche installiert (siehe Abschnitt 2.1, „Hardwareauswahl"), die eigentliche Festplatte wurde mit einem USB-Laufwerk, Speicherkarte oder einer vom BIOS bereitgestellten virtuellen Festplatte mit Treibern verwechselt oder die Festplatte wurde gar nicht erst gefunden.

Entfernen Sie daher alle nicht benötigen USB-Laufwerke und Speicherkarten, diese können bei manchen Systemen auch im Inneren des Gehäuses verbaut sein. Überprüfen Sie die BIOS-Konfiguration und deaktivieren virtuelle Treiberlaufwerke, siehe Abschnitt 2.4, „BIOS". Prüfen Sie die Konfiguration des RAID-Controllers bzw. BIOS-RAIDs, siehe Abschnitt 2.5, „RAID".

Eine Ursache kann auch sein, dass die Festplatte vorher in einem RAID-Verbund genutzt wurde und jetzt noch Steuerinformationen für den vorherigen RAID-Verbund oder unpassende Partitionierungsdaten enthält. Führen Sie in diesem Fall eine Formatierung der Festplatte durch oder verwenden eine bisher unbenutzte Festplatte.

Sollte das Installationsprogramm gar nicht erst starten oder während der Installation abbrechen, haben Sie es vermutlich mit einem Kompatibilitätsproblem zwischen Hardware und Intra2net Software zu tun.

Versuchen Sie als erstes, ein BIOS-Update vom Hersteller des Rechners oder Mainboards zu bekommen und zu installieren. Prüfen Sie auch unter https://www.intra2net.com, ob Sie die neueste Version der Intra2net Installations-DVD verwenden.

3. Kapitel - Installation der Appliance

3.1. Lieferumfang

3.1.1. Intra2net Appliance Micro

Folgendes ist enthalten:

- Intra2net Appliance Micro im Tischgehäuse
- Externes Netzteil für 100-240 VAC, 50/60Hz, Ausgang 12V
- Ein Stromkabel mit Kaltgerätestecker
- Nullmodemkabel mit USB-Wandler für Zugriff auf die serielle Konsole
- Ein Netzwerkkabel
- Das Installationshandbuch "Erste Schritte"

Zum Betrieb des Geräts ist unbedingt ein Lizenzcode für Intra2net Network Security oder Intra2net Security Gateway erforderlich. Dieser muss separat erworben werden. Den Lizenzcode finden Sie auf dem Lizenzzertifikat, welches Sie beim Kauf einer Intra2net Lizenz erhalten.

Die Appliance Micro ist nicht mit dem Intra2net Business Server nutzbar.

3.1.2. Intra2net Appliance Eco

Folgendes ist enthalten:

- Intra2net Appliance Eco im Rack-fähigen Gehäuse mit 1,5 Höheneinheiten
- Externes Netzteil für 100-240 VAC, 50/60Hz, Ausgang 19V
- Ein Stromkabel mit Eurostecker
- 4 Gummifüße für den Betrieb außerhalb eines Racks
- Ein Netzwerkkabel
- Ein Rackmountkit bestehend aus 2 Bügeln
- Das Installationshandbuch "Erste Schritte"

Zum Betrieb des Geräts ist unbedingt ein Lizenzcode eines der Intra2net Produkte erforderlich. Dieser muss separat erworben werden. Den Lizenzcode finden Sie auf dem Lizenzzertifikat, welches Sie beim Kauf einer Intra2net Lizenz erhalten.

3.1.3. Intra2net Appliance Pro

Folgendes ist enthalten:

- Intra2net Appliance Pro im Rack-fähigen Gehäuse mit 2 Höheneinheiten
- Ein Rackmountkit bestehend aus 2 Bügeln

- 4 Gummifüße für den Betrieb außerhalb eines Racks
- Ein Stromkabel mit Kaltgerätestecker
- Ein Netzwerkkabel
- Das Installationshandbuch "Erste Schritte"

Zum Betrieb des Geräts ist unbedingt ein Lizenzcode eines der Intra2net Produkte erforderlich. Dieser muss separat erworben werden. Den Lizenzcode finden Sie auf dem Lizenzzertifikat, welches Sie beim Kauf einer Intra2net Lizenz erhalten.

3.2. Standort

Stellen Sie die Intra2net Appliance in einen Bereich mit kontrollierbarem Zugang (z.B. abschließbarer Raum), da es bei physischem Zugriff mit ausreichenden Systemkenntnissen und etwas Zeit möglich ist, die Intra2net Appliance zu kompromittieren.

Stellen Sie Ihre Intra2net Appliance auf eine feste, ebene Fläche oder montieren sie 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.

Die Appliance Micro wird mit Gummifüßen geliefert und muss immer mit diesen betrieben werden um einen ausreichenden Abstand zum Untergrund zu gewährleisten. Dieser ist notwendig, da die Kühlung über den Gehäuseboden erfolgt. Sollten die Gummifüße beschädigt werden oder verloren gehen, können passende Ersatzteile im Handel unter der Bezeichnung "3M SJ5312" bezogen werden.



Achtung

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

3.3. Reinigung und Pflege

Die Geräte saugen zur Kühlung Luft an. In der Luft ist auch Staub enthalten, der mit angesaugt wird und sich dann vor den Staubschutzgittern außen am Gerät ansammelt.



Achtung

Dieser Staub muss regelmäßig entfernt werden, damit die Geräte nicht überhitzen oder beschleunigt altern.

Wir empfehlen für normale Büroräume die Geräte ein mal pro Jahr zu reinigen. Abhängig von der Menge des angesammelten Staubs kann danach das Reinigungsintervall verlängert oder verkürzt werden.

Zur Reinigung fahren Sie das Gerät über die Oberfläche herunter und warten bis es sich von selbst abgeschaltet hat. Trennen Sie es dann von der Stromversorgung. Saugen Sie danach mit einem handelsüblichen Staubsauger alle Lüftungsöffnungen ab, bis von außen kein Staub mehr zu erkennen ist.

Bei den Intra2net Appliances Micro und Eco befinden sich die Lüftungsöffnungen an der rechten und linken Seite. Bei der Intra2net Appliance Pro an der rechten, linken und hin-

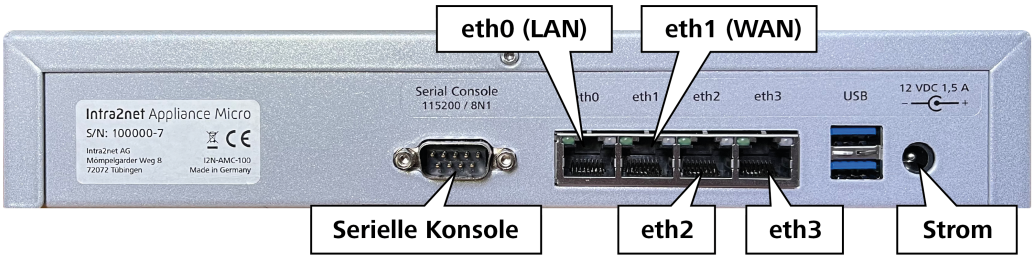
teren Seite. Ist das Gerät in ein Rack eingebaut, müssen Sie zum Zugriff auf die rechte und linke Seite entweder das Gerät ausbauen oder die Seiten des Racks öffnen.

Die Staubschutzgitter im Gerät sind für den zuverlässigen Betrieb notwendig und dürfen nicht entfernt werden. Dringt Staub ungehindert in das Gerät ein und sammelt sich dort an, besteht die Gefahr von Fehlfunktion, Überhitzen, Kurzschluß und Brand.

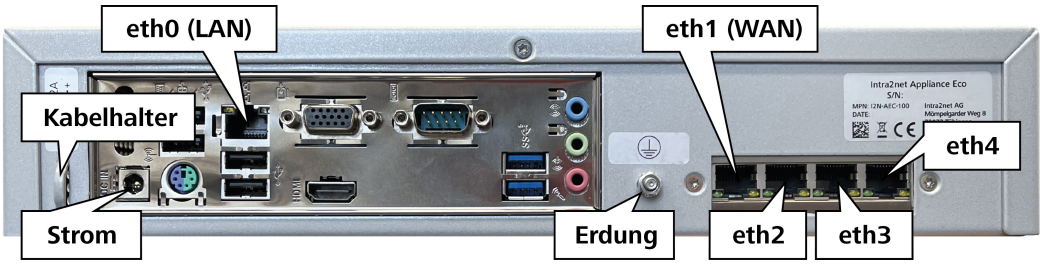
3.4. Anschlüsse

3.4.1. Übersicht

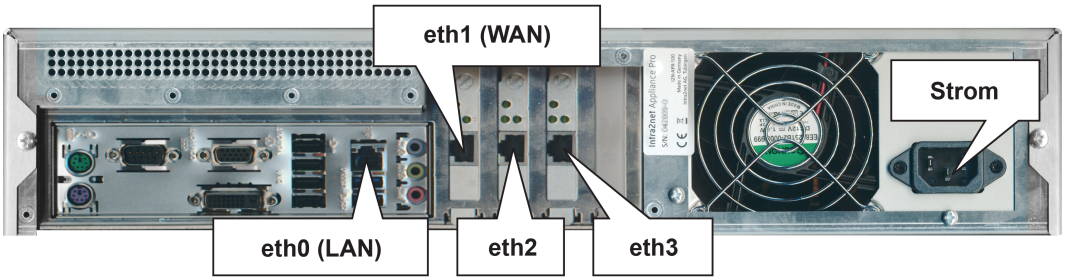
Die Anschlüsse für LAN, DSL und Strom befinden sich auf der Rückseite des Gerätes und sind entsprechend beschriftet.



Rückseite Intra2net Appliance Micro



Rückseite Intra2net Appliance Eco



Rückseite Intra2net Appliance Pro

3.4.2. Netzteile

Appliance Micro und Appliance Eco werden mit externen Netzteilen geliefert. Verwenden Sie die Geräte ausschließlich mit den mitgelieferten Netzteilen. Die Netzteile von Appliance Micro und Appliance Eco sind unterschiedlich und dürfen nur mit dem jeweils passenden Gerät genutzt werden.



Achtung

Vergewissern Sie sich vor dem Einstecken, dass es sich um das korrekte Netzteil handelt. Vergleichen Sie dazu den Aufdruck mit der Spannung an

Appliance und Netzteil. Durch zu hohe Spannung kann die Appliance schwer beschädigt werden.

3.4.3. Erdung (nur Appliance Eco)

Die Appliance Eco wird mit einem Netzteil in Schutzklasse II ausgeliefert. Das Appliance Gehäuse ist nicht mit der Schutzerde verbunden. Bei Verwendung von geschirmten Netzwerkkabeln können über die Kabelschirme Fehlerströme eingeschleppt werden. Daher verfügt das Gehäuse über einen Erdungsbolzen, der mit Schutzerde zu verbinden ist.

Verwenden Sie dafür grün/gelb gekennzeichnetes Kabel mit mindestens 1,5 mm² Kabelquerschnitt und verbinden es mit einem Erdungspunkt z.B. am Netzwerkschrank. Verwenden Sie auf der Seite der Appliance einen Gabel- oder Ringkabelschuh und legen diesen zwischen den beiden Zahnkränzen am Erdungsbolzen ein. Beauftragen Sie im Zweifel eine Elektrofachkraft.



3.4.4. Kabelhalter (nur Appliance Eco)

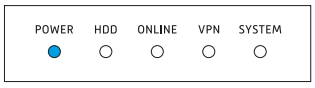
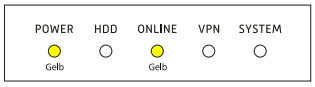
Damit der Stecker des Netzteils sich nicht aus Versehen lösen kann, verfügt die Appliance Eco über einen Kabelhalter. Der mitgelieferte Kabelbinder kann durch Drücken auf die Lasche geöffnet werden, um das Kabel zu befestigen oder wieder zu lösen.

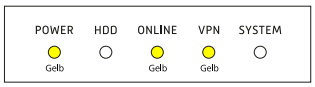
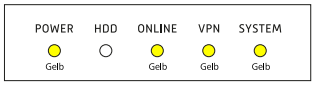


3.5. LED-Anzeige

Vorne rechts am Gehäuse eine befindet sich eine LED-Anzeige. Im Folgenden wird die Bedeutung der Anzeige beschrieben.

3.5.1. Start des Geräts

	Das Gerät startet. Stufe 1 läuft: BIOS, Bootloader und Kernel
	Das Gerät startet. Stufe 2 erreicht: Kernel und Initrd erfolgreich geladen

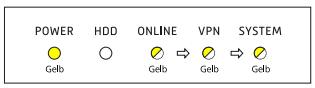
	Das Gerät startet. Stufe 3 erreicht: Rootfs erfolgreich gemountet
	Das Gerät startet. Stufe 4 erreicht: Read/Write-Mount erfolgreich

Während des Starts blinkt die HDD-LED unregelmäßig blau um Festplattenaktivität anzuzeigen.

3.5.2. Normaler Betrieb

Power-LED	konstant blau	Das Gerät ist eingeschaltet
HDD-LED	unregelmäßig blau blinkend	Festplattenaktivität
Online-LED	konstant blau	Internetverbindung aktiv
VPN-LED	konstant blau	VPN aktiv
System-LED	blau blinkend	Normaler Betrieb. Je länger die Blauphase, desto höher ist die Systemlast.

3.5.3. Update läuft

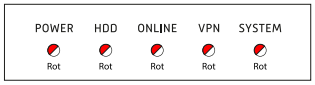
	Ein Update wird installiert. Schalten Sie das Gerät auf keinen Fall aus.

Während des Updates blinkt die HDD-LED unregelmäßig blau um Festplattenaktivität anzuzeigen.

3.5.4. Fehler

System-LED	gelb blinkend	Ein Fehler ist aufgetreten, siehe Hauptseite für Details

System-LED	rot blinkend	Ein schwerer Fehler ist aufgetreten, siehe Hauptseite für Details

	Es liegt ein schwerer Hardwarefehler vor und das Gerät schaltet sich zum Schutz sofort selbst aus. Prüfen Sie die Spannungsversorgung und Umgebungstemperatur.

3.6. Software

Die Intra2net Software ist auf der Intra2net 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.

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 Latenzen hinzukommen.

Die meisten Aufgaben eines Intra2net Systems werden typischerweise durch die Latenz von Festplattenzugriffen beschränkt und nicht durch Festplattendurchsatz oder fehlende CPU-Leistung. Dieser Punkt kann die Leistung eines Intra2net Systems also merklich beeinträchtigen.

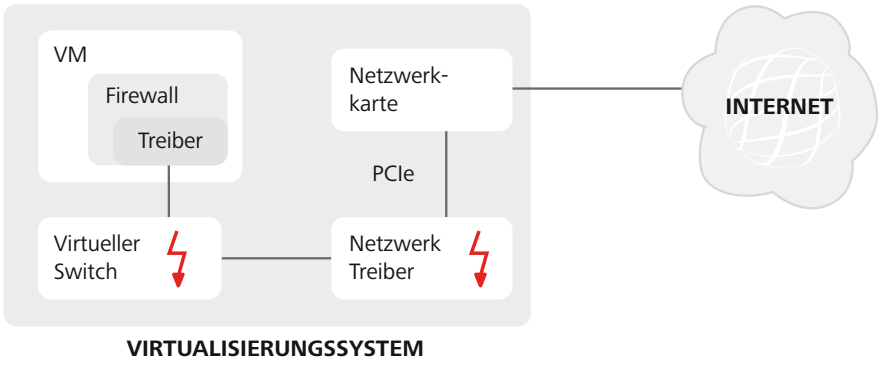
Wir empfehlen, dies durch den Einsatz schnellerer Festplatten (15.000 RPM) oder Solid-State-Disks zu kompensieren.

Außerdem empfehlen wir das virtuelle Laufwerk für das Intra2net System nicht als dynamisch wachsend / bei Bedarf zugeteilt zu konfigurieren, sondern von Anfang an vollständig zuzuweisen und zu allokieren. 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 das Intra2net System als Router und Firewall eingesetzt und stellt damit die Verbindung zum Internet her, kommt er direkt mit Netzwerkpaketen aus dem Internet in Berührung. Das Intra2net System 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.

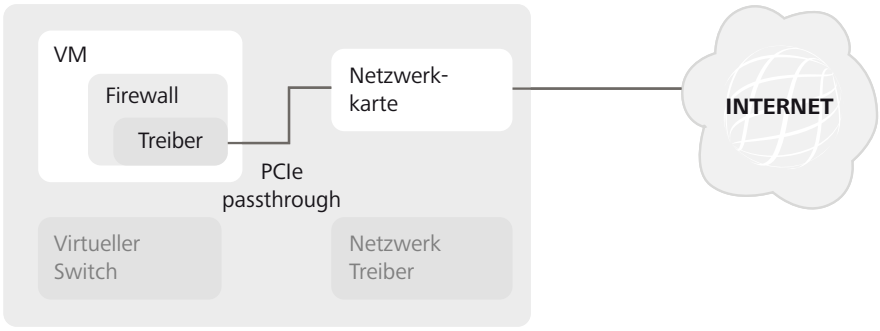
Wird das Intra2net System als virtuelle Maschine betrieben und seine Netzwerkkarten über die regulären Netzwerkfunktionen eines Virtualisierungssystems verwaltet, dann wird das Virtualisierungssystem diesen Paketen ungefiltert ausgesetzt. Dies gilt normalerweise für den Netzwerkkartentreiber und den 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 durchzureichen. Das Intra2net System 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 das Intra2net System 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].

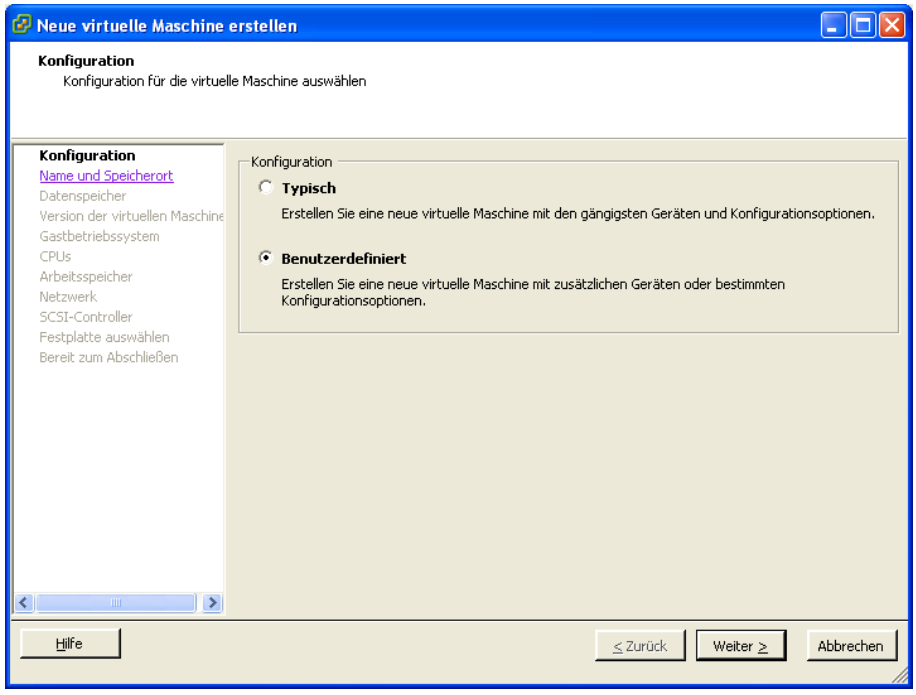
Das Intra2net System enthält von Haus aus alle Treiber und Programme, die für den zuverlässigen Betrieb auf VMware vSphere Hypervisor™ 4 nötig sind. Dies sind der paravirtualisierte Netzwerktreiber (VMXNET 3), der paravirtualisierte SCSI-Treiber (pvscsi) sowie die open-vm-tools. Eine zusätzliche Installation 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:

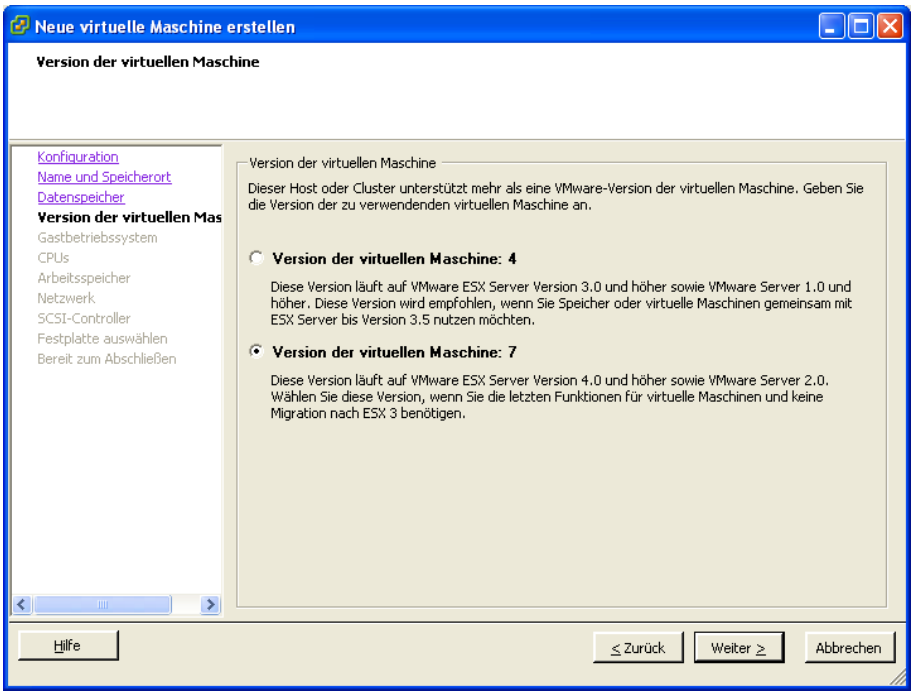
1. Starten Sie den vSphere Client, verbinden sich mit dem vSphere-Server und legen eine neue VM an.

2. Wählen Sie die benutzerdefinierte Konfiguration.

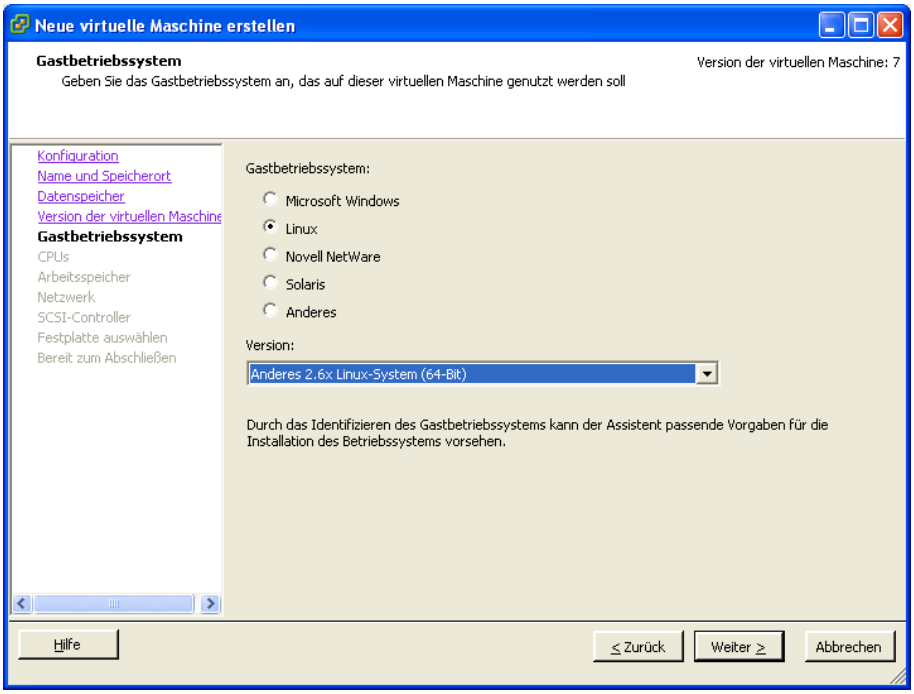


3. Benennen Sie die VM und weisen einen passenden Datenspeicher zu.

4. Wählen Sie eine virtuelle Maschine der Version 7



5. Wählen Sie als Betriebssystem ein "Anderes 2.6x Linux (64-Bit)".

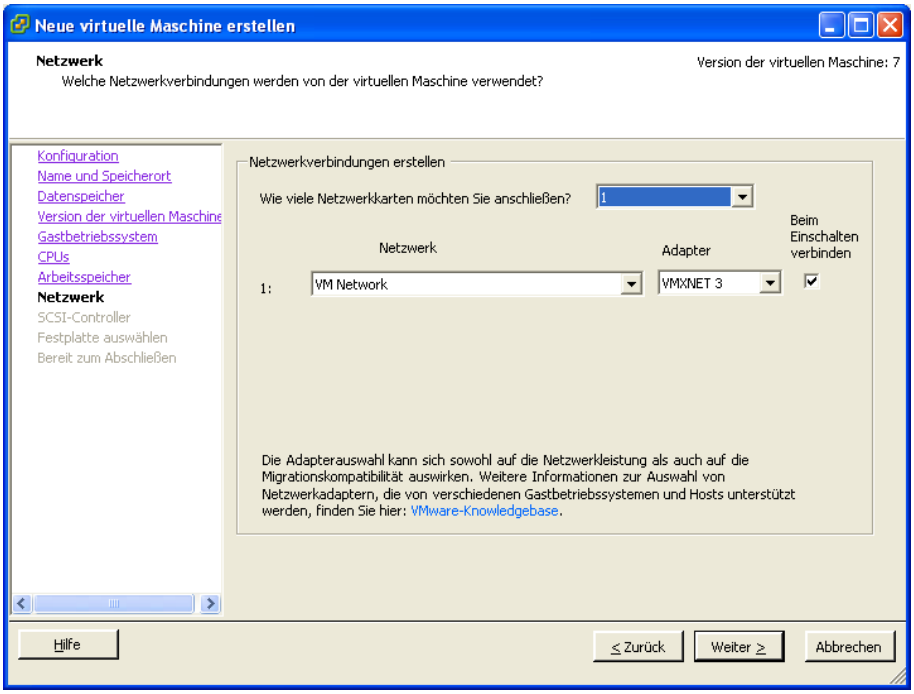


6. Geben Sie für das Intra2net System eine oder mehr CPUs frei. Das System erkennt beim Start automatisch die Anzahl der verfügbaren CPUs und nutzt diese.

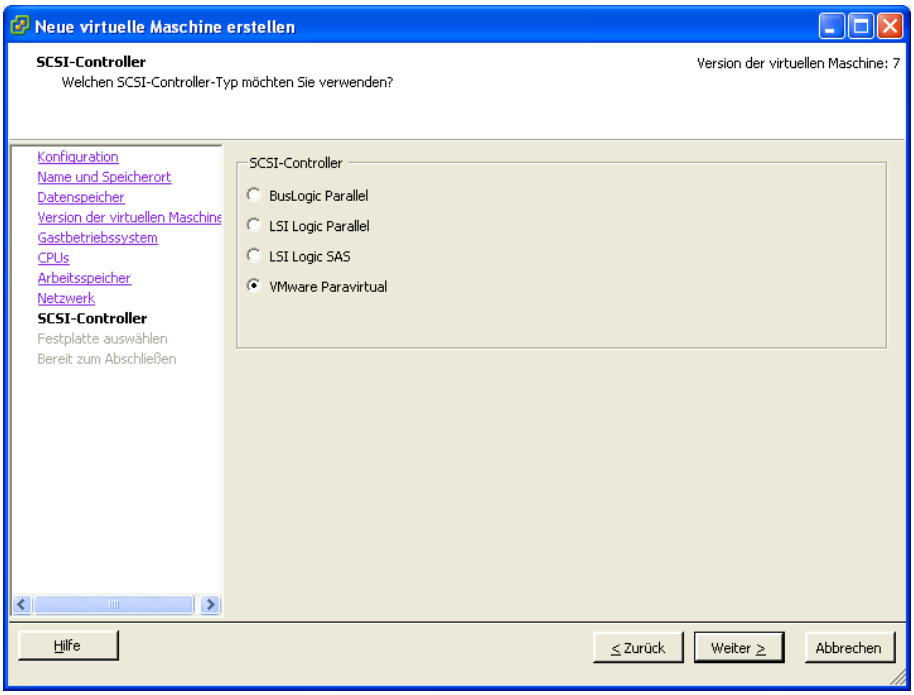
7. Geben Sie für das Intra2net System genügend Arbeitsspeicher frei. Wir empfehlen mindestens 2 GB bis 50 Benutzer, darüber entsprechend mehr.

8. Schließen Sie Netzwerkkarten des Typs "VMXNET 3" an. Die Anzahl hängt vom Layout des lokalen Netzes und dem Einsatzzweck des Intra2net Systems ab.

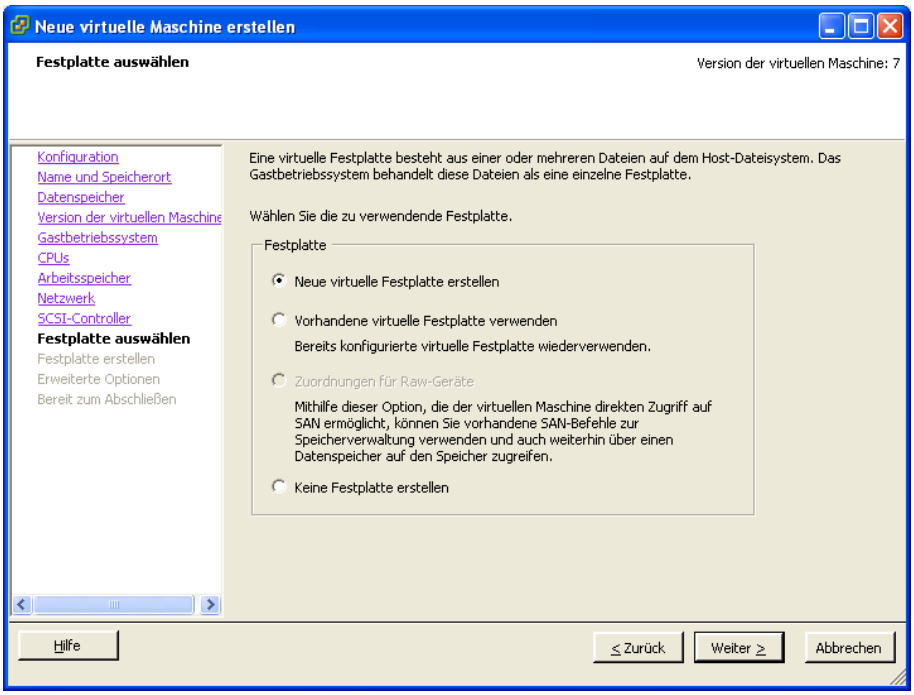
Es wird dringend davon abgeraten, direkt mit dem Internet verbundene Netzwerkkarten auf diese Weise anzubinden. Beachten Sie dazu Abschnitt 5.2, „Virtuelle Maschine mit direktem Internetzugang“.



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



10. Legen Sie eine neue virtuelle Festplatte an.

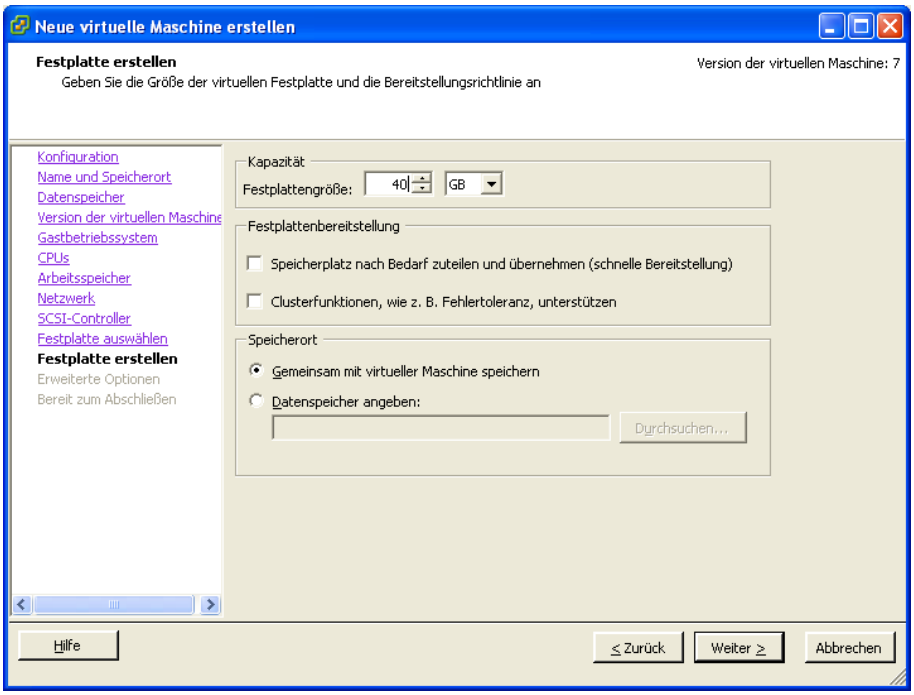


11. Weisen Sie dem Intra2net System eine Festplatte von mindestens 40 GB zu. Wird das Intra2net System nur zum Scannen von E-Mails und als HTTP-Proxyserver eingesetzt, reichen diese 40 GB im Normalfall auch aus. Nur wenn umfangreiche Statistikdaten für viele Benutzer längerfristig gespeichert werden sollen, wird mehr Speicher benötigt.

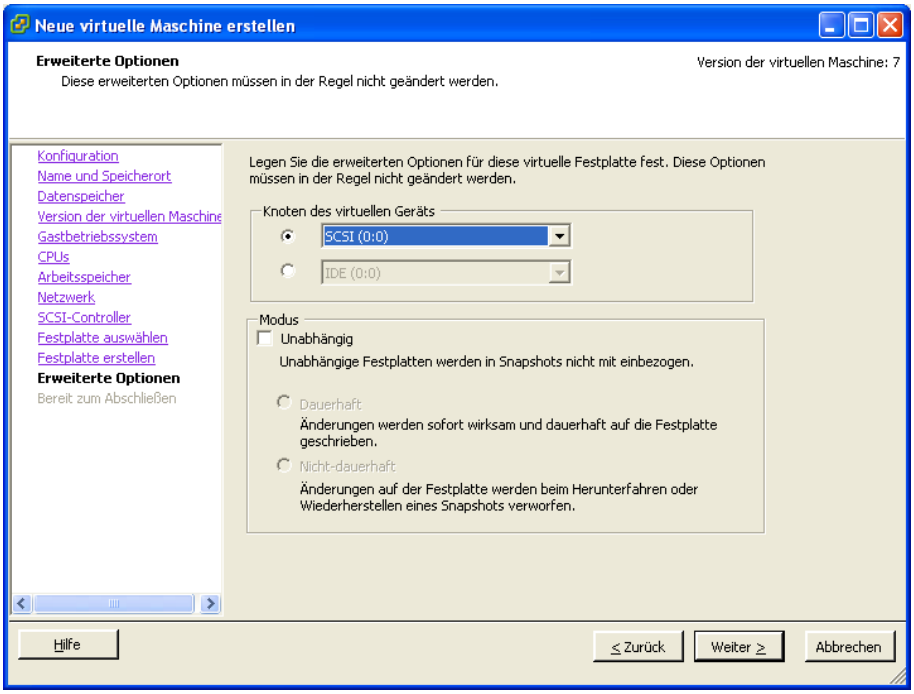
    Werden E-Mails oder Groupwaredaten dauerhaft auf dem Intra2net System abgelegt, wird mehr Festplattenplatz benötigt. Als Faustformel gilt Folgendes: (Gesamtes E-Mail-Volumen aller Benutzer + Statistikdaten) * (Anzahl auf dem System gespeicherter Backupsätze + 2) + 20 GB. Die Anzahl auf dem System gespeicherter Backupsätze beträgt dabei mindestens 1, empfohlen wird 2.

    Kalkulieren Sie immer etwas Reserve ein, da ein Vergrößern der Festplatte im Betrieb nur durch den Intra2net Support durchgeführt werden kann.

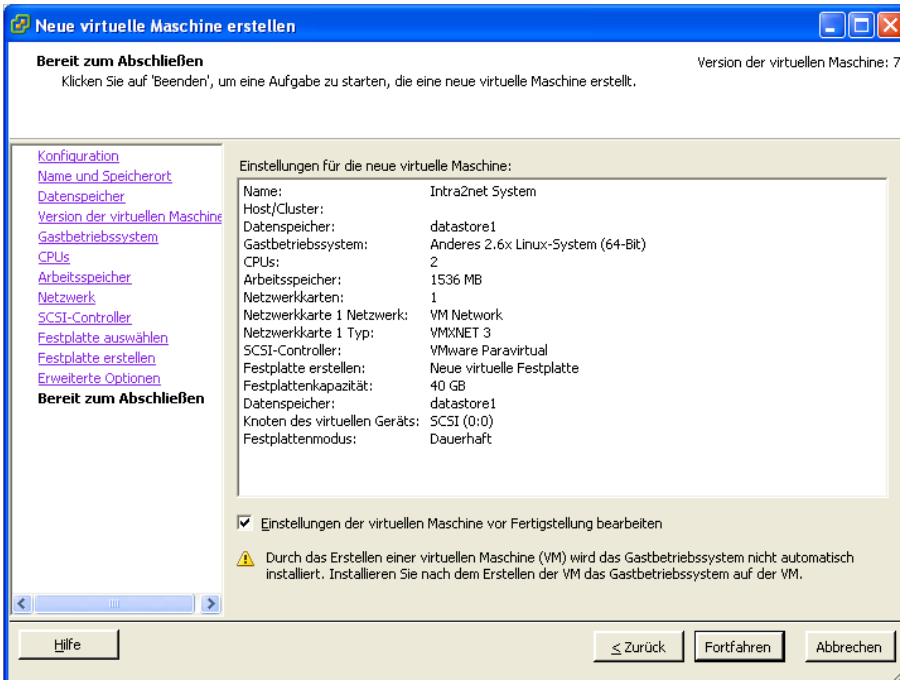
    Weisen Sie dem Intra2net System die gesamte Festplattenkapazität sofort zu, da dies in der Regel zu schnelleren Zugriffszeiten führt.



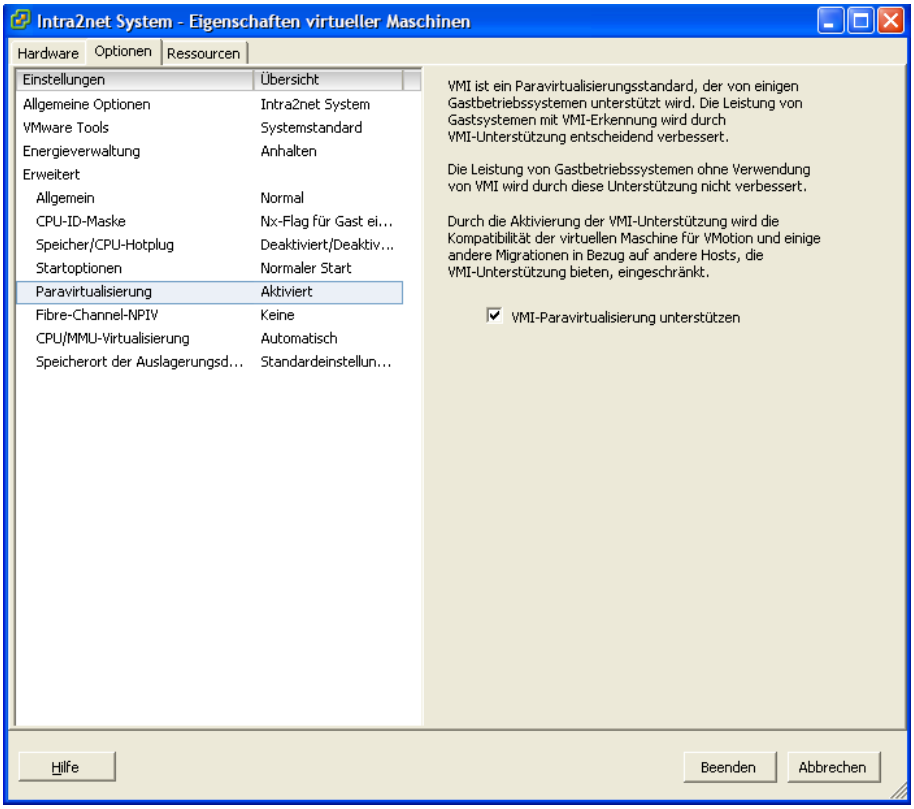
12. Weisen Sie die Festplatte auf Knoten SCSI(0:0) zu.



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

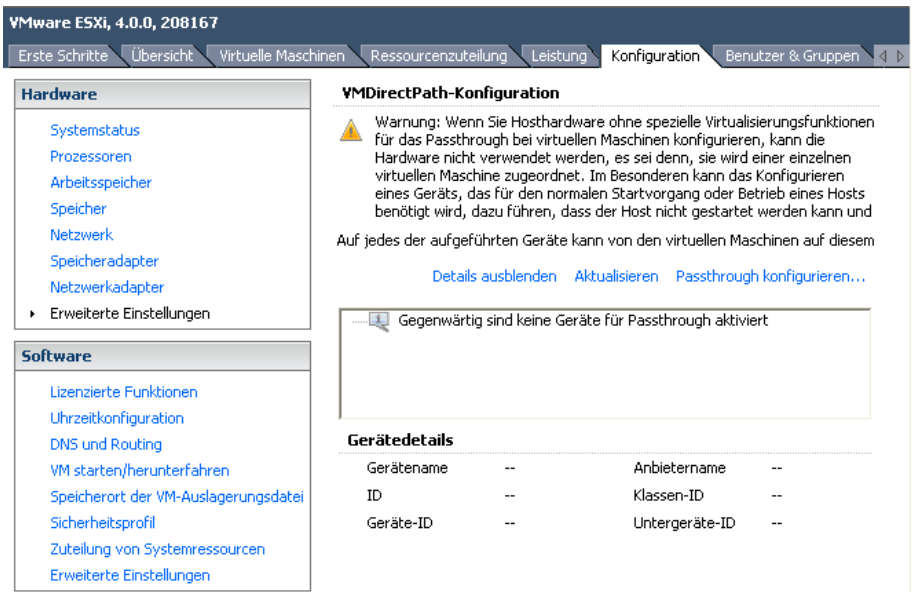
Wie in Abschnitt 4.1.3, „Kontakt mit ungefilterten Netzwerkpaketen“ beschrieben, empfehlen wir, Netzwerkkarten, die direkt mit dem Internet verbunden sind, als komplette PCI-Geräte an die VM durchzureichen.

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.

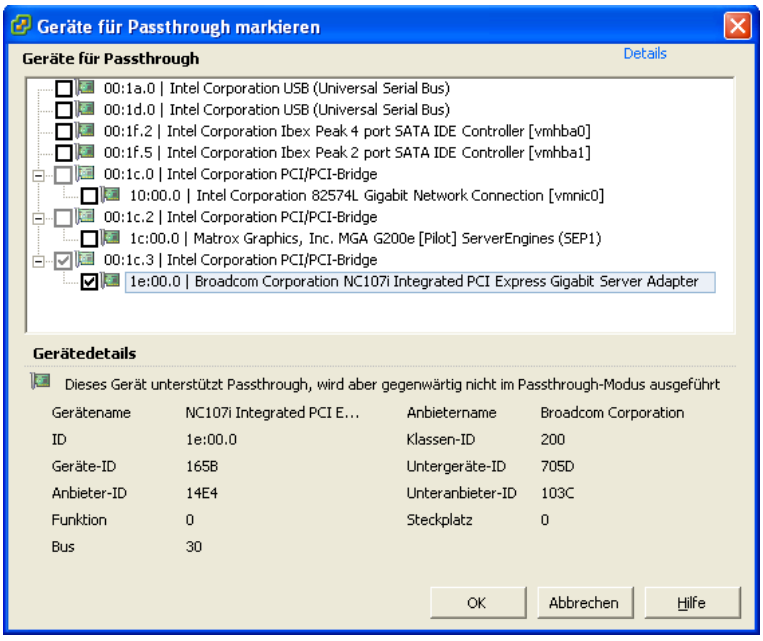
5.2.1. Vorbereitung des Servers

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

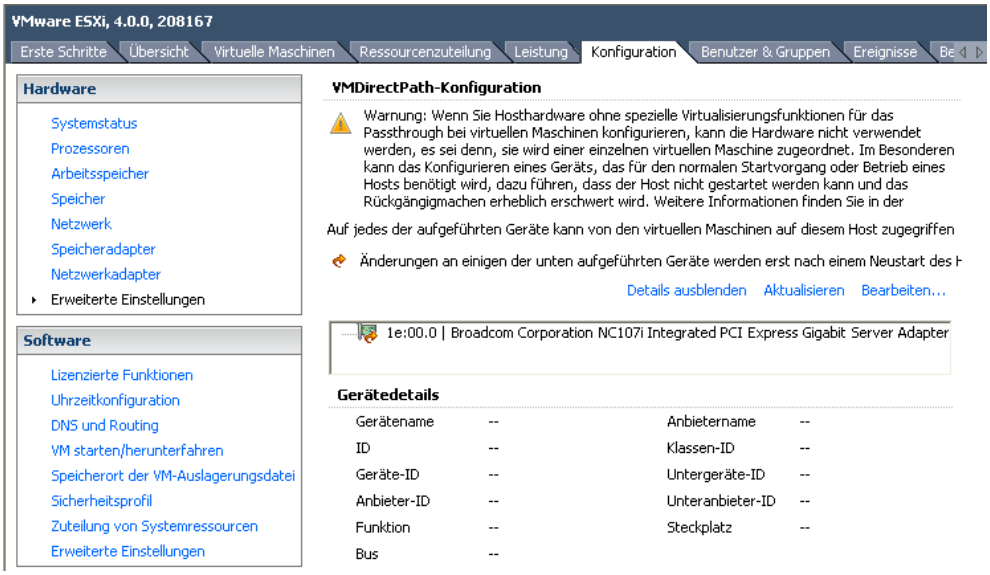
1. Starten Sie den vSphere Client und verbinden sich mit dem ESXi-Server. Wählen Sie links den Server selbst aus und öffnen das Menü "Konfiguration".



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.

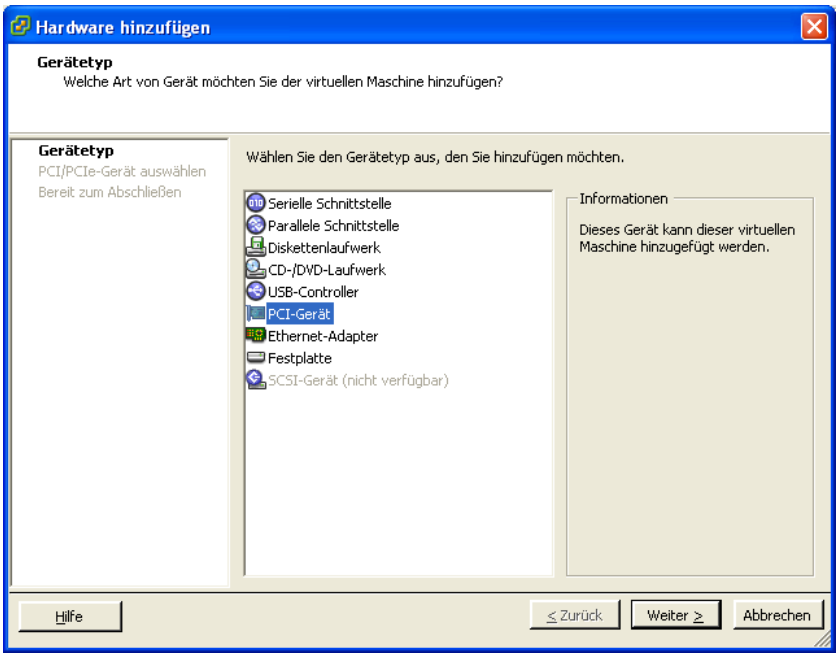


5.2.2. Einbinden der Netzwerkkarte in die VM

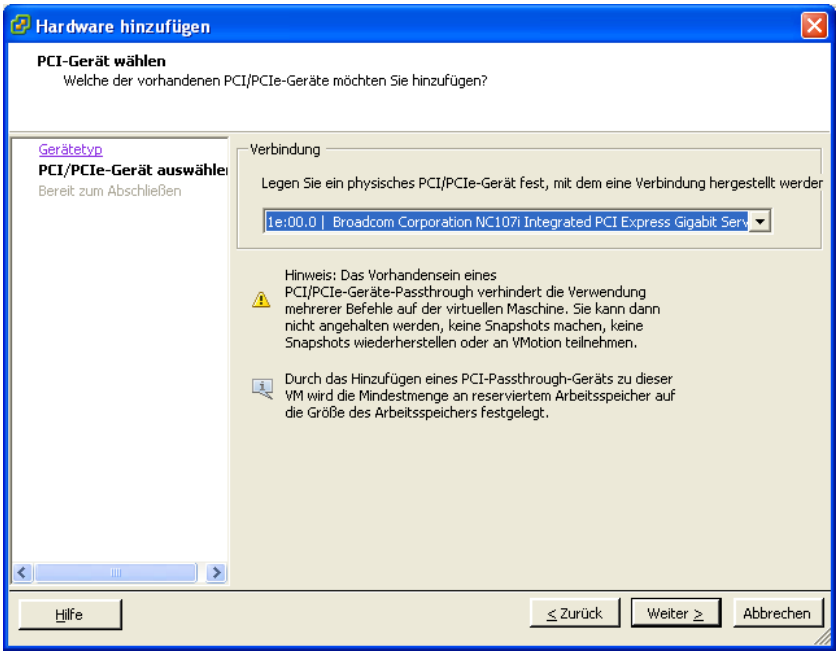
Die Netzwerkkarte kann nun wie folgt eingebunden werden:

1. Öffnen Sie die Konfiguration der VM und klicken im Menü "Hardware" auf "Hinzufügen".

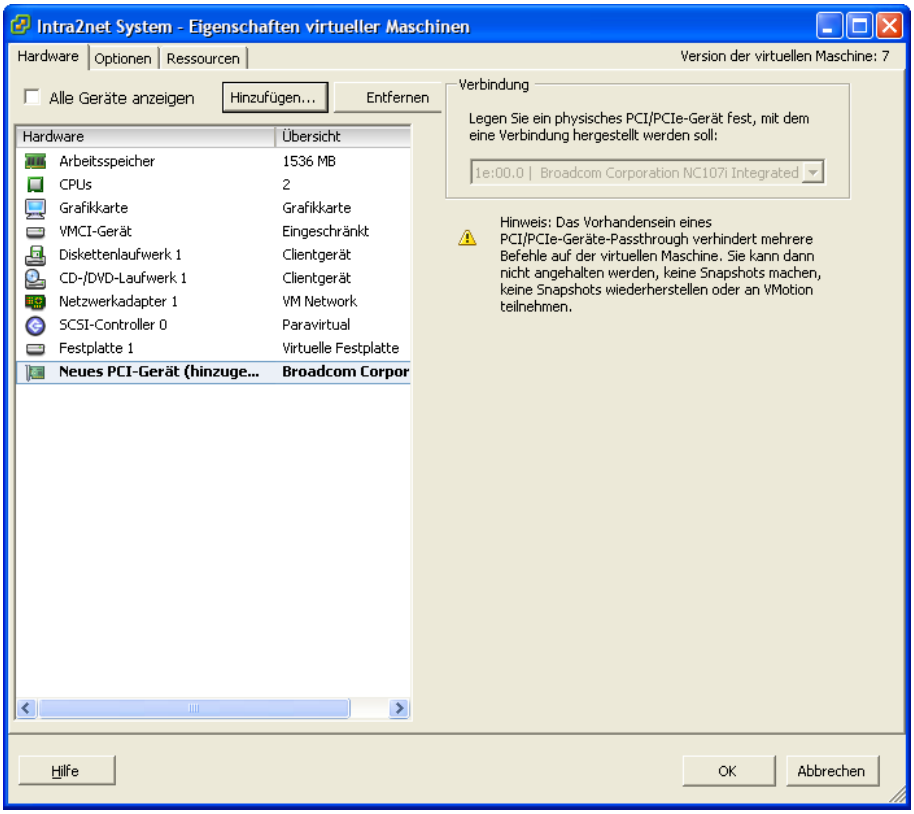
2. Fügen Sie ein PCI-Gerät hinzu.



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



4. Die Netzwerkkarte wird jetzt als zusätzliches Gerät angezeigt.

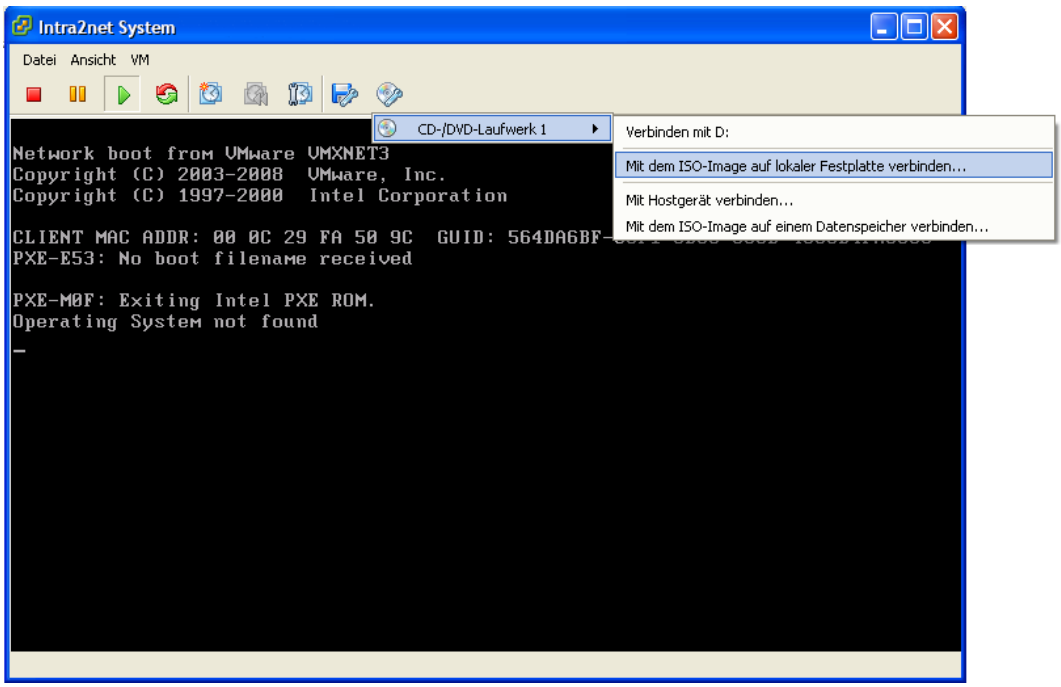


5.3. Installation des Intra2net Systems

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 Werkzeugleiste der Konsole auf das CD-Symbol und verbinden damit das CD-Laufwerk der virtuellen Maschine mit der ISO-Datei der Intra2net 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 Intra2net Installations-CD.

Die restliche Installation läuft ab wie in Abschnitt 2.6.2, „Installation von DVD“ 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.

Das Intra2net System 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.



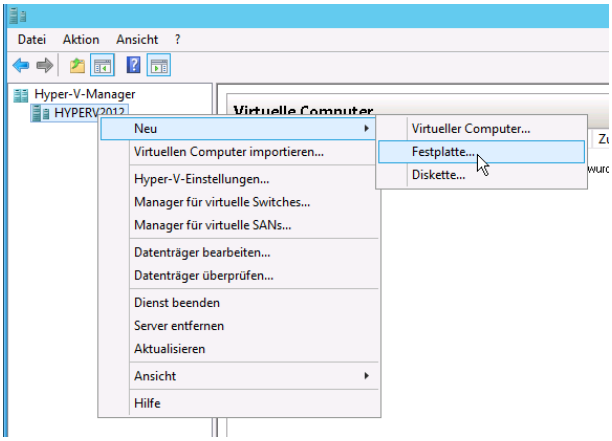
Achtung

Hyper-V bietet keine Möglichkeit PCI-Geräte wie Netzwerkkarten direkt an eine VM durchzureichen. Wir empfehlen Ihnen daher, ein mit Hyper-V virtualisiertes Intra2net System in Kombination mit einer zusätzlichen Hardware-Firewall einzusetzen. Weitere Informationen dazu finden Sie in Abschnitt 4.1.3, „Kontakt mit ungefilterten Netzwerkpaketen“.

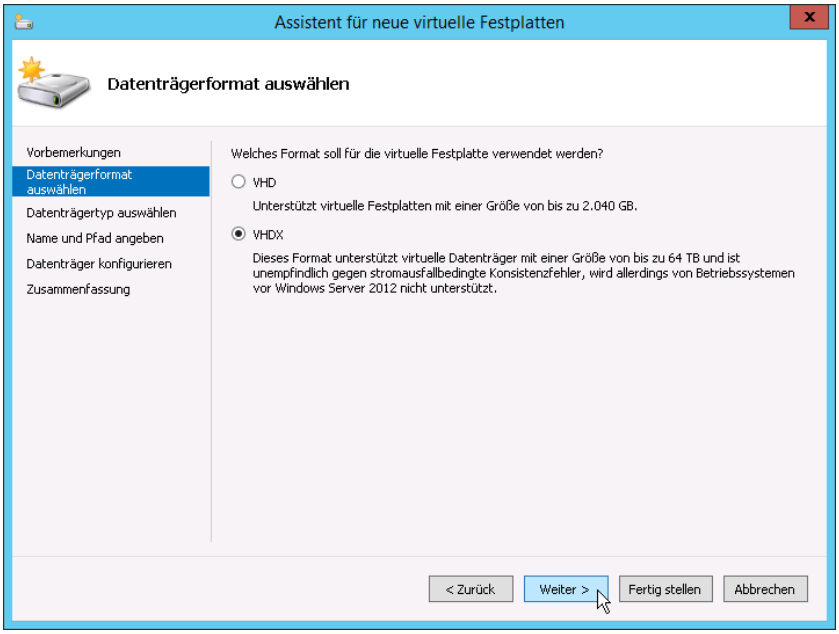
6.1. Konfiguration der virtuellen Maschine

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

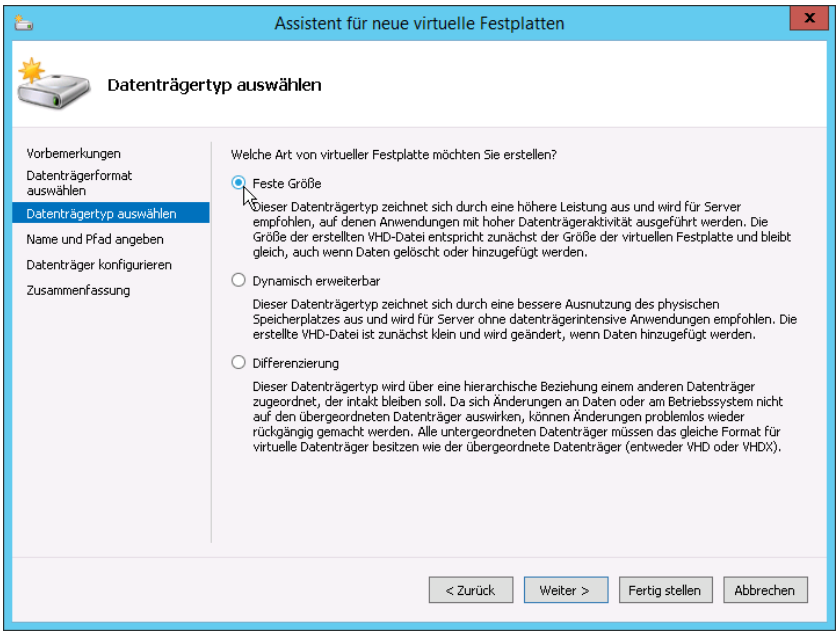
1. Öffnen Sie den Hyper-V-Manager und klicken mit der rechten Maustaste auf die gewünschte Hyper-V-Instanz. Wählen Sie "Neu > Festplatte...".



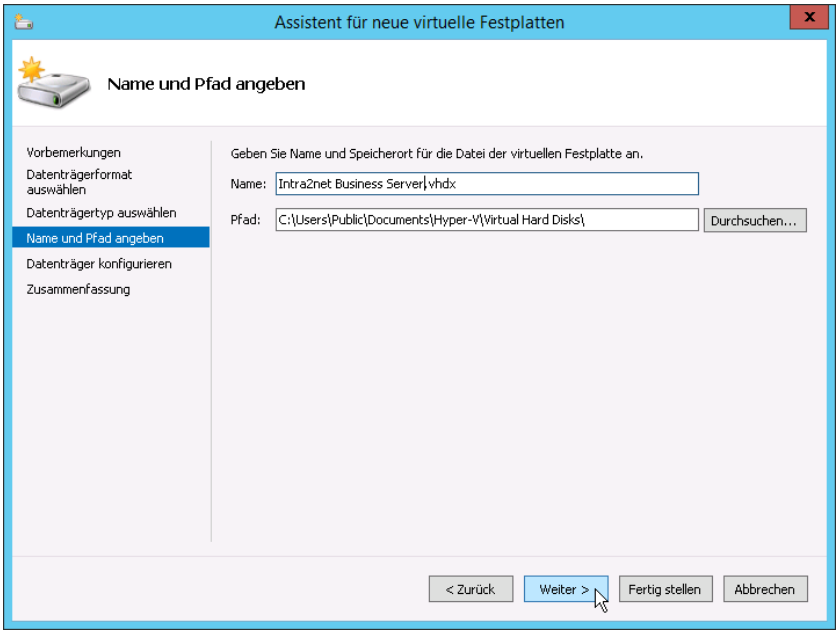
2. Wählen Sie das Format "VHDX".



3. Wählen Sie eine virtuelle Festplatte mit "Fester Größe".



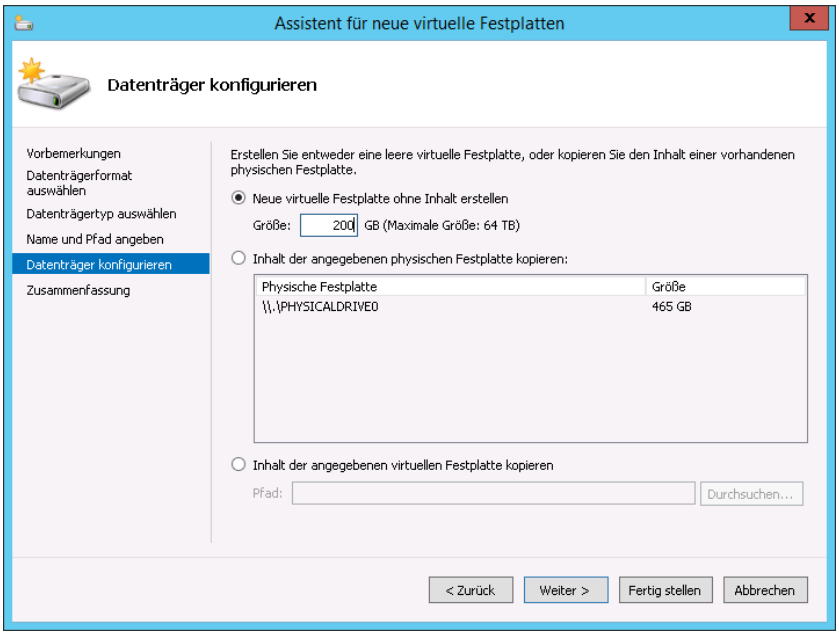
4. Geben Sie der virtuellen Festplatte einen zur zukünftigen VM passenden Namen.



5. Weisen Sie dem Intra2net System eine Festplatte von mindestens 40 GB zu. Wird das System 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.

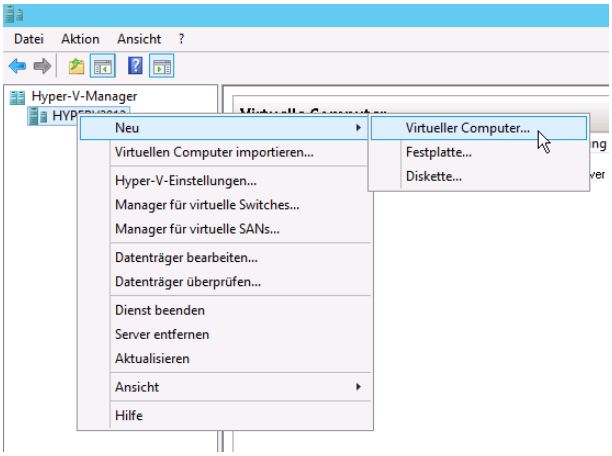
   Werden E-Mails oder Groupwaredaten dauerhaft auf dem Intra2net System abgelegt, wird mehr Festplattenplatz benötigt. Als Faustformel gilt Folgendes: (Gesamtes E-Mail-Volumen aller Benutzer + Statistikdaten) * (Anzahl auf dem System gespeicherter Backupsätze + 2) + 20 GB. Die Anzahl auf dem System gespeicherter Backupsätze beträgt dabei mindestens 1, empfohlen wird 2.

   Kalkulieren Sie immer etwas Reserve ein, da ein Vergrößern der Festplatte im Betrieb nur durch den Intra2net Support durchgeführt werden kann.

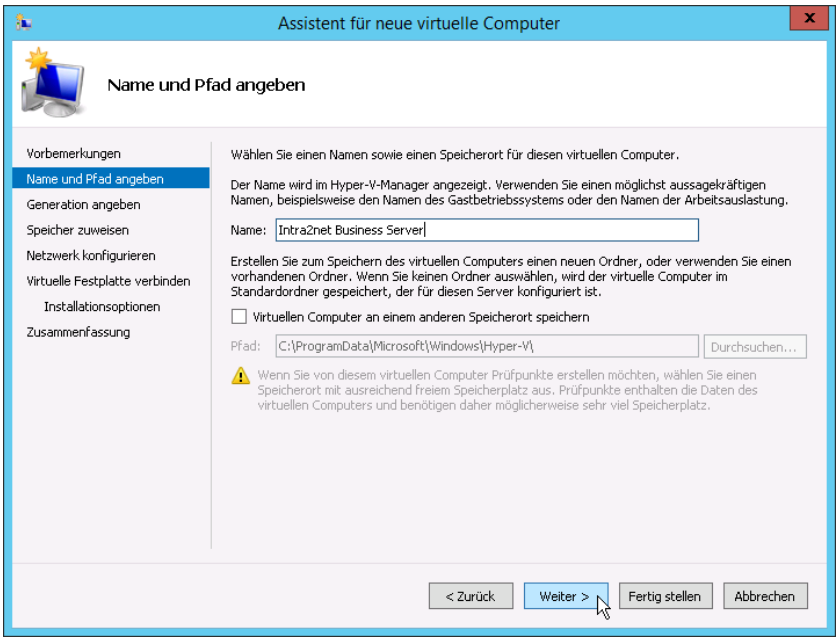


6. Legen Sie die virtuelle Festplatte fertig an.

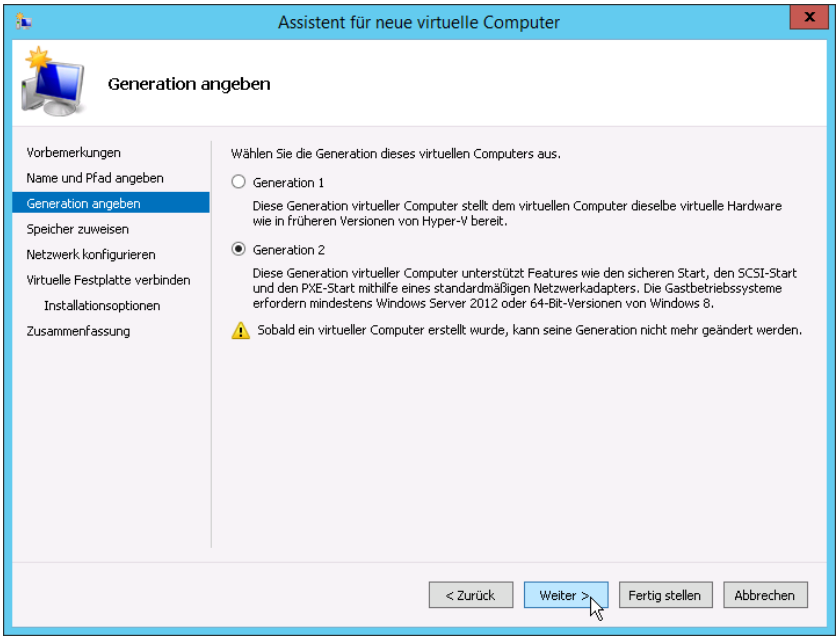
7. Klicken mit der rechten Maustaste auf die gewünschte Hyper-V-Instanz und wählen "Neu > Virtueller Computer...".



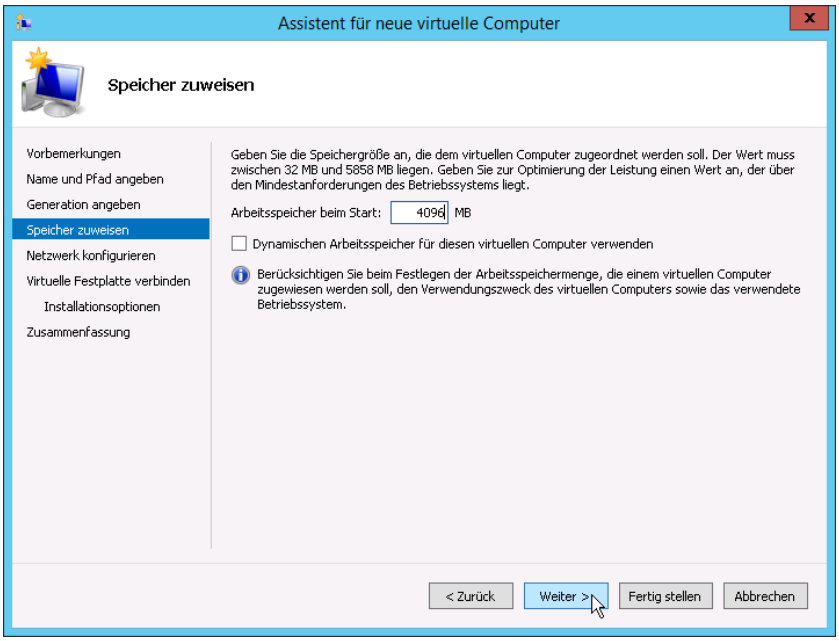
8. Geben Sie der VM einen Namen.



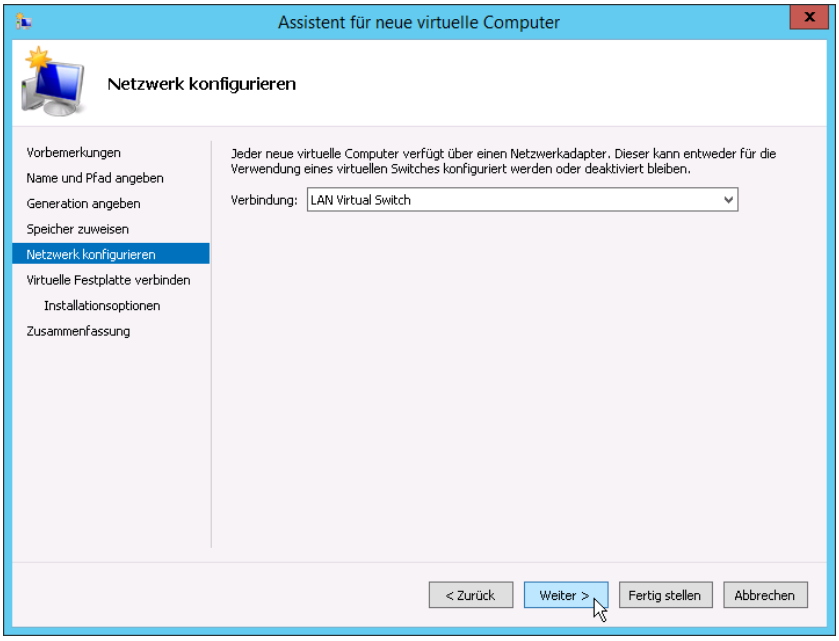
9. Wählen Sie Generation 2.



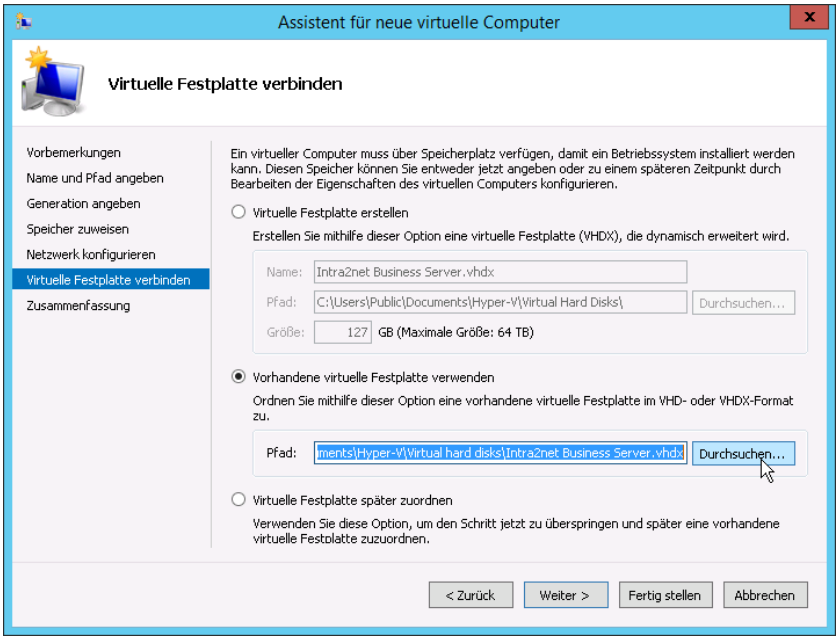
10. Weisen Sie der VM ausreichend Arbeitsspeicher zu. Verwenden Sie mindestens 2 GB. Deaktivieren Sie die Funktion "Dynamischer Arbeitsspeicher".



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



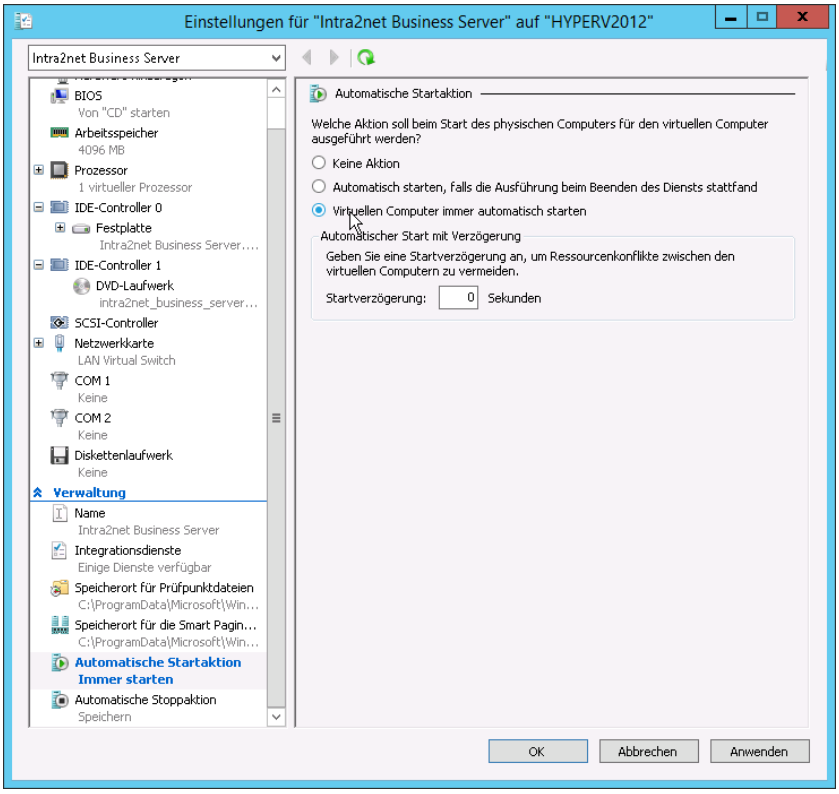
12. Weisen Sie die vorher erstellte virtuelle Festplatte zu.



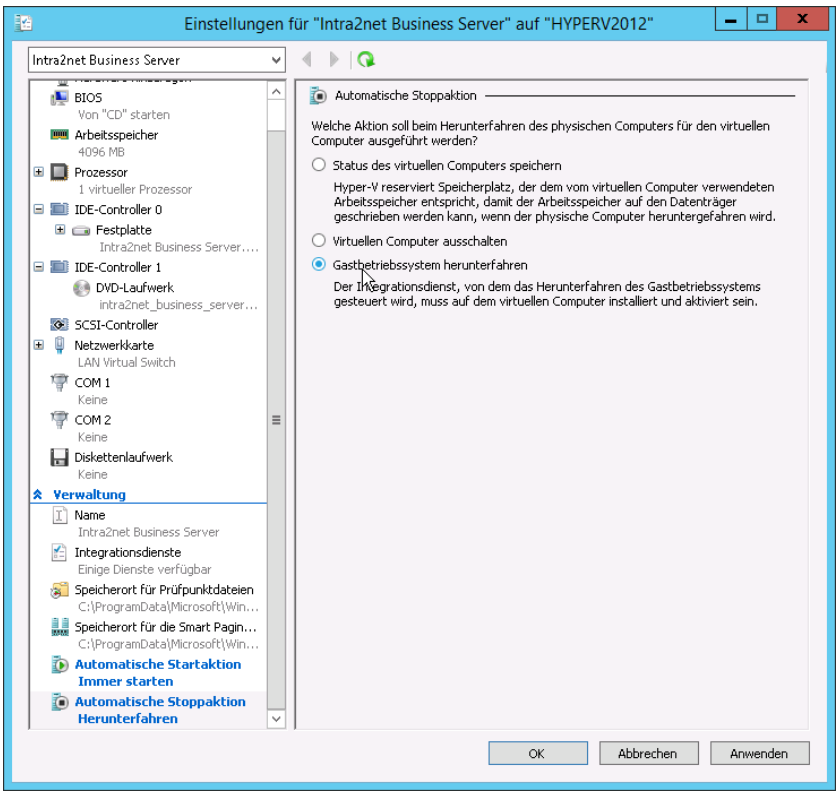
13. Schließen Sie das Anlegen der VM ab.

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

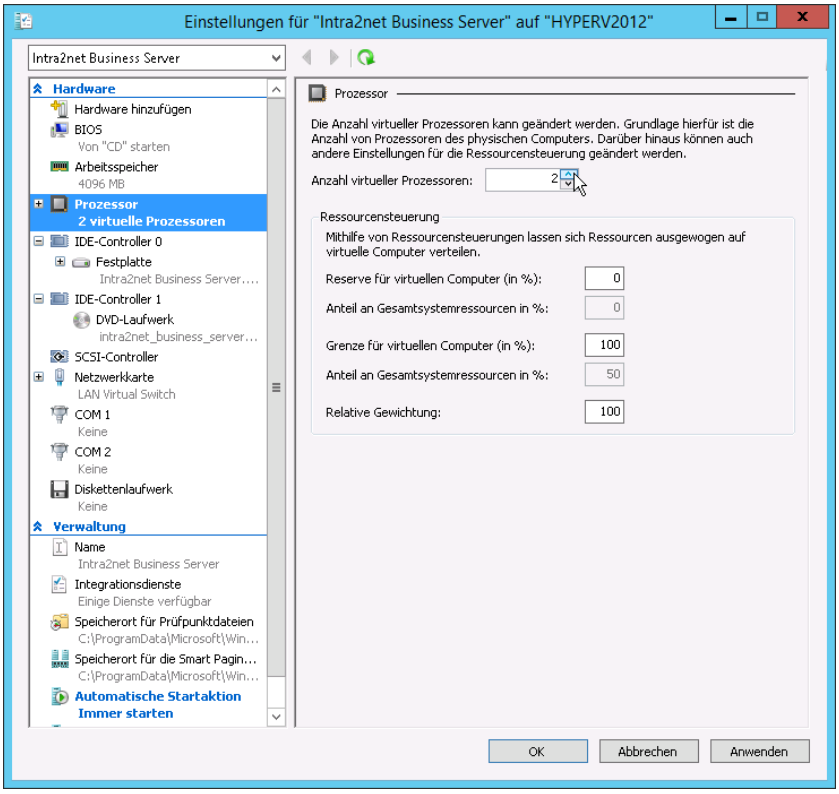
15. Lassen Sie die VM immer automatisch starten damit die VM immer verfügbar ist.



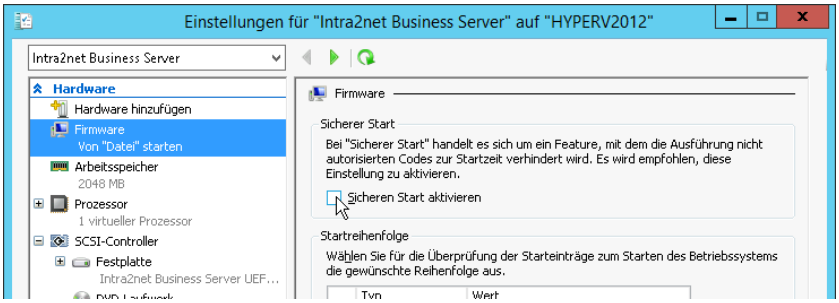
16. Lassen Sie die VM bei Herunterfahren des Hyper-V-Servers immer herunterfahren. Dies beugt Problemen durch Zeitsprünge vor.



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



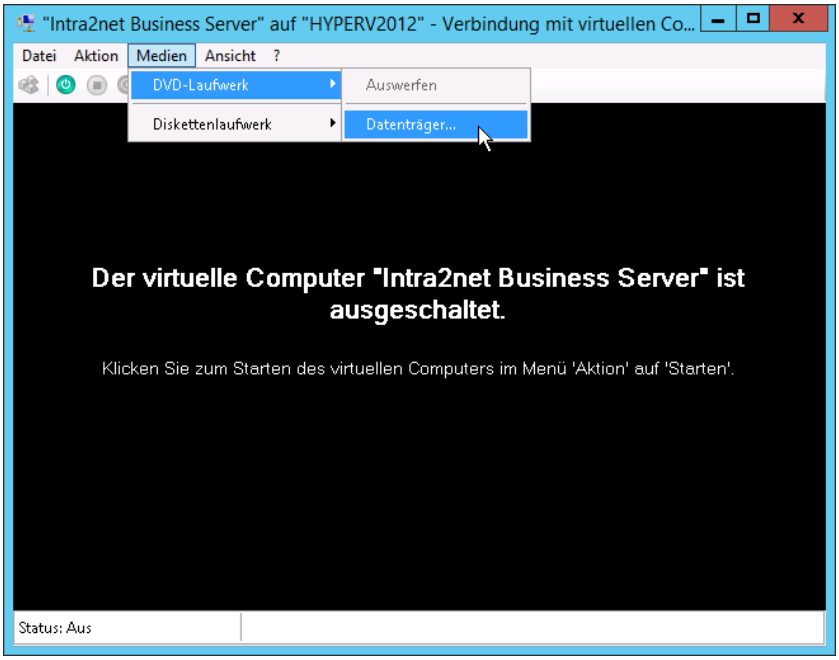
18. Deaktivieren Sie unter "Firmware" die Option "Sicheren Start aktivieren".



6.2. Installation des Intra2net Systems

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 Intra2net Installations-CD aus. Diese können Sie unter https://www.intra2net.com/ herunterladen.



3. Starten Sie die virtuelle Maschine über den grünen Startknopf.

Die restliche Installation läuft ab wie in Abschnitt 2.6.2, „Installation von DVD“ beschrieben.

7. Kapitel - Die Konsole

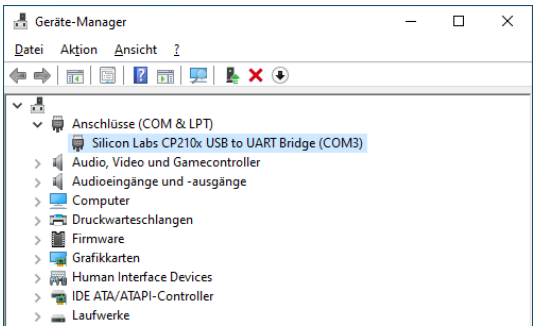
Nach der Grundinstallation startet das Intra2net System direkt in das Konsolenmenü.

Dies können Sie auch bei einem fertig installierten Intra2net System erreichen, indem Sie Monitor und Tastatur anschließen und sich mit Benutzername und Passwort eines Mitglieds der Administratorengruppe (standardmäßig **admin**) anmelden.

7.1. Intra2net Appliance Micro

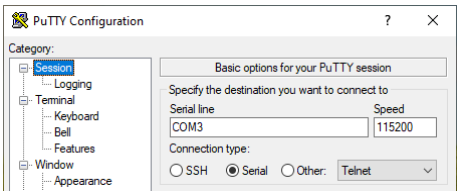
Die Appliance Micro verfügt über keinen Monitorausgang für die Konsole, sondern nutzt statt dessen eine serielle Konsole. Schließen Sie für den Zugriff das beiliegende Nullmodemkabel mit USB-Wandler an einen anderen PC an. Der D-sub/DE-9 Anschluss kommt dabei an die Appliance Micro, USB an den anderen PC von dem aus auf die Konsole zugegriffen werden soll.

Das Kabel verwendet einen Silabs CP2104-Wandler. Unter Windows müssen Sie dafür von https://www.silabs.com den "CP210x Universal Windows Driver" herunterladen und installieren. Öffnen Sie danach den Gerätemanager aus der Windows-Systemsteuerung und lesen die COM-Portnummer ab.



Für die Nutzung wird ein Terminalprogramm benötigt. Unter Windows sind PuTTY und TeraTerm empfehlenswert, unter Linux picocom.

Wählen Sie im Terminalprogramm eine serielle Verbindung, die passende Portnummer und stellen folgende Parameter ein: 115200 Baud, 8 Bit, No Parity, 1 Stoppbit. Bei TeraTerm geht dies über das Menü "Setup > Serial Port", bei PuTTY stellen Sie den "Connection type" auf "Serial", tragen die COM-Portnummer ein und unter "Speed" die Baudrate.



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 das Intra2net System über dieses Menü an die neue Konfiguration angepasst werden.

7.3. DNS und DHCP

Über dieses Menü können der Rechnername und die Domain des Intra2net Systems festgelegt werden.



Achtung

Wir raten klar davon ab, im lokalen Netz eine offizielle Domain (endet z.B. auf ".de", ".com" oder ähnliches) zu verwenden. Nutzen Sie statt dessen eine nur lokal gültige (endet z.B. auf ".internal", ".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 42.4, „Firewall-Notmodus“.

7.5. In Auslieferungszustand zurücksetzen

Mit dieser Funktion kann das Intra2net System in den Zustand nach der Auslieferung oder Erstinstallation zurückgesetzt werden. Alle Einstellungen, Benutzerdaten, Passwörter, E-Mails, Statistikdaten, Logdateien und Backups werden vom System gelöscht. Nur die Version der Intra2net-Software bleibt auf dem aktuellen Stand und wird nicht zurückgesetzt.

Das Gerät startet danach automatisch neu.

7.6. Das root-Passwort

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

Es wird bei Intra2net Appliances für jede Maschine individuell per Zufallsgenerator erzeugt und verschlüsselt bei Intra2net gespeichert. Falls ein Händler oder Kunde Zugriff auf die Linux-Shell wünscht, kann es über den Intra2net-Support angefordert werden.

Wird statt einer Intra2net Appliance eine Softwareversion des Intra2net Systems verwendet, muss das root-Passwort am Ende der Installation 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.

Das root-Passwort zählt zur Installation, nicht zur Konfiguration des Systems. Es ist daher nicht im Backup enthalten und wird beim Zurücksetzen der Konfiguration in den Auslieferungszustand nicht angetastet.

Das root-Passwort wird auch zum Schutz des Bootmanagers verwendet. Sollen die dort angebotenen Bootoptionen geändert werden, so muss sich der Nutzer mit Login **`root`** und dem root-Passwort anmelden.

Um das root-Passwort zu ändern, loggen Sie sich per SSH oder an der Konsole auf der Linux-Shell ein und verwenden das Programm set_root_grub_pwd.sh.

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 Intra2net System-Konsole auf den Login der Linux-Shell.

Bei einer seriellen Konsole loggen Sie sich mit dem Login **`root`** ein. Wählen Sie im Menü dann "Linux shell" für den Zugriff auf die Shell.



Achtung

Änderungen auf der Linux-Shell können die Funktion, Stabilität und Sicherheit des Intra2net Systems 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 das Intra2net System 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

Das Intra2net System befindet sich nach dem ersten Start für 30 Tage im Demomodus. In diesem Demomodus können alle Funktionen der Software ausprobiert werden, lediglich das Rückspielen von Backups, die im Demomodus erstellt wurden, ist nur mit einer vollwertigen Lizenz möglich.

Sobald das Gerät über eine Internetverbindung verfügt, können Sie im Menüpunkt Information > Lizenz einen Lizenzcode eingeben und damit das Gerät dann vollständig und dauerhaft betreiben.

Sollten Sie bis zum Ablauf der 30 Tage Demomodus keinen Lizenzcode eingeben haben, stellt das System danach seine Funktion ein und erlaubt u.a. weder Internetzugang noch Zugriff auf E-Mail und Groupware.

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.

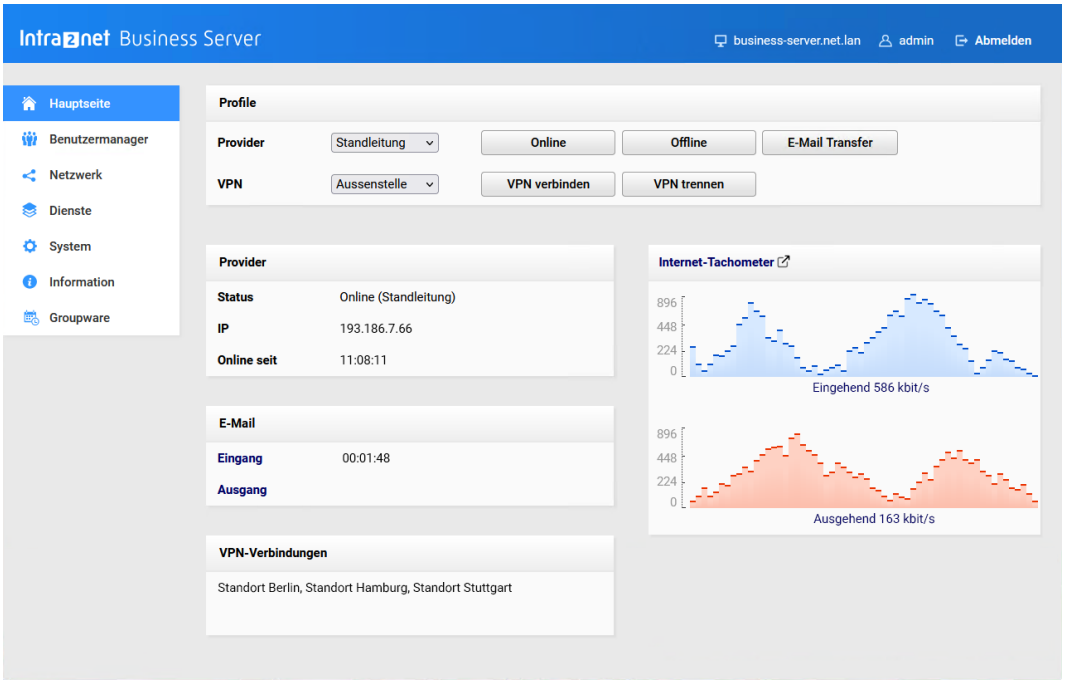
Der Informationsbereich zeigt Status- und Fehlermeldungen an. Fehlermeldungen können, wenn Sie zur Kenntnis genommen wurden, durch Klicken auf das "OK" dahinter entfernt werden. Ansonsten verschwinden sie nach einem Timeout (abhängig von Wichtigkeit und Typ).

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. Über einen Klick auf das Diagramm erreichen Sie die Live-Mitverfolgung im Statistikmenü.



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".

8.6. Herunterfahren notwendig

Intra2net Systeme müssen vor Trennen der Stromversorgung immer sauber heruntergefahren werden. Dies ist notwendig um die Integrität von Dateisystem und (wenn vorhanden) RAID-Spiegelung zu erhalten.

Drücken Sie zum Herunterfahren kurz (=kürzer als 1 Sekunde) den Powertaster. Das Gerät piepst, beginnt mit dem Herunterfahren und schaltet sich dann selbst aus. Alternativ können Sie das Menü "System > Herunterfahren" verwenden.

Ein zeitgesteuertes Hoch- und Herunterfahren ist auch möglich, Details finden Sie in Abschnitt 17.7, „Zeitgesteuertes Herunterfahren“.

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 Intra2net Systems umgeschrieben (Network Adress 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 das Intra2net System 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 9.3, „Zugriffsrechte eines Netzwerkobjekts“.

9.2. VLAN-Tagging

VLAN-Tagging ist die Aufteilung eines Netzes in virtuelle Teilnetze auf Ethernet-Ebene (OSI-Schichtmodell Ebene 2). Hierfür wird jedes Netzwerkpaket mit einer zusätzlichen Nummer markiert, dem VLAN-Tag. Ein managebarer, VLAN-fähiger Switch kann diese VLAN-Tags nutzen, um Teilnetze oder einzelne Geräte abzuschotten. Die Firewall des Intra2net Systems kann dann die Kommunikation zwischen diesen Teilnetzen überwachen und regeln.

Jede VLAN-Schnittstelle erscheint im Menü Netzwerk > Interfaces als eigenständige Schnittstelle. Neue VLAN-Schnittstellen können über die Schaltfläche "Neues VLAN" erstellt werden. Die zu vergebende VLAN-ID ist eine frei wählbare Nummer zwischen 1 und 4095. Jeder VLAN-Schnittstelle wird eine physische Schnittstelle zugeordnet.



Hinweis

Einige Switche weisen der VLAN-ID 1 eine besondere Stellung zu. Verwenden Sie am besten eine VLAN-ID ab 2 oder höher.

Über die Schaltfläche "VLAN entfernen" wird eine VLAN-Schnittstelle wieder gelöscht. Änderungen an den VLAN-Schnittstellen starten alle Netzwerkdienste neu, das System geht kurzzeitig offline.

Aus technischen Gründen ist es nicht möglich, VLANs auf Schnittstellen des Typs "DSL/Router" zu erstellen. Ist das System offline, so wird die physische Schnittstelle abgeschaltet und würde alle VLANs abschalten. Wenn Sie mehrere DSL/Router Schnittstellen auf einer physischen Schnittstelle bündeln möchten, so konfigurieren Sie die physische Schnittstelle auf den Typ "nicht verwendet" und erstellen anschließend beliebig viele VLAN-Schnittstellen auf dieser Schnittstelle.

Aus technischen Gründen können im System insgesamt maximal 50 verschiedene VLAN-Schnittstellen verwendet werden.

Für erhöhte Sicherheit empfehlen wir, LAN- und WAN-Datenverkehr über verschiedene physische Schnittstellen anzuschließen, anstatt sich nur auf VLANs zu verlassen. Fehlkonfigurationen am Switch leiten sonst ungefiltert Internet-Datenverkehr ins lokale Netz.

9.3. 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 Intra2net System 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 das Intra2net System 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.

9.4. Domain und DNS

Das Intra2net System leitet DNS-Anfragen ins Internet weiter. Wie und wohin wird beim aktuell aktiven Provider eingestellt, siehe 11. Kapitel, „Internet“.

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

9.4.1. Das Intra2net System als lokaler DNS-Server

Wenn Sie noch keinen vollwertigen DNS-Server in Ihrem lokalen Netzwerk haben, verwenden Sie das Intra2net System als DNS-Server und konfigurieren es wie in diesem Abschnitt

beschrieben. Wenn Sie bereits einen anderen DNS-Server (z.B. einen Windows Domain Controller) verwenden, gehen Sie dagegen wie in Abschnitt 9.4.2, „Anderen DNS-Server im LAN anbinden“ beschrieben vor.

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.

Das Intra2net System 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 das Intra2net System ja DNS-Server für die lokale Domain ist, kann es 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.

9.4.2. Anderen DNS-Server im LAN anbinden

Verwenden Sie einen anderen DNS-Server für die lokale Domain (z.B. einen Windows Domain Controller), tragen Sie den Rechnernamen des Intra2net Systems und die im lokalen Netz verwendete Domain 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 das Intra2net System mit seiner IP. Für Windows Server ist dies im folgenden Abschnitt beschrieben.

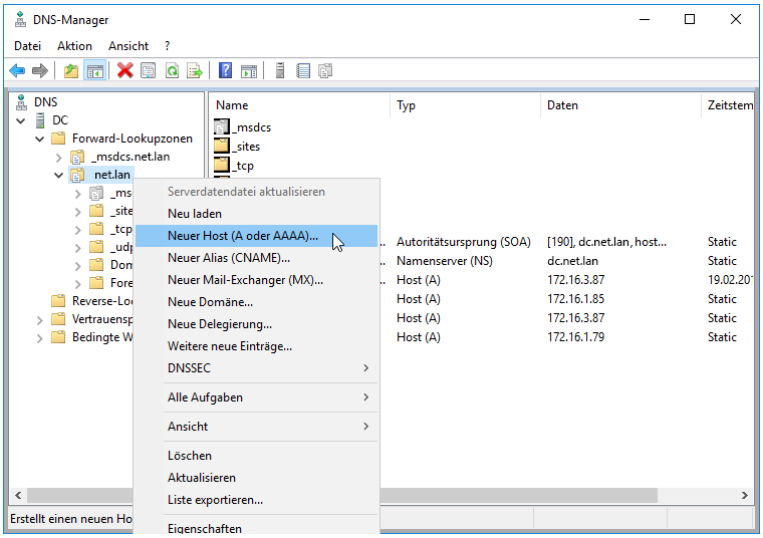
9.4.2.1. Eintragen des Intra2net Systems auf einem Windows DNS-Server

Wenn Sie einen Windows DNS-Server im lokalen Netz verwenden, muss dieser den Namen und die IP des Intra2net Systems auflösen können, damit alle Rechner im lokalen Netz das Intra2net System unter seinem DNS-Namen ansprechen können. Gehen Sie wie folgt vor um einen DNS-Eintrag für das Intra2net System anzulegen:

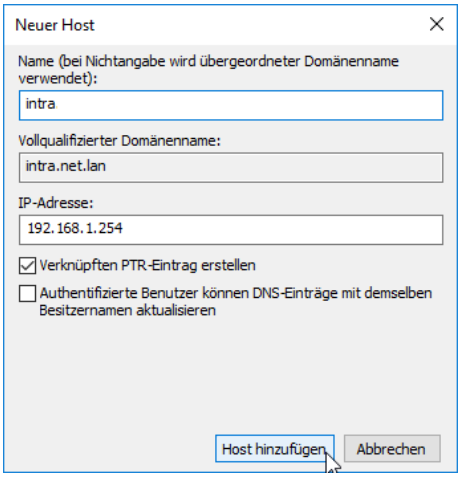
1. Öffnen Sie auf dem Windows Server den DNS-Manager über das Menü "Start > Windows-Verwaltungsprogramme > DNS".

2. Öffnen Sie im Baum auf der linken Seite die Forward-Lookupzonen Ihres Servers.

3. Klicken Sie mit Rechts auf die von Ihnen verwendete lokale Domain und wählen im Kontextmenü "Neuer Host (A oder AAAA)".



4. Tragen Sie den Namen und die IP des Intra2net Systems ein. Lassen Sie einen verknüpften PTR-Eintrag erstellen.



9.4.3. DNS für andere Domains weiterleiten

Das Intra2net System 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.

9.4.4. 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].

Das Intra2net System kann diese Angriffe wirkungsvoll verhindern, indem es 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.

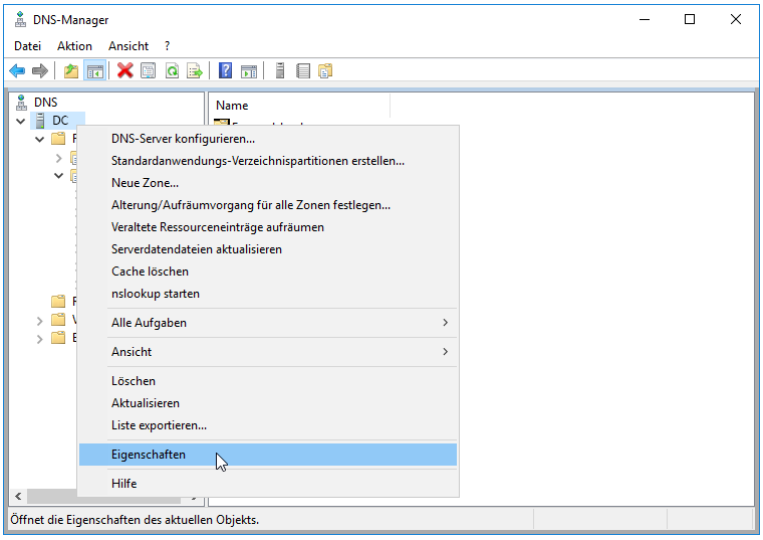
Alle DNS-Server, die für lokale oder lokal geroutete Domains zuständig sind, müssen unter den entsprechenden Domains als DNS-Weiterleitung konfiguriert werden. Die dort hinterlegten Server dürfen dann mit lokalen IPs antworten.

9.4.4.1. DNS-Rebind-Schutz für Windows DNS-Server

Windows DNS-Server haben keinen eigenen Schutz vor DNS-Rebind-Angriffen. Wenn Sie einen Windows DNS-Server im lokalen Netz verwenden und wie in Abschnitt 9.4.2, „Anderen DNS-Server im LAN anbinden“ konfiguriert haben, gehen Sie wie folgt vor um diesen vor DNS-Rebind zu schützen:

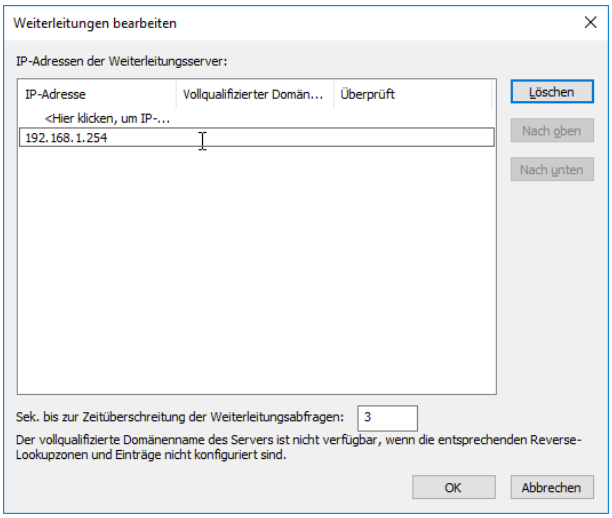
1. Öffnen Sie auf dem Windows Server den DNS-Manager über das Menü "Start > Windows-Verwaltungsprogramme > DNS".

2. Klicken Sie im Baum auf der linken Seite mit Rechts auf den Namen des DNS-Servers und öffnen im Kontextmenü die "Eigenschaften".

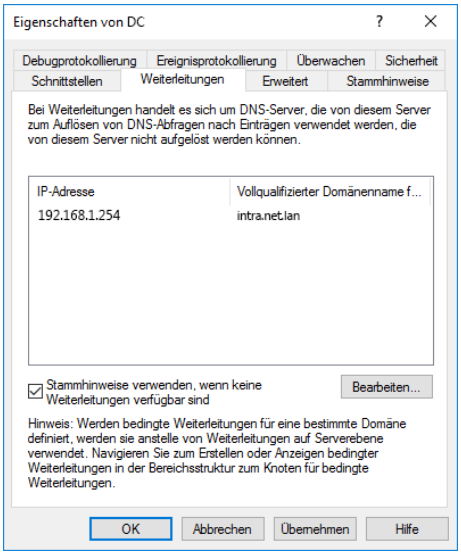


3. Wechseln Sie auf den Reiter "Weiterleitungen" und klicken auf "Bearbeiten".

4. Tragen Sie die IP des Intra2net Systems ein und entfernen alle anderen Einträge (wie z.B. Router oder DNS-Server des Internetproviders).



5. In der Weiterleitungsübersicht wird jetzt nur noch das Intra2net System angezeigt. Alle DNS-Anfragen ins Internet laufen jetzt über das Intra2net System und werden vor DNS-Rebind geschützt.



9.5. Clients eintragen

Unter Netzwerk > Intranet > Rechner können einzelne Rechner eingetragen werden. Jedem eingetragenen Rechner können damit eigene Zugriffsrechte (siehe Abschnitt 9.3, „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 im lokalen Netz gesucht werden.

9.5.1. Wake-On-LAN

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

Damit auch Endanwender einfach Wake-On-LAN verwenden können, z.B. um ihre Workstations aus der Ferne durch ein VPN hindurch einzuschalten, gibt es Wake-On-LAN-Links. Durch das einfache Öffnen des Links, z.B. mit einem Webbrowser oder Skript, wird direkt die Wake-On-LAN-Funktion ausgelöst. In dem Link sind alle nötigen Informationen enthalten, daher ist keine weitere Eingabe, Bestätigung, Login oder ähnliches zum Auslösen des Wake-On-LAN notwendig.

Der Wake-On-LAN-Link enthält einen Zufallswert, der zur Authentifizierung verwendet wird. Soll den bisherigen Nutzern das Recht zur Nutzung entzogen werden, klicken Sie auf "Link erstellen". Es wird der bisherige Link angezeigt. Klicken Sie jetzt auf "Bisherigen Link ungültig machen". Dadurch wird ein neuer Link erstellt und der bisherige Link ist ungültig geworden.

9.5.2. DHCP

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 sowie Wake-On-LAN-Links zu erstellen. 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 herauszunehmen und eine andere IP außerhalb eines Pools zuzuweisen. Ändern Sie dazu einfach die IP und klicken auf "Einstellungen speichern".

9.6. DHCP-Server

Das Intra2net System 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 9.7, „Bereiche eintragen“) zu.

Es darf in einem Netz immer nur ein DHCP-Server aktiv sein. Das Intra2net System prüft daher beim Start, ob ein anderer DHCP-Server aktiv ist und deaktiviert seinen eigenen gegebenenfalls.

Normalerweise übermittelt das Intra2net System 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 das Intra2net System 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.

9.7. Bereiche eintragen

Unter Netzwerk > Intranet > Bereiche können IP-Bereiche (Von-Bis) eingetragen werden. Diesem gesamten Bereich können damit eigene Zugriffsrechte (siehe Abschnitt 9.3, „Zugriffsrechte eines Netzwerkobjekts“) zugewiesen werden.

Im Gegensatz zu den einzelnen Rechnern kann das Intra2net System 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

9.8. 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 das Intra2net System hochladen bzw. herunterladen. Dies ist besonders sinnvoll, wenn Sie bereits eine Rechnerdatenbank besitzen, aus der sich die Daten exportieren lassen.

9.8.1. 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

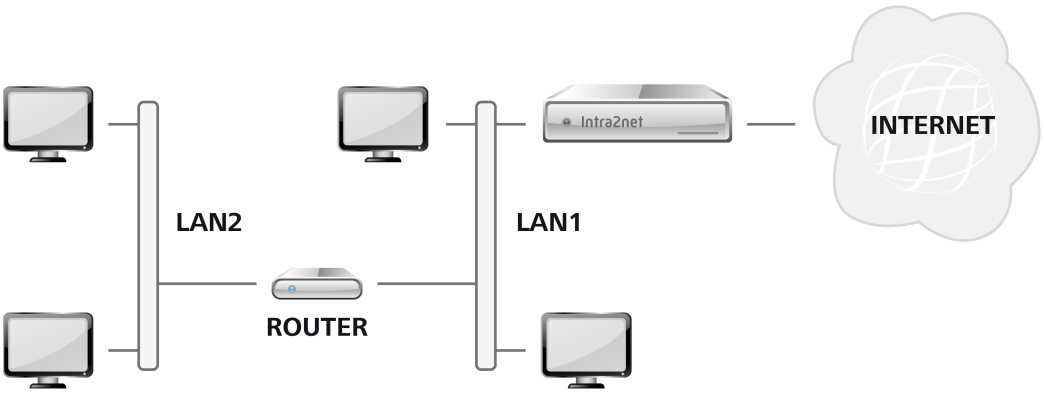
Bitte beachten Sie, dass das eingetragene Zugriffsrecht exakt mit dem Namen eines Zugriffsrechts im System übereinstimmen muss.

9.8.2. 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.

9.9. Routing im Intranet

Das Intra2net System kann über mehrere interne Netze routen. Dies ist sinnvoll z.B. wenn mehrere Firmen sich ein Intra2net System teilen oder wenn einzelne Stockwerke oder Abteilungen unterschiedliche Netze verwenden.



Ein Rechner oder Router im Netz des Intra2net Systems muss dabei zwischen den Netzen routen. Geben Sie dessen IP unter Netzwerk > Intranet > Routing als Gateway IP ein. Soll das Intra2net System selbst zwischen den Netzen routen, so schließen Sie das andere Netz an eine der Netzwerkkarten des Intra2net Systems 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 11.3, „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 Intra2net Systems ist nur für Verbindungen von dem gerouteten Netz ins Internet und andere, direkt an das Intra2net System angeschlossene Netze wirksam. Die Firewall funktioniert prinzipbedingt nicht für Verbindungen zwischen dem gerouteten und dem am Intra2net System und Router angeschlossenen Netz. Um die System-Firewall zwischen verschiedenen lokalen Netzen nutzen zu können, müssen diese Netze direkt an eine Netzwerkschnittstelle des Intra2net Systems 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 das Intra2net System z.B. über die Rechnernamen **`intra.net.lan`** und **`meinintra.dyndns.org`** ansprechen wollen, benötigen Sie 2 verschiedene Zertifikate.

Das Intra2net System 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 das Intra2net System von allen Clients im lokalen Netz unter seinem konfigurierten DNS-Namen erreichbar sein. Beachten Sie daher unbedingt Abschnitt 9.4, „Domain und DNS“ und testen, ob das Intra2net System 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. die Bundesnetzagentur momentan 2048 Bit und SHA2-256 als Signaturalgorithmus (siehe Algorithmenkatalog 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.

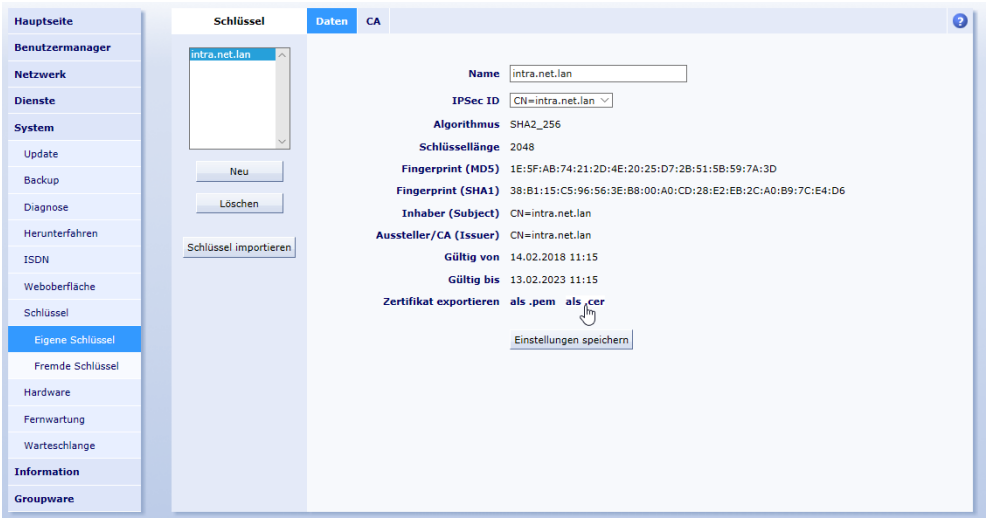
10.3.1. Installation unter Windows

Im Folgenden wird beschrieben, wie Sie das Zertifikat des Intra2net Systems 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 Intra2net System genutzt werden, muss das Zertifikat dort zusätzlich installiert werden.

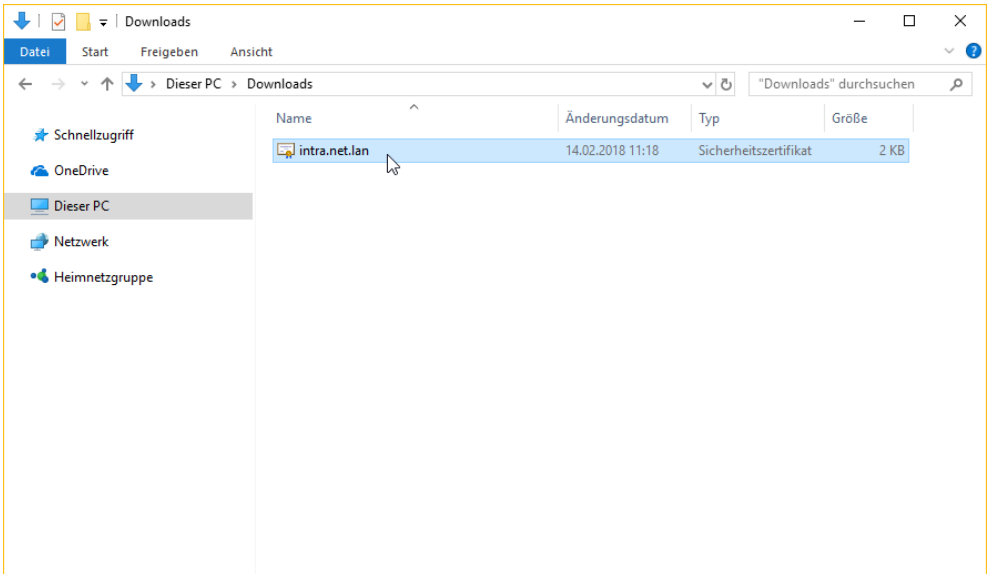
1. Öffnen Sie die Weboberfläche des Intra2net Systems. Dabei müssen Sie unter Umständen das (noch) nicht vertrauenswürdige Zertifikat temporär akzeptieren und die Verbindung dennoch öffnen.

2. Öffnen Sie das Menü System > Weboberfläche > Sicherheit und klicken auf das Lupen-Symbol hinter der Option "SSL Serverschlüssel (lokale Verbindungen)".

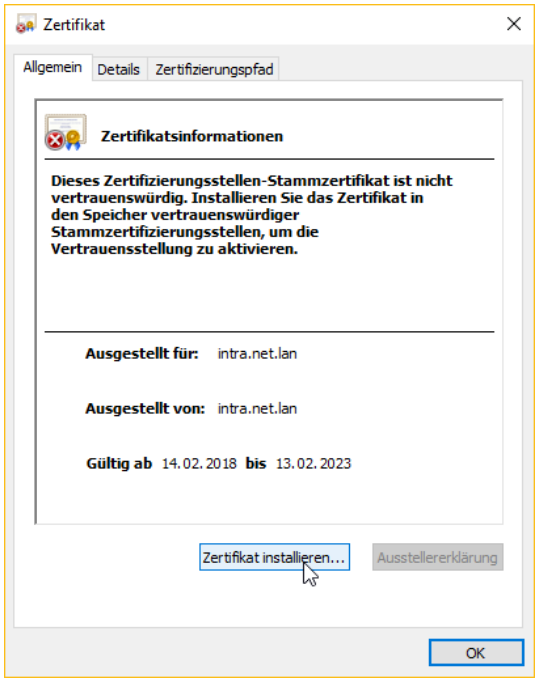
3. Exportieren Sie das Zertifikat "als .cer" und speichern es als Datei.



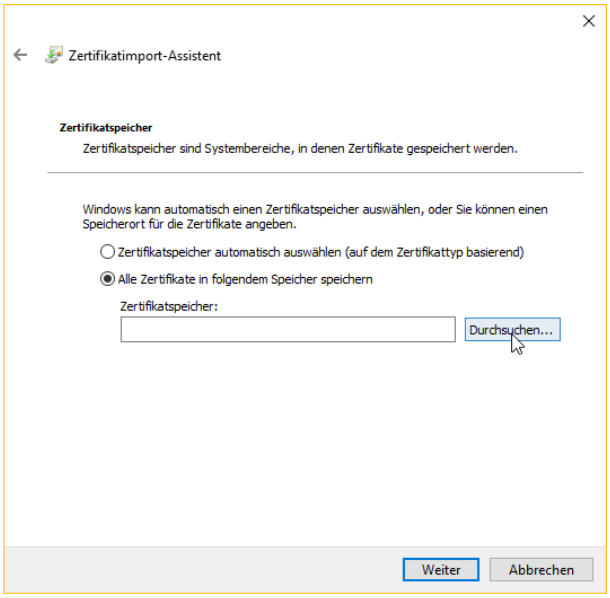
4. Öffnen Sie die eben exportierte Datei über den Windows Explorer mit einem Doppelklick.



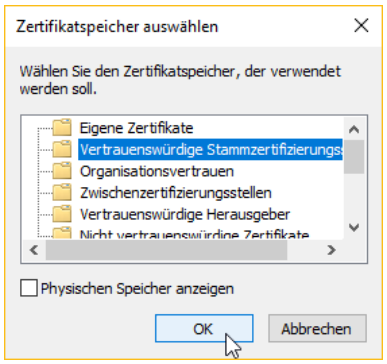
5. Klicken Sie in der Zertifikatsanzeige auf "Zertifikat installieren". Ist diese Schaltfläche nicht vorhanden, so fehlen die nötigen Administrationsrechte.



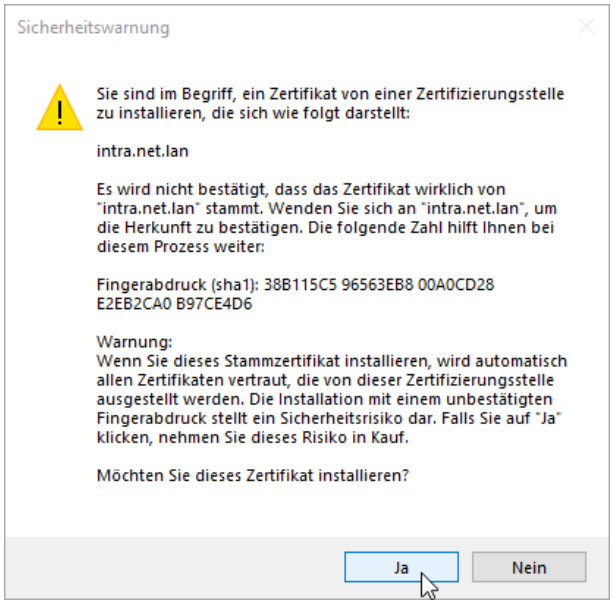
6. Es öffnet sich ein Assistent zum Zertifikatsimport. Lassen Sie das Zertifikat in einem ausgewählten Speicher speichern und klicken auf "Durchsuchen..." zur Auswahl des Zertifikatsspeichers.



7. Wählen Sie den Zertifikatsspeicher "Vertrauenswürdige Stammzertifizierungsstellen".



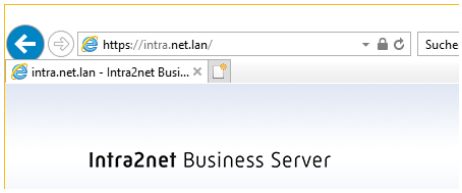
8. Schließen Sie den Assistent ab. Sie bekommen eine Sicherheitswarnung vom Betriebssystem angezeigt. Bestätigen Sie, dass Sie das Zertifikat installieren möchten.



9. Schließen Sie den Internet Explorer.

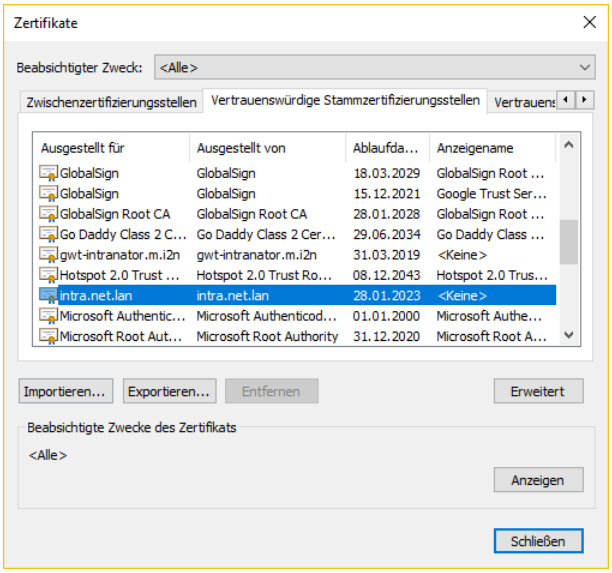
10. Öffnen Sie den Internet Explorer erneut, diesmal nicht mit Administratorrechten, sondern mit normalen Benutzerrechten.

11. Öffnen Sie wieder die Oberfläche des Intra2net Systems. 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 Intra2net Systems 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: `HKCU\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 Intra2net Systems an alle zu verteilen.

Exportieren Sie dazu das verwendete Zertifikat aus dem Intra2net System über das Menü System > Schlüssel > Eigene Schlüssel als .cer-Datei.

Befolgen Sie dann die Hinweise von Microsoft zur Verteilung des Zertifikats: https://docs.microsoft.com/de-de/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy

Verteilen Sie das Zertifikat als vertrauenswürdige Stammzertifizierungsstelle.

Durch die dort beschriebenen Schritte wird eine Gruppenrichtlinie erstellt. Weisen Sie diese dann den Benutzern und Computern im lokalen Netz zu.

Nach dem Bereitstellen der Gruppenrichtline dauert es normal bis zu 2 Stunden bis diese bei den Client-PCs automatisch aktiv wird. Über den Befehl gpupdate /force kann man auf einem Client-PC die sofortige Aktualisierung starten. Wenige Minuten danach sollte dort das Zertifikat im Zertifikatsspeicher vorhanden sein.

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 Intra2net 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. intra.net.lan) oder IP-Adressen zu nutzen.

Zur Auswahl stehen klassische, kommerzielle Zertifizierungsstellen, bei denen die Beantragung, Prüfung und Ausgabe des Zertifikats über die Webseite des Anbieters stattfindet und für die ein geringer Betrag pro Jahr Gültigkeit fällig wird.

Alternativ bietet der Anbieter Let's Encrypt [https://letsencrypt.org/] Zertifikate an, die über das ACME-Protokoll vollautomatisch und kostenlos ausgestellt und verlängert werden. Vor allem wegen der einfacheren Bedienung und automatischen Verlängerung empfehlen wir Let's Encrypt.

10.5.1. Zertifikate von Let's Encrypt

Gehen Sie wie folgt vor um ein Zertifikat von Let's Encrypt zu nutzen:

1. Konfigurieren Sie einen DNS-Namen für die externe IP des Intra2net Systems in einer offiziellen Domain die Ihnen gehört (z.B. **`mail.meinedomain.de`**). Dies kann normalerweise beim Webspace-Provider, der die eigene Domain verwaltet, kostenlos und zeitnah eingerichtet werden. Wenn eine dynamische IP verwendet wird, richten Sie statt dessen einen dynamischen DNS-Dienst ein, siehe Abschnitt 11.13, „DynDNS“.

2. Tragen Sie den externen DNS-Namen im Menü "Netzwerk > DNS > Einstellungen" als Rechnername für Verbindungen aus dem Internet ein.

3. Für die Validierung des Zertifikats ist eine eingehende HTTP-Verbindung erforderlich. Wählen Sie daher im Menü "Netzwerk > Provider > Profile : Firewall" eine Firewall-Regelliste aus, die eingehende HTTP-Verbindungen erlaubt. HTTP-Verbindungen werden vom Intra2net System nur angenommen, während eine Zertifikatsvalidierung ansteht. Ansonsten ist der Port geschlossen.

4. Prüfen Sie, wie das Intra2net System 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 Intra2net System 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 80 (http) auf die IP des Intra2net Systems konfiguriert werden.

5. Legen Sie im Menü "System > Schlüssel > Eigene Schlüssel" ein neues, von Let's Encrypt signiertes Zertifikat an. Prüfung und Ausstellung des Zertifikats laufen vollautomatisch ab.

6. Stellen Sie das für Verbindungen aus dem Internet verwendete Zertifikat auf das neue um. Dies können Sie im Menü "System > Weboberfläche > Sicherheit" auswählen.

7. Ob das neue Zertifikat korrekt ausgestellt und installiert ist, können Sie im Menü "System > Diagnose > Externes HTTPS" testen.

Von Let's Encrypt ausgestellte Zertifikate sind nur wenige Wochen gültig und werden vom Intra2net System automatisch rechtzeitig vor Ablauf verlängert. Daher müssen die oben beschriebenen Firewall-Einstellungen und Portforwardings dauerhaft konfiguriert bleiben.

10.5.2. Zertifikate von klassischen Zertifizierungsstellen

Gehen Sie wie folgt vor um ein Zertifikat einer klassischen Zertifizierungsstelle zu nutzen:

1. Konfigurieren Sie einen DNS-Namen für die externe IP des Intra2net Systems in einer offiziellen Domain die Ihnen gehört (z.B. **`mail.meinedomain.de`**). Dies kann normalerweise beim Webspace-Provider, der die eigene Domain verwaltet, kostenlos und zeitnah eingerichtet werden.

2. Erstellen Sie auf dem Intra2net System ein selbstsigniertes 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 [https://www.comodo.com/], DigiCert [https://www.digicert.com/], GlobalSign [https://www.globalsign.com/], Go Daddy [https://www.godaddy.com/ssl/].

   Erfahrungsgemäß sind Zertifikate über Wiederverkäufer günstiger zu beziehen als über die Anbieter direkt. Beispiele für solche Wiederverkäufer sind (alphabetisch) Cheap SSL Shop [https://www.cheapsslshop.com] und GoGetSSL [https://www.gogetssl.com].

4. Kaufen Sie ein Zertifikat über die Webseite der von Ihnen gewählten Zertifizierungsstelle oder des Wiederverkäufers. Es reicht ein einfaches, Domain-validiertes SSL-Zertifikat für eine einzelne Domain bzw. Webseite. Extended Validation (EV), Organisationsvalidierte Zertifikate oder ein Wildcard-Zertifikat sind normalerweise nicht notwendig. Stehen bei der Bestellung verschiedene Servertypen zur Auswahl, so wählen Sie **`Apache (mod_ssl)`**.

5. Im Verlauf der Zertifikatsausstellung werden Sie von der Zertifizierungsstelle aufgefordert, eine Zertifikatsanforderung (*Certificate Request* oder CSR) zu liefern. Diese können Sie aus dem Intra2net System im Menü System > Schlüssel > Eigene Schlüssel : CA exportieren. Achten Sie darauf, dass Sie die Zertifikatsanforderung nicht durch die Zertifizierungsstelle oder dynamisch im Webbrowser erzeugen lassen, sondern laden

Sie unbedingt die vom Intra2net System erzeugte in das System der Zertifizierungsstelle hoch.

6. Sie bekommen von der Zertifizierungsstelle am Ende 2 Dinge: Ein Zertifikat und eine Zertifikatskette (*Certificate Chain*, *CA bundle* oder *Intermediate Certificate* genannt). Beides importieren Sie im Intra2net System im Menü System > Schlüssel > Eigene Schlüssel : CA.

7. Stellen Sie das für Verbindungen aus dem Internet verwendete Zertifikat auf das neue um. Dies können Sie im Menü "System > Weboberfläche > Sicherheit" auswählen.

8. Ob das neue Zertifikat korrekt ausgestellt und installiert ist, können Sie im Menü "System > Diagnose > Externes HTTPS" testen.

10.6. Schlüsselimport

Normalerweise wird ein privater Schlüssel auf dem Intra2net System erzeugt und es gibt keine Möglichkeit ihn zu exportieren. Nur die für den Schlüssel ausgestellten Zertifikate bzw. öffentliche Schlüssel können über das Menü Menü System > Schlüssel > Eigene Schlüssel : CA importiert werden.

Haben Sie jedoch ein fertiges Paar aus privatem und öffentlichen Schlüssel und wollen dieses importieren, so ist das über das Menü System > Schlüssel > Eigene Schlüssel mit der Schaltfläche "Schlüssel importieren" möglich.

Darüber können Sie Schlüsselpaare entweder per Cut&Paste im PEM-Format importieren, dabei darf der private Schlüssel nicht passwortgeschützt sein. Oder Sie können das Schlüsselpaar als PKCS#12-Datei importieren. Hierbei müssen Sie das zum Schutz der Datei gewählte Passwort eingeben.

Achten Sie vor dem Import eines Schlüsselpaars unbedingt darauf, wo es erstellt wurde und ob diese Quelle und der Transportweg voll vertrauenswürdig sind. Jeder, der den privaten Schlüssel kennt, kann die mit diesem Schlüssel übertragenen Daten lesbar machen. Lassen Sie auf keinen Fall eine externe Zertifizierungsstelle Schlüsselpaare erzeugen, erzeugen Sie die Schlüssel statt dessen immer lokal und senden nur die Zertifikatsanforderung an die externe Zertifizierungsstelle. Lassen Sie Schlüsselpaare auch nicht in einem Webbrowser erzeugen, da dies zusätzliche Angriffsmöglichkeiten eröffnet.

10.7. 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.

Das Intra2net System 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:

Normal	Nur Verbindungen mit TLS 1.2 und TLS 1.3 werden akzeptiert. Erzwingt PFS für alle Verbindungen. Dies ist die empfohlene Einstellung für alle Verbindungen.
Kompatibel mit Windows 7	Wie "Normal", nur wird für den IMAP-Dienst auch TLS 1.0 erlaubt. Diese Einstellung ist gedacht um E-Mail-Clients mit Windows 7 anbinden zu können, auf denen TLS 1.2 noch nicht in der Registry freigeschaltet wurde (siehe unten).
Schwach (Windows XP-kompatibel)	Erlaubt schwächere Verschlüsselung und Schlüssel-Austauschverfahren sowie TLS 1.0, um Kompatibilität mit älteren Betriebssystemen wie z.B. Windows XP herzustellen. Diese Einstellung deaktiviert jedoch das als geknackt geltende RC4-Verfahren. Mit neueren Systemen, die diese unterstützen, werden automatisch stärkere Verfahren, inkl. PFS, ausgehandelt.
Sehr schwach (nur für Testzwecke)	Erlaubt Verbindungen mit schwachen und als geknackt geltenden Verschlüsselungsverfahren wie z.B. RC4. Diese Einstellung ist ein Sicherheitsrisiko und sollte nur kurzzeitig zu Testzwecken aktiviert werden.

Perfect Forward Secrecy (PFS): bewirkt, dass die übermittelten Daten auch dann nicht entschlüsselt werden können, wenn zu einem späteren Zeitpunkt der private Schlüssel des Intra2net Systems bekannt werden sollte und eine früher aufgezeichnete Übertragung dann mit Kenntnis des privaten Schlüssels analysiert wird.

Windows 7 und TLS 1.2: Windows 7 unterstützt zwar grundsätzlich TLS 1.2, allerdings ist diese Unterstützung nicht standardmäßig für alle Systembibliotheken freigeschaltet. Dies muss über eine Einstellung in der Registry nachgeholt werden. Die .reg-Datei mit den passenden Einstellungen finden Sie in der Onlinehilfe des Intra2net Systems für das Menü "System > Weboberfläche > Sicherheit" verlinkt. Wenn TLS 1.2 auf allen Windows 7 Clients freigeschaltet wurde, sollte die Verschlüsselungsstärke auf "Normal" umgestellt werden.

11. Kapitel - Internet

Das Intra2net System kann für mehrere Provider konfiguriert werden. Fällt ein Provider aus, so kann vollautomatisch auf einen anderen Provider ausgewichen werden.

11.1. Einwahl mit DSL (PPPoE)

Das Intra2net System unterstützt DSL mit PPPoE wie es z.B. von der Deutschen Telekom eingesetzt wird. In das Intra2net System ist kein DSL-Modem eingebaut, daher muss an eine Netzwerkschnittstelle eines angeschlossen werden und diese auf den Typ „DSL/Router" konfiguriert werden. Es werden DSL-Modems mit Ethernetanschluss unterstützt. Hier finden Sie eine Übersicht über von Intra2net empfohlene VDSL-Modems [https://www.intra2net.com/de/support/vdsl-modems.php].

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. Siehe Abschnitt 11.6, „Router vs. Modem".

Bei VDSL-Anschlüssen, aber auch bei einigen ADSL-Anschlüssen, müssen zur Einwahl die PPPoE-Pakete mit einer VLAN-ID markiert werden. Bei Anschlüssen, die über die Infrastruktur der Deutschen Telekom bereitgestellt werden, ist dies VLAN-ID 7. Diese VLAN-ID muss entweder auf dem Intra2net System oder auf dem DSL-Modem hinterlegt werden, nicht aber auf beiden gleichzeitig.

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.

11.2. Einwahl mit DSL (PPTP)

Das Intra2net System 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.

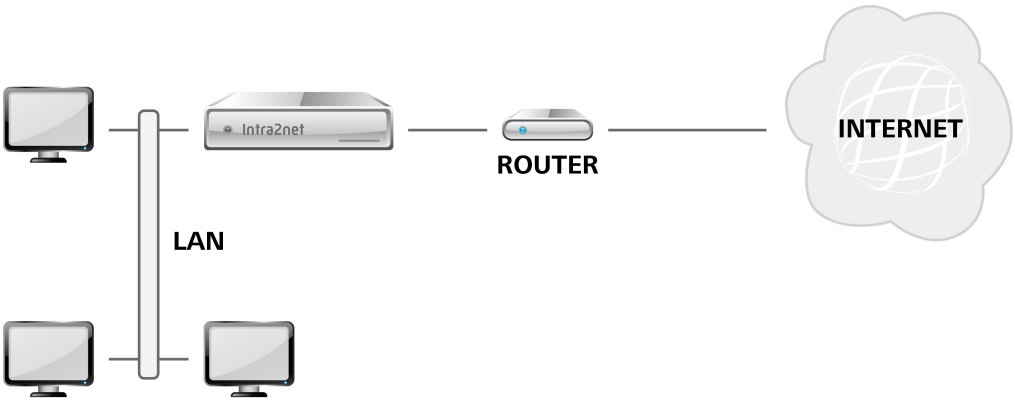
Das DSL-Modem wird wie bei PPPoE über die Ethernetschnittstelle an das Intra2net System angeschlossen.

Bei PPTP-Verbindungen muss zum Aufbau der Verbindung die IP des DSL Modems eingestellt werden. Bei den allermeisten Modems wird hier die 10.0.0.138 verwendet. Manche Provider vergeben diese IP auch per DHCP. Im Intra2net System 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 Konfigurationsdaten.

11.3. Router mit fester IP

Beim Providertyp Router mit fester IP kann an einer auf den Typ „DSL/Router" konfigurierten Netzwerkschnittstelle ein Router angeschlossen werden. Das Intra2net System routet die IP-Pakete dann direkt an diesen weiter.



Geben Sie bei der Konfiguration unter „Lokale IP“ die externe IP des Intra2net Systems 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 9.9, „Routing im Intranet“) überschneiden.

11.4. Router mit DHCP oder Kabelmodem

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 das Intra2net System an das Kabelmodem und nicht an einen Router angeschlossen.

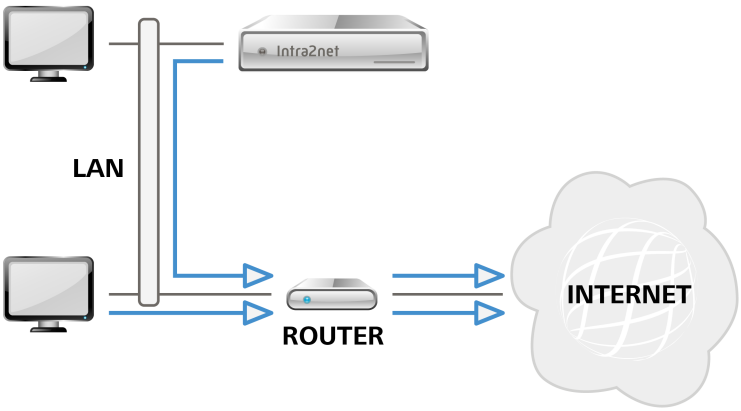


Tipp

Sie müssen das Kabelmodem kurz ausschalten, wenn Sie das Intra2net System das erste Mal anschließen oder die Netzwerkkarte getauscht haben. Dadurch kann es sich auf die MAC-Adresse des Intra2net Systems einstellen.

11.5. Router im lokalen Netz

Soll das Intra2net System 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 das Intra2net System 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.

11.6. Router vs. Modem

Bei den meisten Internetanschlüssen hat man die Wahl zwischen zwei verschiedenen Anschlussvarianten:

1. Ein typischerweise vom Provider gestellter Router übernimmt die eigentliche Einwahl. Das Intra2net System wird dann über die Konfiguration "Router mit fester IP" mit diesem verbunden.

2. Die Leitung ist an ein reines Modem angeschlossen und dieses mit dem Intra2net System verbunden. Das Intra2net System übernimmt die Einwahl.

Die Variante 1. mit dem Router hat den Vorteil schneller eingerichtet zu sein, da der Router meist fertig konfiguriert vom Provider geliefert wird. Wenn dieser Router noch weitere Funktionen integriert, wie z.B. VoIP-Umsetzung, kann es auch sein, dass weniger einzelne Geräte zum Erreichen der gewünschten Funktionen benötigt werden.

Die Variante 1. mit dem Router hat dabei aber auch folgende Nachteile:

- Die eine externe IP wird vom Router selbst belegt. Alle anderen Geräte, wie z.B. das Intra2net System, können nur noch über NAT und Portforwarding kommunizieren.

- Soll von außen auf das Intra2net System zugegeriffen werden können, z.B. für Active-sync, VPN oder E-Mail-Zustellung per SMTP, muss auf dem Router jeweils ein Portfor-warding konfiguriert werden.

- Einige Router haben Schwierigkeiten VPN-Verbindungen korrekt und ohne Störungen weiterzuleiten. Oft kann dies mit einem Firmware-Update des Routers behoben werden, aber nicht in allen Fällen. In einigen Fällen haben wir beobachtet, dass langlebige Ver-bindungen, wie sie bei Site-to-Site-VPNs üblich sind, nicht zuverlässig funktionieren und nach einigen Tagen oder Wochen unterbrochen werden.

- Die wenigsten Router unterstützen den Zugriff auf Portforwarding aus dem lokalen Netz. Das ist notwendig, damit mobile Geräte wie Notebooks aus dem LAN und aus dem Internet für den Zugriff beidesmal den externen DNS-Namen oder die externe IP verwenden können.

Die Variante 2. mit dem separaten Modem hat den Nachteil, dass ein zusätzliches Modem benötigt wird und die Einwahl einmal eingerichtet werden muss. Auch eine evtl. gewünschte VoIP-Umsetzung muss über ein separates Gerät hinter dem Intra2net System gelöst werden.

Dafür haben Sie aber den Vorteil dass für die Dienste des Intra2net Systems, insbesondere das VPN, kein Portforwarding oder NAT benötigt wird. Auch ist der interne Zugriff auf die Dienste an der externen IP problemlos möglich.

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

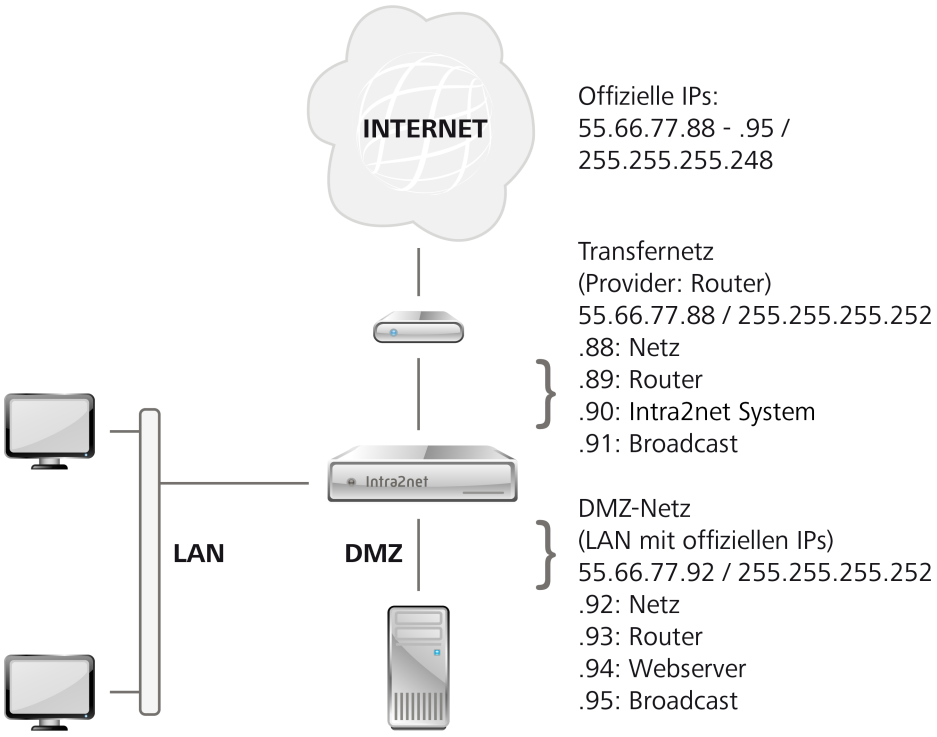
Bitte beachten Sie, dass Sie bei allen Verfahren immer mindestens 8 offizielle IPs benötigen, um (mindestens) einen Server in einer DMZ anbinden zu können.

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 Intra2net System und ein DMZ-Netz. Da pro Subnetz immer zwei IPs für Netzadresse und Broadcast benötigt werden und das Intra2net System in beiden Netzen eine IP benötigt, steht 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 das Intra2net System geroutet wird. Da der Benutzer auf einen vom Provider gestellten Router oft keinen Zugriff hat, muss diese Einstellung der Provider für Sie vornehmen.



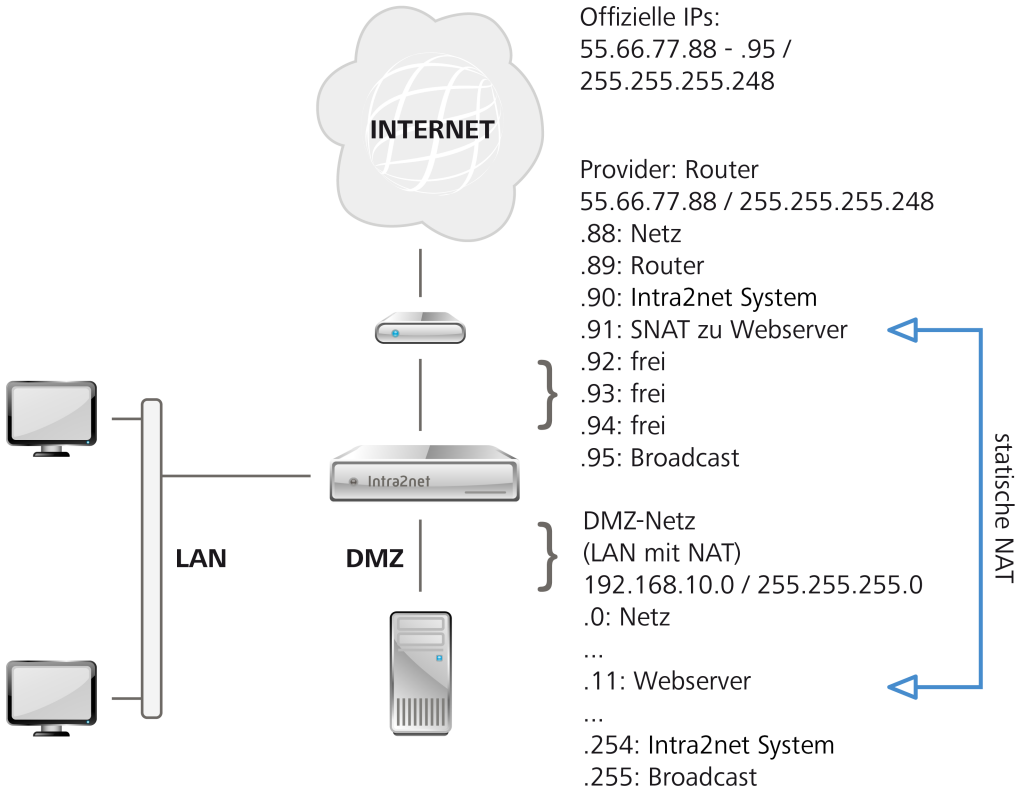
11.7.2. Statische NAT

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 einem 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 öffentlichen IP auf den Server in der DMZ konfiguriert.

Das Intra2net System beantwortet automatisch ARP-Anfragen für die IPs mit Statischer NAT sobald sie im Netz zwischen Router und Intra2net System liegen. Deshalb benötigen Sie auf dem Router keine speziellen Routingeinträge für diese IPs.

Da der Server nur seine IP aus dem LAN - nicht aber seine öffentliche - kennt, funktionieren manche Protokolle nicht, denn einige Protokolle übertragen zusätzlich die verwendete IP im normalen Datenstrom. Bei einigen Protokollen kann das Intra2net System 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 Intra2net System 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 Intra2net System 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. Das Intra2net System geht davon aus, dass alle dort nicht eingetragenen Rechner in dem Netz zwischen Intra2net System und Router liegen.

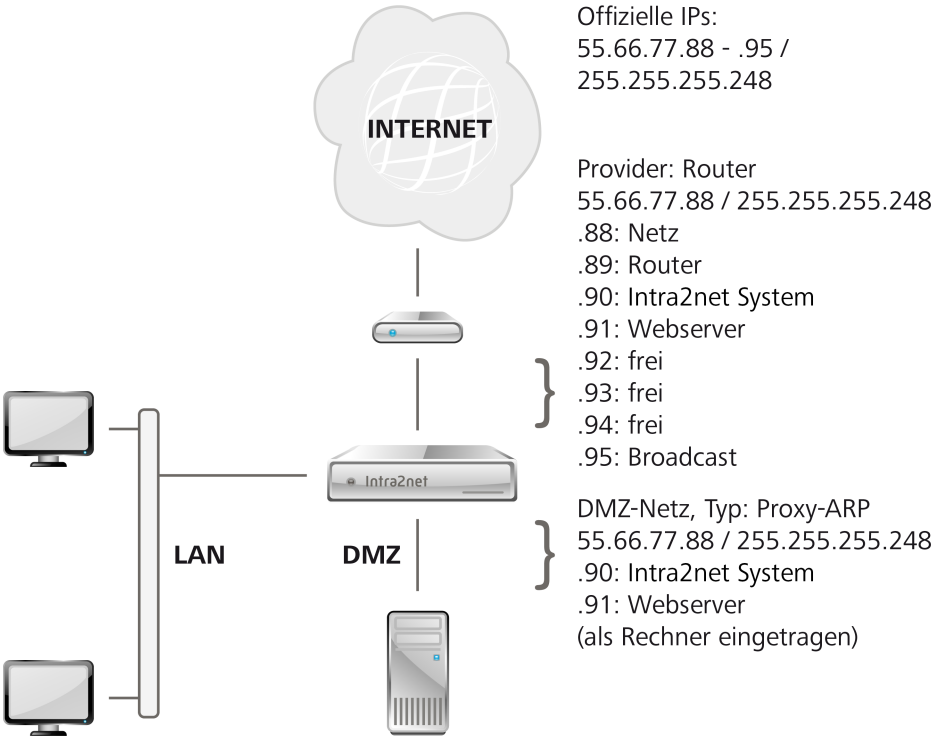
Stellen Sie das Default-Gateway auf dem Server in der DMZ auf das Intra2net System. Das Intra2net System vermittelt jetzt zwischen den beiden Netzteilen, ohne dass die beteiligten Rechner davon etwas mitbekommen. Für die Rechner sieht es so aus, als ob es sich um ein einzelnes, größeres Netz handelt. 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 Intra2net System liegt. Konfigurieren Sie zuerst das Intra2net System, 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 Verbindungsaufbau verwendet wird. Außerdem wird der Modus des Verbindungsaufbaus konfiguriert.

Bei manuellem Verbindungsaufbau geht das Intra2net System nur Online, wenn ein Benutzer auf der Hauptseite auf "Online" klickt oder eine zeitgesteuerte Aktion (z.B. automatischer E-Mail-Transfer) gestartet wird.

Bei Verbindungsaufbau bei Bedarf geht das Intra2net System 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 das Intra2net System auf immer online gestellt, versucht das Intra2net System ständig eine Verbindung offen zu halten.

Bei manuellem und bei Verbindungsaufbau bei Bedarf bleibt das Intra2net System 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 das Intra2net System 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. Verbindungsüberwachung

Die Verbindungsüberwachung wird aktiviert, indem im Reiter "Dienste" eines Providerprofils eine Serverliste für die Verbindungsüberwachung ausgewählt wird. Die Verbindungsüberwachung sendet dann kontinuierlich Ping-Pakete an die in der Serverliste hinterlegten Gegenstellen. Kommt von der Hälfte dieser Server über einen Zeitraum von 90 Sekunden keinerlei Antwort zurück, wird die Leitung als gestört betrachtet und die Verbindung auf Offline gestellt.

Bei Zugangsarten mit Anwahlvorgang wird zuerst versucht die Verbindung erneut aufzubauen. Kann auch dadurch keine stabile Verbindung erreicht werden, wird, sofern konfiguriert, auf einen anderen Provider ausgewichen (Fallback). Bei Zugangsarten ohne Anwahlvorgang wird direkt der Ausweichprovider aktiviert. Zum Ausweichen auf andere Provider siehe Abschnitt 11.10, „Ausweichen auf andere Provider im Fehlerfall (Fallback)“.

Im Menü Netzwerk > Provider > Verbindungsüberwachung können Sie Listen von Gegenstellen hinterlegen, die zur Verbindungsüberwachung per Ping kontaktiert werden. Verwenden Sie für normale Internetverbindungen am besten die von Intra2net vordefinierte Serverliste, da sie breit über das Internet verstreute Server in verschiedenen Rechenzentren enthält und somit ein gutes Bild über den Verbindungszustand gibt.

Wenn Sie eigene Serverlisten definieren, müssen Sie darauf achten, dass die Server auf ICMP Echo-Requests (Ping) antworten. Wir empfehlen in eine Liste mindestens 4, besser 6 bis 8 Server einzutragen, damit der Ausfall eines einzelnen oder einiger weniger Server nicht zu einer Trennung der Verbindung führt.

11.10. Ausweichen auf andere Provider im Fehlerfall (Fallback)

Erkennt das Intra2net System, dass die Verbindung zu einem Provider gestört ist, kann es 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.

11.11. Bandbreitenmanagement und VoIP-Priorisierung

11.11.1. Bandbreitenmanagement

Internetprotokolle wie z.B. TCP sind darauf optimiert, die auf der Strecke zwischen Client und Server vorhandene Bandbreite voll auszulasten um die Daten so schnell wie möglich zu transportieren. Konkurrieren nun z.B. ein größerer Download, bei dem kontinuierlich eine große Menge an Daten zur Übertragung bereitsteht, und eine interaktive Fernwartungssitzung, bei der der Benutzer nur hin und wieder eine Aktion ausführt und damit

nicht ständig Daten zur Übertragung anstehen, miteinander um eine Leitung, so wird der Download die Leitung dominieren, da er konstant Daten überträgt. Die Pakete der Fernwartungssitzung kommen nicht alle im ersten Anlauf durch die Leitung und müssen wiederholt werden, was für der Benutzer als "Ruckeln" wahrnehmbar wird.

Das Bandbreitenmanagement kann durch Regeln dafür sorgen, dass die Pakete von interaktiven Sitzungen nicht durch größere Downloads oder andern Datenverkehr in großen Paketen ausgebremst werden. Dies funktioniert rein anhand der Paketgröße und der Empfangsbestätigungen und ohne dass spezielle Protokolltypen priorisiert werden müssen.

Damit das Bandbreitenmanagement wirksam werden kann, muss es die Verbindungspuffer im Modem oder Router vor dem Intra2net System leer halten und die Pufferung anstehender Datenpakete komplett selbst übernehmen. Dafür ist eine genaue Kenntnis der auf der Leitung von und zum Internet zur Verfügung stehenden Bandbreite notwendig. Gibt das Bandbreitenmanagement mehr Daten ins Internet frei als durch die Leitung passen, wird das Modem oder der Router wieder anfangen zu puffern. Dieser Puffer ist nicht priorisiert, damit wird das Bandbreitenmanagement wirkungslos. Gibt das Bandbreitenmanagement weniger Daten ins Internet frei als durch die Leitung passen, bleibt die zusätzliche Bandbreite ungenutzt.

Die genaue Kenntnis der tatsächlichen Bandbreite ist daher für die Konfiguration des Bandbreitenmanagements entscheidend. Wir empfehlen folgende Vorgehensweise zur Ermittlung der Bandbreite (das Bandbreitenmanagement muss dabei deaktiviert sein):

1. Öffnen Sie die Hauptseite des Intra2net Systems in einem Browserfenster.

2. Bereiten Sie in einem anderen Browserfenster den Download der Installations-CD des Intra2net Systems von https://www.intra2net.com vor, starten ihn aber noch nicht.

3. Bereiten Sie in einem weiteren Browserfenster Downloads von 2 anderen größeren Programmdateien von unterschiedlichen Anbietern (z.B. eine Linux-Live-CD und ein freies Office-Paket) vor, starten sie aber noch nicht.

4. Starten Sie alle 3 Downloads direkt hintereinander.

5. Beobachten Sie die Auslastung der Leitung im Fenster "Eingehend" auf der Hauptseite.

6. Durch kleine Schwankungen der Messzeit und Auswirkungen von Puffern kann es zu Ausreißern in der Auslastung kommen. Ignorieren Sie diese Ausreißer und bilden über einen Zeitraum von vielleicht 30 Sekunden grob den Durchschnitt über die Datenübertragungsrate.

7. Bereiten Sie eine E-Mail an einen externen Empfänger mit einem größeren (z.B. 15 MB) Anhang vor, versenden diese aber noch nicht.

8. Bereiten Sie den Upload einer größeren Datei an einen Cloud-Storage-Dienstleister vor, starten diesen aber noch nicht.

9. Versenden Sie die E-Mail mit dem großen Anhang. Beobachten Sie auf der Hauptseite wie die E-Mail in der Warteschlange landet, überprüft wird und dann versendet wird.

10. Starten Sie den Upload sobald die E-Mail über die Leitung übertragen wird.

11. Beobachten Sie die Auslastung der Leitung im Fenster "Ausgehend" auf der Hauptseite. Bilden Sie den Durchschnitt wie unter Punkt 6.

12. Da bei vielen Internetzugangstechnologien die Übertragungsrate dynamisch an Leitungsstörungen und ähnliches angepasst wird, sollten Sie diese Schritte 3 mal zu unterschiedlichen Tageszeiten wiederholen. Verwenden Sie jeweils die niedrigsten ermittelten Werte für das Bandbreitenmanagement.

Das Bandbreitenmanagement können Sie Im Menü Netzwerk > Provider > Profile : Firewall konfigurieren.

11.11.2. VoIP- und Echtzeitdaten priorisieren

Wenn das Bandbreitenmanagement genutzt wird, kann es auf Wunsch eine weitergehende Priorisierung für Internettelefonie und Verbindungen von Echtzeit-Anwendungen vornehmen. Die betroffenen IP-Pakete werden anhand von DiffServ-Einträgen im Paketkopf erkannt. Das Bandbreitenmanagement reagiert dabei auf die DiffServ-Gruppe Expedited Forwarding (EF). Für diese wird ein DSCP-Wert von 46 / 0x2E verwendet, was dem Eintrag 184 / 0xB8 im ToS-Byte entspricht.

Viele VoIP-Geräte setzen automatisch die DiffServ-Gruppe Expedited Forwarding oder lassen sich entsprechend konfigurieren.

Wir empfehlen VoIP-Geräte nicht mit dem normalen lokalen Netz zu verbinden, sondern für alle VoIP-Geräte und TK-Anlagen ein separates Netz zu konfigurieren und dieses über eine andere Schnittstelle mit dem Intra2net System zu verbinden. Achten Sie darauf, dass für dieses Netz nicht nur andere IP-Adressen verwendet werden, sondern die Netze auf Ethernet-Ebene sauber voneinander getrennt sind. Dies bringt folgende Vorteile:

- VoIP-Gespräche können auch priorisiert werden, wenn sie durch einen VPN-Tunnel laufen, z.B. zu einer anderen Niederlassung. Eine Priorisierung ist hier nur möglich wenn für VoIP ein anderes IP-Netz, und damit ein separater VPN-Tunnel, verwendet wird. Ansonsten würde die Replay-Protection des VPNs eine Veränderung der Paketreihenfolge verhindern.

- Viele Hersteller und Dienstleister von VoIP-Infrastruktur legen nicht die selben hohen Sicherheitsstandards für Sicherheitstests, Patch-Management und langfristige Produktpflege im Vergleich zu sonstigen IT-Produkten an. Auch werden TK-Anlagen wesentlich länger eingesetzt als andere IT-Produkte, was die Pflege für den Hersteller erschwert. Daher sind VoIP-Produkte mit erhöhter Vorsicht einzusetzen. Durch die Abtrennung der VoIP-Geräte in ein separates LAN kann die Firewall den VoIP-Geräten den Zugriff auf das restliche Netz einschränken.

- Große Datentransfers im LAN können die Switch-Infrastruktur auslasten. Wird für VoIP ein getrennter Switch eingesetzt, so bleibt das VoIP davon unbeeinträchtigt.

Eine Alternative zum Einsatz der VoIP-Priorisierung ist die Verwendung eines komplett unabhängigen Internetzugangs rein für VoIP. Damit lässt sich eine noch höhere Dienstqualität erreichen. Gleichzeitig kann ein solcher Anschluss, sofern er über einen anderen Zugangsanbieter realisiert wird, auch beim Ausfall des primären Internetzugangs automatisch als Ersatz dienen (siehe Abschnitt 11.10, „Ausweichen auf andere Provider im Fehlerfall (Fallback)“). Auch bei dieser Variante sollte die oben beschriebene Trennung zwischen LAN und VoIP-Netz umgesetzt werden.

11.12. Masquerading / NAT

Alle lokalen IP Adressen werden beim Internetzugriff maskiert und auf die externe IP des Intra2net Systems 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 Intra2net System vollautomatisch korrigiert:

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

Für die fehlenden (z.B. ICQ oder Gnutella) verfügt das Intra2net System 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.

11.13. DynDNS

Damit das Intra2net System trotz wechselnder IP Adressen z.B. für VPN oder externen HTTPS-Zugriff über das Internet erreichbar bleiben kann, kann das Intra2net System seine IP Adresse über DynDNS-Dienste bekanntgeben. Dabei teilt das Intra2net System seine neue IP nach jeder Einwahl einem DynDNS-Anbieter mit. Über einen normalen DNS-Namen wie z.B. intra.dyndns.org kann man dann auf das Intra2net System unter seiner momentan verwendeten externen IP zugreifen.

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

11.13.1. Anbieter

Folgende DynDNS-Dienste werden momentan vom Intra2net System unterstützt:

Anbieter	Preis	Einstellungen im Intra2net System
No-IP [http://www.no-ip.com/]	Kostenlos (bis 5 Einträge)	• Protokoll: dyndns • Alternativer Server: dynupdate.no-ip.com
Dynu [http://www.dynu.com/]	Kostenlos	• Protokoll: gnudip-fullhostname • Alternativer Server: gnudip.dynu.com
ChangeIP.com [http://www.changeip.com/]	Kostenlos	• Protokoll: dyndns • Alternativer Server: nic.changeip.com
DyNS [http://www.dyns.cx/]	5 US$ einmalig	• Protokoll: dyns
Dyn [http://www.dyn.com/dns/]	25 US$ / Jahr	• Protokoll: dyndns

Anbieter	Preis	Einstellungen im Intra2net System
Namemaster [http://www.dyndnsfree.de/]	12 € / Jahr	• Protokoll: dyndns • Alternativer Server: dynup.de
DHS [http://www.dhs.org/]	5 US$ / Jahr	• 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 Intra2net System kompatibel sind.

11.13.2. 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 Intra2net Systems. 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. Das Intra2net System fragt dann vorher einen Webserver nach der IP, von der die Anfrage kommt, und übermittelt diese dann an den DynDNS-Server.

11.14. Zugriff von außen

Das Intra2net System 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 Firewallregelliste 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 Intra2net Systems als Rechnername (CN) an (siehe auch Abschnitt 10.2, „Zertifikate richtig erstellen“).

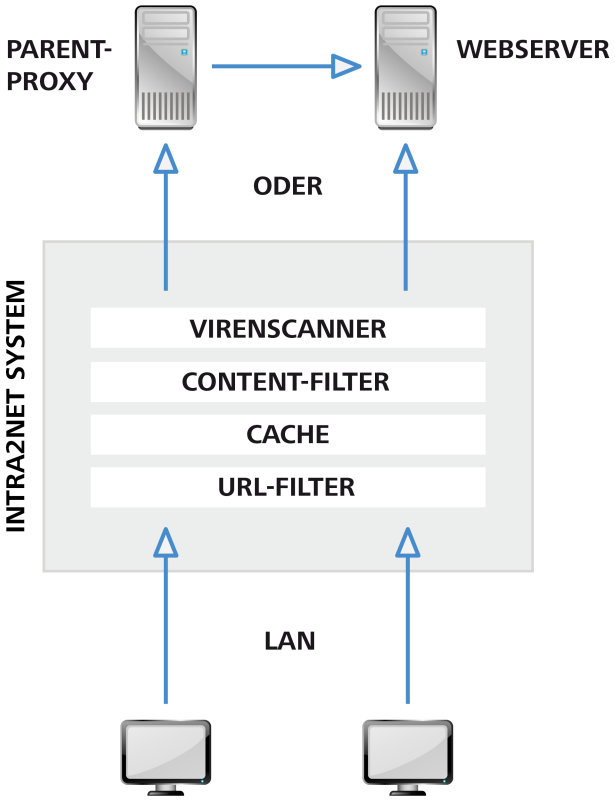
12. Kapitel - Proxy

12.1. Überblick

Das Intra2net System 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 Intra2net Systems 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 das Intra2net System leitet alle HTTP-Zugriffe (transparent für

den Client) auf den Proxy weiter. Der Transparente Proxy funktioniert nicht für HTTPS und FTP. Im Intra2net System 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 das Intra2net System 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 9.3, „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 hizuzufügen.

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.

Die verwendeten Wortlisten enthalten Bewertungen und berechnete Abhängigkeiten der Worte untereinander. Dies macht das Erstellen und Bearbeiten sehr komplex. Daher ist

es nicht möglich die Wortlisten selbst anzupassen. Durch die mehrstufige Architektur des Proxysystems ist es außerdem nicht möglich den Schwellwert oder die Ausnahmeliste abhängig vom Clientrechner oder Benutzer einzustellen.

12.6. Proxy-Virenscanner

Der Proxy-Virenscanner kann alle Daten, die den Proxy passieren, auf Viren untersuchen. Dazu wird zuerst die komplette Datei auf das Intra2net System 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 das Intra2net System 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 Intra2net System.

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

Der Virenscanner bietet die Möglichkeit der Cloud-basierten Virenerkennung. Dabei werden von ausführbaren Dateien Prüfsummen errechnet und an ein Rechenzentrum gesendet. Sind die Prüfsummen dort als bösartig bekannt, wird der Zugriff darauf blockiert. Dadurch wird die Zeit zwischen dem ersten Auftreten eines Virus und der Erkennung deutlich verkürzt. Die Cloud-basierte Virenerkennung sendet aus Gründen des Datenschutz nur Prüfsummen und Dateinamen, nicht aber vollständige Dateien an das Rechenzentrum.

Der Virenscanner kann neben Viren und Trojanern auch Ad- und Spyware erkennen. Sollten solche Programme tatsächlich erwünscht sein, so kann die Erkennung dafür abgeschaltet werden.

Der Virenscanner enthält eine Komponente zur Erkennung von Makroviren mit heuristischen Verfahren. Die Erkennungsrate für die Heuristik kann eingestellt werden. Bei höheren Erkennungsraten werden mehr Makros als Virus erkannt, damit steigt aber auch die Quote von fälschlicherweise als Virus erkannten Dateien.

13. Kapitel - Statistik und Datenschutz

13.1. Proxy-Statistik

13.1.1. Proxy-Protokollierung

Im Menü Information > Statistik > Einstellungen wird konfiguriert, ob der im Intra2net System 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/“ wird in beiden Fällen „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 das Intra2net System 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 das Intra2net System 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 Rechner werden Pakete gezählt, die ins Internet oder auf den Proxyserver des Intra2net Systems gehen. Sollten über den Proxy Webseiten eines Intranet-Servers abgerufen werden, so können diese Zugriffe die Statistik verfälschen. Sollte ein Rechner Daten in einen VPN-Tunnel senden, so wird das unverschlüsselte

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

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

Die Onlinezeit eines Rechners 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. Tachometer

Diese Statistik bietet einen Live-Überblick über den Datenverkehr auf dem System, aufgeschlüsselt nach den Rechnern, von denen die Verbindungen ausgehen.

Für das Tachometer sind die Verbindungen und Datentransfers der letzten sechzig Sekunden ausschlaggebend. Vom in diesem Zeitraum angefallenen Transfervolumen der Rechner wird ein laufender Durchschnitt gebildet. Die Werte für die empfangenen und gesendeten Bytes, sowie deren Summe werden jeweils in einer eigenen Tabellenspalte gelistet. In einer weiteren Spalte wird das ein- und ausgehende Volumen zudem als Balkendiagramm veranschaulicht. Sofern ein Rechner im System mit einem Profil registriert ist oder eindeutig einem definierten Netzbereich oder VPN zugeordnet werden kann, wird der hierfür ermittelte Name angezeigt. Dem System unbekannte Rechner werden als IP-Adresse gezeigt.

Die Datendarstellung gliedert sich in drei Tabellen. In der mit "Interne Rechner" überschriebenen werden Rechner aufgeführt, die aus dem Intranet über das Intra2net System Verbindungen ins Internet oder zum Proxy aufgebaut haben. Unter "Externe Rechner" kann der Datenverkehr zwischen dem Intra2net System und Rechnern im Internet verfolgt werden. Darunter fallen beispielsweise Datenanfragen des Proxyservers und VPN-Verbindungen. Eine dritte Tabelle, "Übersicht", fasst den Traffic in den Kategorien Intern, Extern und Proxy zusammen.

13.3.1. Methodik

Sobald die Tachometer-Seite unter Information > Statistik > Tachometer geöffnet wird, beginnt das System, Daten über IP-Verbindungen zu erheben. Daher dauert es beim Öffnen des Menüs bis zu 10 Sekunden bis Daten angezeigt werden. Diese werden je nach Ursprung in den Tabellen der internen und externen Rechner dargestellt.

Eine Verbindung gilt als *intern*, wenn sie von einem Rechner ausgeht, dessen IP-Adresse einem lokalen Adressbereich zugeordnet werden kann, und die Zieladresse nicht auch lokal ist. Andernfalls gilt sie als *extern*. Diese Unterscheidung ist ausschlaggebend dafür, in welcher Tabelle eine Verbindung angeführt wird.

Die angezeigten Werte für den Datendurchsatz entsprechen dem laufenden Durchschnitt des Datenverkehrs der letzten Minute. Diese Durchschnittswerte werden im Zehnsekundentakt für jeden Rechner neu errechnet. Verbindungen, für welche für mindestens eine Minute kein Traffic registriert wird, gelten als inaktiv und werden nicht länger verfolgt. Rechner ohne aktive Verbindungen werden aus der Statistik entfernt, nachdem die Verbindungsinformationen in die Datenbank der Internetstatistik aufgenommen wurden. Da dies aus Effizienzgründen nicht immer gleich passiert, wenn die letzte Verbindung eines

Rechners ausläuft, kann es dazu kommen, daß Rechner ohne aktive Verbindungen für eine Weile in der Tachometer-Übersicht verbleiben.

Verbindungen werden anhand verschiedener Eigenschaften klassifiziert: ob es sich um externe Verbindungen handelt und ob das Ziel der Verbindung der Proxyserver des Systems ist. Das Datenvolumen, das für diese Traffic-Kategorien insgesamt anfällt, wird auf der Übersichtsseite in einer gesonderten Tabelle zusammengefaßt. Die Werte in dieser Tabelle beziehen sich allein auf die aktiven Verbindungen und müssen nicht notwendigerweise mit der tatsächlichen Bandbreitennutzung des WAN-Uplinks identisch sein. Zum Beispiel fallen bei durch ein VPN geroutetem Datenverkehr mindestens zwei aktive Verbindungen an: Eine für den Tunnel zur Gegenstelle und eine für die darüber transportierten Daten. In der Verbindungsübersicht werden beide Verbindungen erfaßt: Der vom Intra2net System aufgebaute IPsec-Tunnel wird der externen Tabelle zugeschrieben, die eigentliche Verbindung der internen. Durch derartige Überlagerungseffekte kann bisweilen der Eindruck entstehen, daß der in der Zeile „gesamt" angegebene Wert das nominelle Maximum der Anbindung übersteigt. Der tatsächliche ein- und ausgehende Traffic ist im Internettachometer auf der Hauptseite einsehbar.

13.3.2. Seiten

Die Tachometer-Funktionalität ist in drei Ebenen untergliedert. Neben der Hauptseite, die einen Überblick über Rechner bietet, von denen Datenverkehr ausgeht, können Sie sich zu jedem Rechner eine Liste von bestehenden Verbindungen ausgeben und diese in einem weiteren Schritt nach verschiedenen Kriterien einschränken lassen.

13.3.2.1. Rechner

Die Hauptseite des Internettachometers listet Rechner, von denen aktive Verbindungen ausgehen.

Die Daten werden in Spalten angezeigt. Von links nach rechts handelt es sich um:

- Die *laufende Nummer* des Eintrags in der jeweiligen Tabelle;
- die *IP-Adresse* eines Rechners sowie gegebenenfalls der interne Name eines bekannten Rechners, des Netzbereichs oder VPNs;
- die *Durchschnittswerte* für empfangenes und gesendetes Volumen im Erfassungsintervall sowie deren Summe;
- eine Darstellung des ein- und ausgehenden Datenverkehrs als *Balkendiagramm*.

Oberhalb der Tabellen befinden sich auf der Hauptseite zwei Bedienelemente. Über ein Dropdown-Menü kann die Anzahl der angezeigten Rechner erhöht oder reduziert werden. Mittels des Schalters "Zurücksetzen" können Sie die momentan erfaßten Daten verwerfen und die Erfassung von neuem beginnen. Die vom System bereits registrierten Daten werde zuvor in die Statistik-Datenbank übernommen.

13.3.2.2. Verbindungen

Durch Anklicken eines Rechners in der Hauptseite gelangen Sie zu dessen Verbindungstabelle. Diese gibt einen Überblick über die derzeit als aktiv gewerteten Verbindungen, die vom gewählten Rechner aufgebaut wurden. Die verfügbaren Daten werden in neun Spalten präsentiert:

- Die *laufende Nummer* des Eintrags in der jeweiligen Tabelle;
- die *IP-Adresse* des Zielhosts;
- das für die Verbindung verwendete *IP-Protokoll*;
- der *Zielport* sowie gegebenenfalls die Einstufung als Traffic zum Proxy oder der mit diesem Port registrierte Dienst (der tatsächlich verwendete Dienst kann davon selbstverständlich abweichen);
- die *Richtung*, in welche die Verbindung aufgebaut wurde, d. h., ob es sich um eine eingehende, ausgehende, externe oder interne Verbindung handelt;
- die *Durchschnittswerte* für empfangenes und gesendetes Volumen im Erfassungsintervall, sowie deren Summe;
- eine Darstellung des auf der gegebenen Verbindung ein- und ausgehenden Datenverkehrs als *Balkendiagramm*.

13.3.2.3. Filter

Indem Sie auf eines der hinterlegten Elemente in der Verbindungstabelle klicken, können Sie die Verbindungsauswahl eingrenzen. Sie gelangen so zur Filterdarstellung, in welcher nur Verbindungen gezeigt werden, auf die das gewählte Kriterium zutrifft. Als mögliche Kriterien können Sie die IP-Adresse des Zielrechners, das Transportprotokoll, der Zielport sowie die Verbindungsrichtung wählen.

13.3.3. Datenschutz

Aus Datenschutzgründen werden nicht alle erfaßbaren Verbindungsdaten auch in der Trafficverfolgung angezeigt.

13.3.3.1. Passwortschutz

Wenn für das System ein Datenschutzpasswort eingerichtet ist, kann damit unter Information > Datenschutz auch das Internet-Tachometer vor unbefugten Zugriffen geschützt werden. Die Passwortabfrage erfolgt immer dann, wenn die Detailansicht eines Rechners angefordert wird: Die Tachometer-Hauptseite, auf welcher interne und externe Rechners gezeigt werden, ist auch bei aktivem Datenschutzpasswort von Nutzern mit Administratorrechten einsehbar.

13.3.3.2. Adreßverschleierung

Die Zieladressen ausgehender Verbindungen werden vom System ausschließlich in verschleierter Form bereitgestellt. Dasselbe gilt für externen Traffic des Systems zu den Ports von HTTP und HTTPS, die in der Regel auf vom Proxy bediente Anfragen hindeuten. Dieser Mechanismus ist immer aktiv und läßt sich auch durch Eingabe des Datenschutzpassworts nicht umgehen. Konkret bedeutet Verschleierung, daß die unteren sechzehn Bits der IPv4-Adresse des Zielhosts ignoriert werden. In der Weboberfläche werden die ausgeblendeten Felder mit „x" gekennzeichnet. Sinn dieser Maßnahme ist es, die Privatsphäre von Nutzern im Intranet zu wahren und zugleich die für die Diagnose des Datenverkehrs erforderlichen Informationen bereitzustellen.

13.4. 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.

13.5. 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 Gast 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-Warteschlangenzeit 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-Relaying" kann man steuern, ob sich die Mitglieder der Gruppe zum Versand von E-Mails an externe Empfänger am Intra2net System anmelden können (SMTP-Authentifizierung). Beachten Sie, dass die Mitglieder einer Gruppe mit E-Mail-Relaying aus dem Internet unbedingt Passwörter hoher Qualität benötigen. Ansonsten kann das Passwort automatisiert erraten und das Intra2net System 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 33.2.2, „Signaturen anhängen“, die für ActiveSync in Abschnitt 35.3.3, „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 das Intra2net System 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

Das Intra2net System 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 9.3, „Zugriffsrechte eines Netzwerkobjekts“) und die Firewalleinstellungen Zugriff auf den SMTP-Port erlauben, dürfen das Intra2net System zum Senden von E-Mails ins Internet (relayen) ohne weitere Authentifizierung verwenden.

Aus lokalen Netzen ohne das Recht „E-Mail Relaying erlaubt“ und 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 Intra2net Systems 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, das Intra2net System zu nutzen, um von unterwegs aus E-Mails zu versenden. Daher unterstützt das Intra2net System 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 Benutzernamen auf dem Intra2net-System. 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 einige 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.

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 wenn möglich 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 angenommen 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 Intra2net Systems 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 Intra2net Systems zeigen. Um diesen DNS-Eintrag anzulegen, wenden Sie sich an Ihren Webspace- 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.

15.1.6. Auswahl der Versandmethode

Normalerweise werden alle E-Mails mit der selben Versandmethode und -konfiguration versendet. Diese wird im Menü Dienste > E-Mail > Versand im Profil "Standard" ausgewählt. Bei Bedarf können entweder anhand des momentan aktiven Internetproviders oder anhand der Absenderadresse einer E-Mail unterschiedliche Versandmethoden verwendet werden.

Eine vom momentan aktiven Internetprovider abhängige Versandmethode ist vor allem dann sinnvoll, wenn beim primären Provider die E-Mails direkt versendet werden sollen, bei einem Fallback-Provider dies aber z.B. wegen der verwendeten externen IP-Adresse nicht möglich ist.

Legen Sie in diesem Fall unter Dienste > E-Mail > Versand ein neues Profil vom Typ "Provider" an. Unter Netzwerk > Provider > Profile : Dienste können dann bei allen Internetprovidern, die nicht die Standardversandmethode verwenden sollen, diese Profile ausgewählt werden.

Ein von der Absenderadresse einer E-Mail abhängiges Versandprofil ist vor allem dann notwendig, wenn E-Mails über Relayserver versendet werden sollen, aber keiner der in Frage kommenden Relayserver erlaubt, E-Mails mit beliebigen Absenderadressen zu versenden. In diesem Fall können dann mehrere Relayserver oder unterschiedliche Logins

am selben Relayserver passend zu der Absenderdomain oder auch individuellen Absenderadresse gewählt werden.

Legen Sie in diesem Fall unter Dienste > E-Mail > Versand ein neues Profil vom Typ "Absender" an und wählen die passende Absenderadresse oder Absenderdomain.

Beim Typ Absenderdomain müssen die Domains immer vollständig angegeben werden. Subdomains werden nicht automatisch behandelt wie eine darüberliegende Domain, es müssen separate Profile für sie angelegt werden.

Die Priorität der Versandprofile ist wie folgt:

1. Einzelne Absenderadresse

2. Absenderdomain

3. Das dem aktuell aktiven Provider zugewiesene Versandprofil

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

Jeder Benutzer bekommt automatisch einen E-Mail-Account mit seinem Namen auf dem Intra2net System. Es kann per POP3 und IMAP4 auf diesen Account zugegriffen werden, eine Umstellung auf dem Intra2net System ist dafür nicht nötig.

Wir empfehlen für den Transfer der E-Mails vom Intra2net System 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 Smartphone 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. 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 Intra2net System 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.

Das Intra2net System 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

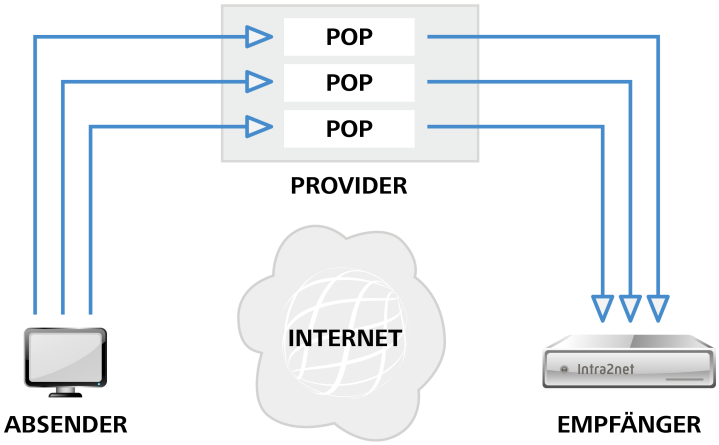
Wir raten bei Verwendung von POP3 dringend davon ab, die Option "E-Mails für *n* Tage auf dem Server belassen" im E-Mail-Client zu aktivieren, denn dem POP3-Protokoll fehlen die für eine zuverlässige Funktion nötigen Operationen. Verwenden Sie statt dessen IMAP.

15.3. E-Mail-Empfang auf dem Intra2net System

15.3.1. Konzepte

Es gibt 3 verschiedene Konzepte, wie eingehende E-Mails auf das Intra2net System kommen können.

15.3.1.1. Abruf einzelner POP-Konten



Bei einem Provider wird für jede E-Mail-Adresse ein eigenes POP-Postfach angelegt. Das Intra2net System holt jedes dieser Postfächer separat ab und stellt den Inhalt an den Empfänger zu.

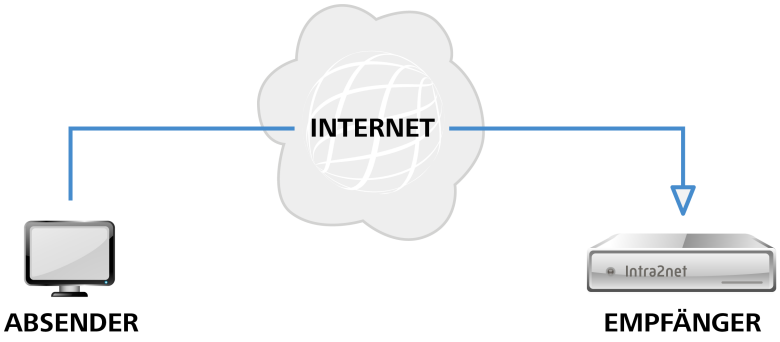
Vorteile:

- 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 Intra2net System.

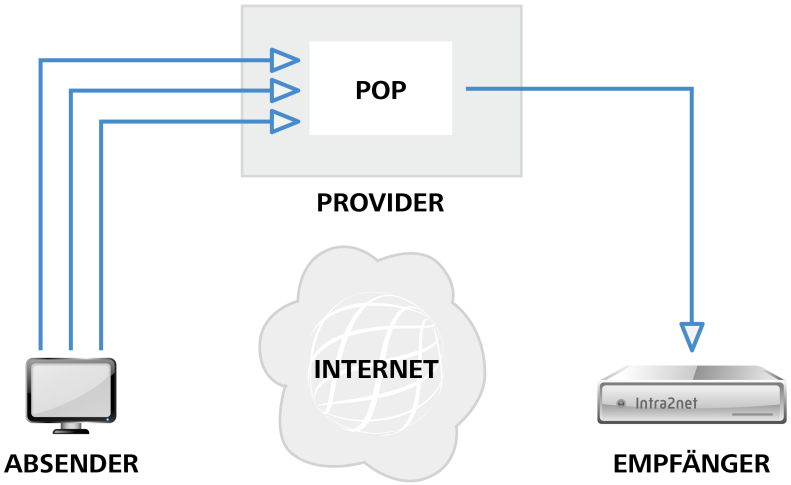
Vorteile:

- 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. Das Intra2net System ruft dieses eine 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 Intra2net System 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 40.3, „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 das Intra2net System 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)

Das Intra2net System 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 Domainkennung. Tragen Sie die Domainkennung in das „Multidrop Header" Feld ein. Beispiele dafür sind „mbox-ihredomain.de-" oder „ihredomain.de-"
Received	Die E-Mail enthält keinen Multidrop-Header. Das Intra2net System versucht, die Empfängeradresse aus den Recieved-Informationen im Header zu ermitteln. Dies kann bei manchen Providern zu Problemen führen. Einige E-Mails werden dann an den Postmaster (siehe Abschnitt 15.12, „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 g3SMO2D10977
    for <gerd@localhost>; Wed, 29 Apr 2015 00:24:02 +0200
Envelope-to: gerd@klickmich.de
Delivery-date: Tue, 28 Apr 2015 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); Wed, 29 Apr 2015 00:24:02 +0200 (CEST)
Received: from [4.43.46.11] (helo=intra.net.lan)
    by mxng00.kundenserver.de with smtp (Exim 3.22 #2)
    id 171uF3-0007Sd-00
    for gerd@klickmich.de; Sun, 28 Apr 2015 21:21:50 +0200
Message-Id: <j60jo.a5626@intra.net.lan>
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 2015 14:47:38 -0000
Received: from moutng1.kundenserver.de (212.227.126.171)
    by pluto.link-m.de with SMTP; 30 Jun 2015 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; Tue, 30 Jun 2015 16:47:37 +0200
Received: from [217.81.153.239] (helo=intra.net.lan)
    by mrelayng1.schlund.de with asmtp (Exim 3.35 #1)
    id 17OfzF-0002Mf-00
    for m.muster@klickmich.de; Tue, 30 Jun 2015 16:47:37 +0200
Received: from storm (storm.net.local [172.16.1.2])
    by intra.net.lan (8.11.6/8.11.6) with SMTP id g5UElmD25862
    for <m.muster@klickmich.de> Tue, 30 Jun 2015 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 Domainkennung „klickmich.de-“. Tragen Sie diese in das „Multidrop-Header“ Feld im Intra2net System 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 Intra2net Systems 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 Intra2net System 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 Intra2net Systems 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 das Intra2net System 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 das Intra2net System zugestellt, kennt das System 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 das Intra2net System 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 das Intra2net System 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 das Intra2net System 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.

Das Intra2net System 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 das Intra2net System automatisch den passenden Distinguished Name.



Achtung

Es wird dringend davon abgeraten, ein Konto mit Administrationsrechten zu verwenden. Das Passwort muss auf dem Intra2net System intern im Klartext abgelegt werden und könnte daher bei einem erfolgreichen Angriff auf das Intra2net System 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.

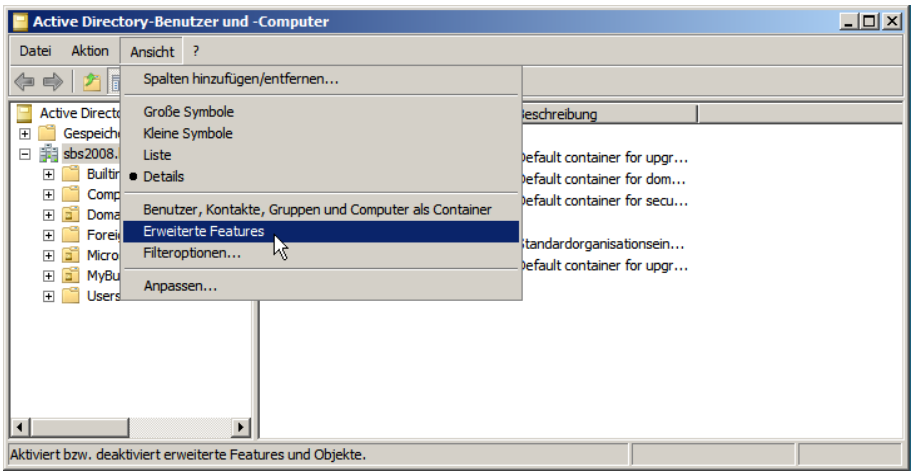
Direkt nachdem die Empfängeradressprüfung konfiguriert wurde, versucht das Intra2net System die Daten per LDAP auszulesen. Dies muss regelmäßig wiederholt werden. Das Intervall dafür wird unter Dienste > E-Mail > Automatik eingestellt.

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.

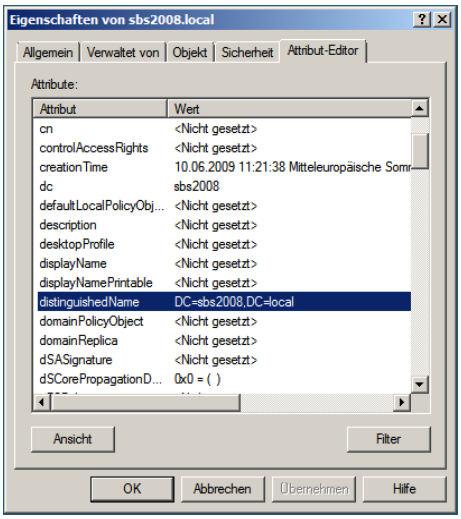
1. Öffnen Sie die Management-Konsole für "Active-Directory-Benutzer und -Computer". Diese finden Sie normalerweise unter "Verwaltung".

2. Aktivieren Sie im Menü "Ansicht" die Option "Erweiterte Features".



3. Klicken Sie mit Rechts auf die Domain und Öffnen den Dialog "Eigenschaften".

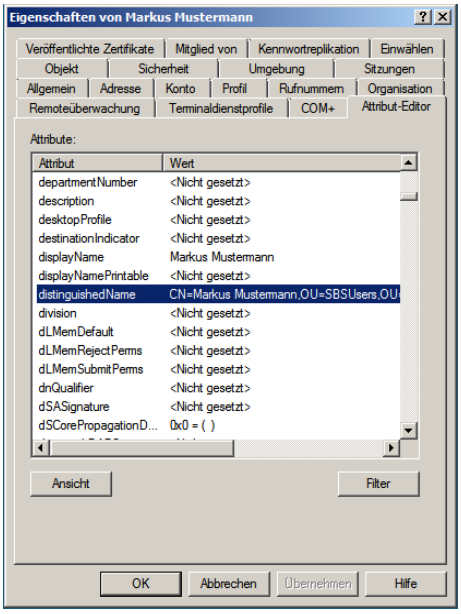
4. Im Reiter "Attribut-Editor" finden Sie das Attribut "distinguishedName". Diesen geben Sie im Intra2net System als LDAP-Suchbasis ein.



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 Intra2net System 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.lan`**).

Unter Dienste > E-Mail > Abholen wählen Sie dann als Empfänger nicht einen lokalen Benutzer des Intra2net Systems aus, sondern tragen eine E-Mail-Adresse in der weiterge-

leiteten 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-Adressierung

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.

Die E-Mail-Kopie kann bei Bedarf mit der Zeitsteuerung der Automatischen Antwort verknüpft werden. Stellen Sie dafür die Weiterleitung auf "während Abwesenheit Kopie an" und konfigurieren unter Benutzermanager > Benutzer : Abwesenheit einen Zeitraum.

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 Abwesenheitsschaltung 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 eingestellen 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) Sortierkriterium 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.

15.6.4. Automatisch Löschen

Unter Benutzermanager > Benutzer : Groupware können Zeiten eingestellt werden, nach denen E-Mails automatisch gelöscht werden.

Zum einen können E-Mails automatisch aus dem Papierkorb gelöscht werden. Diese Option ist standardmäßig beim Anlegen neuer Benutzer aktiv und auf 30 Tage eingestellt.

Zum anderen können E-Mails in allen Ordnern eines Benutzers nach einer einstellbaren Zeit gelöscht werden. Dies ist vor allem zur Umsetzung von Datenschutzvorgaben interessant. Diese Löschung betrifft nur Ordner mit E-Mails, Groupwaredaten werden nicht automatisch gelöscht.

Zur Berechnung des Löschzeitpunkts wird ausschließlich das Empfangsdatum der E-Mail (IMAP INTERNALDATE) verwendet, nicht das vom Absender gesetzte Versanddatum ("Date:"-Kopfzeile) oder der Moment, in dem eine E-Mail in einen neuen Ordner verschoben wurde. Bei von anderen Systemen importierten E-Mails kommt es daher darauf an, dass das Empfangsdatum korrekt mit importiert wurde.

Das Löschen wird automatisch jede Nacht ausgeführt. Direkt nach dem Speichern der Einstellung wird also in der Regel noch nicht sofort mit dem Löschen begonnen.

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

Das Intra2net System 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 Wortbasis 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 das Intra2net System 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 Intra2net System 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 Intra2net System 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 verändern" 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 Intra2net System 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 Postmasteradresse des Intra2net Systems (Menü Dienste > E-Mail > Einstellungen) dort in die Whitelist eintragen. Die Postmasteradresse des Intra2net Systems wird für die Reports als Absenderadresse verwendet.

15.7.1.5. Benutzerabhängiger Spamfilter

Der benutzerabhängige Spamfilter kann für jeden Benutzer auf dem Intra2net System 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 Intra2net System 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.

Das Intra2net System 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): Das Intra2net System 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 Intra2net System gehen. Hier müssen die IPs oder DNS-Namen aller Zwischenserver in die Liste der „weiteren glaubwürdigen Server“ eingetragen werden.

2. Das Intra2net System 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 das Intra2net System oder für die Domain B zuständigen Server weitergeleitet. Das Intra2net System 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: Das Intra2net System 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 notwenig 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. Das Intra2net System 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 das Intra2net System 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. Virenscanner

Unter Dienste > E-Mailfilter > Antivirus kann der E-Mail-Virenscanner aktiviert werden. Ist er aktiviert, werden alle E-Mails, die das Intra2net System 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.

Der Virenscanner bietet die Möglichkeit der Cloud-basierten Virenerkennung. Dabei werden von ausführbaren Dateien Prüfsummen errechnet und an ein Rechenzentrum gesendet. Sind die Prüfsummen dort als bösartig bekannt, wird die E-Mail blockert. Dadurch wird die Zeit zwischen dem ersten Auftreten eines Virus und der Erkennung deutlich verkürzt. Die Cloud-basierte Virenerkennung sendet aus Gründen des Datenschutz nur Prüfsummen und Dateinamen, nicht aber vollständige Dateien an das Rechenzentrum.

Der Virenscanner kann neben Viren und Trojanern auch Ad- und Spyware erkennen. Sollten solche Programme tatsächlich erwünscht sein, so kann die Erkennung dafür abgeschaltet werden.

Der Virenscanner enthält eine Komponente zur Erkennung von Makroviren mit heuristischen Verfahren. Die Erkennungsrate für die Heuristik kann eingestellt werden. Bei höheren Erkennungsraten werden mehr Makros als Virus erkannt, damit steigt aber auch die Quote von fälschlicherweise als Virus erkannten Dateien.

15.7.3. Anhangfilter

E-Mail-Anhänge können neue, dem Virenscanner bisher unbekannte Viren enthalten. Diese müssen aber als ausführbare Dateien auf den PC gelangen bevor sie Schaden anrichten können. Das Intra2net System kann daher E-Mail-Anhänge untersuchen und bestimmte Dateitypen 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 und RAR, aber auch PDF, werden entpackt und durchsucht.

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.

15.7.3.1. Verschlüsselte Anhänge

Verschlüsselte (mit einem Passwort geschützte) Archive können vom Anhangfilter nicht untersucht werden. In der Praxis sind öfters Viren zu beobachten, die in verschlüsselten Archiven verschickt werden und deren Passwort dann im Text der E-Mail oder einem angehängten Bild enthalten ist. Normalerweise wird daher empfohlen, verschlüsselte Archive herauszufiltern.

In einigen Unternehmen wird ein signifikanter Anteil der Kommunikation mit verschlüsselten PDF-Dateien abgewickelt. Für diesen Fall gibt es die Möglichkeit, für verschlüsselte PDFs Ausnahmen zu definieren. Diese gelten immer nur für bestimmte, im entsprechenden Feld hinterlegte Absenderadressen. Da die Absenderadresse von E-Mails beliebig gefälscht werden kann und in der Praxis beobachtet wurde, dass auf infizierten Systemen von Geschäftspartnern etc. durch die Angreifer die E-Mail-Programme systematisch nach untereinander kommunizierenden E-Mail-Adressen ausgelesen werden, wird davon abgeraten, verschlüsselte Anhänge komplett ungefiltert durchzulassen.

Der Empfänger sollte E-Mails mit verschlüsselten Anhängen immer darauf überprüfen, dass das verwendete Passwort nicht in der E-Mail selbst enthalten oder verlinkt ist, sondern mit diesem Kommunikationspartner vorher über einen anderen Kanal wie z.B. per Telefon ausgemacht wurde. Um den Empfänger auf die Notwendigkeit dieser Prüfung hinzuweisen gibt es den Modus "Hinweis mit Freigabe-Link an den Empfänger". Der Empfänger bekommt dabei statt dem Anhang einen Link, unter dem er die nötigen Prüfungen bestätigen muss und dann den Anhang selbst freigeben kann.



15.7.3.2. Office-Makros

Da auch Office-Dateien ausführbare Bestandteile (Makros, VBA-Script, etc.) enthalten können, besteht auch die Möglichkeit Office-Dateien auf diese untersuchen zu lassen. Mit der Einstellung "nach Filterliste" wird keinerlei spezifische Filterung für Office-Dateien vorgenommen, es gelten rein die Einstellungen wie sie unter "Dateiendungen" vorgenommen wurden. Bei der Einstellung "mit verdächtigen Makros" werden Office-Dateien geöffnet, vorhandene Makros extrahiert und bewertet. Enthält eine Office-Datei Makros, die mehrere typische Kriterien für Malware erfüllen, wird die Datei blockiert. Bei der Einstellung "mit jeglichem Makro" werden alle Office-Dateien gefiltert, sobald sie Makros enthalten.

15.7.3.3. Standard-Filterliste und Gruppen

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.

15.7.3.4. Freigabe

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.

Der Zugriff auf die Quarantäne kann, wie auf jeden anderen Menüpunkt, unter Benutzermanager > Gruppen > Administrationsrechte jeder beliebigen Benutzergruppe erlaubt werden.

15.8. DKIM

15.8.1. Grundlagen

Das zum Transport von E-Mails verwendete SMTP-Protokoll sieht keine Möglichkeit vor, die Absenderadresse einer E-Mail zu verifizieren. Grundsätzlich können also Absenderadressen beliebig gefälscht werden und man kann als Empfänger nicht wissen von wem eine E-Mail wirklich stammt. Dies erleichtert Betrugsversuche, Spam, Phishing und ähnliches.

DKIM wurde entwickelt um prüfen zu können, ob eine E-Mail wirklich vom angegebenen Absender (`From:`-Kopfzeile) stammt. Das Protokoll sieht dabei eine Prüfung auf Domain-Ebene vor, es ist also jeder Absenderdomain selbst überlassen, ob und welche Mechanismen sie vorsieht, um Fälschungen innerhalb der Absenderdomain zu verhindern. Als Empfänger kann man sich daher bei DKIM nur darauf verlassen, dass die Domain stimmt, nicht aber auf die Adresse innerhalb der Domain.

Bei DKIM versieht der E-Mail-Server des Absenders jede versendete E-Mail mit einer digitalen Signatur und fügt diese in eine zusätzliche Kopfzeile ein (`DKIM-Signature:`). Gleichzeitig wird im DNS-Eintrag der Domain der öffentliche Schlüssel, mit dem die Signaturen erstellt werden, publiziert. Jeder Empfänger kann nun prüfen, ob die E-Mail wirklich mit dem richtigen Schlüssel signiert wurde. Dies funktioniert unabhängig vom Server des Absenders. Die E-Mail kann daher über beliebige Server verschickt oder weitergeleitet werden ohne die Prüfung zu beeinträchtigen.

Grundsätzlich kann jeder Absender selbst entscheiden, ob er seine E-Mails mit DKIM signiert oder nicht. Dies erlaubt eine graduelle Einführung. Einige Empfänger oder deren E-Mail-Dienstleister haben sich aber entschieden, nicht signierte E-Mails generell abzulehnen. Dies übt Druck auf alle Absender aus, ihre E-Mails auch zu signieren, da sie sonst mit diesen Empfängern nicht mehr per E-Mail kommunizieren können.

15.8.2. Umsetzung

Der Absender entscheidet bei DKIM welche Teile einer E-Mail er signiert und welche nicht. Die Liste der in der Signatur enthaltenen Teile wird dabei zusammen mit der Signatur im `DKIM-Signature:`-Header abgelegt und nicht zentral im DNS gespeichert. Damit ist es möglich, jede E-Mail unterschiedlich zu signieren und z.B. für einige Empfänger eine andere Konfiguration zu verwenden.

Grundsätzlich muss der `From:`-Header immer signiert werden. Es wird aber dringend empfohlen zusätzlich auch `Date:`, `Subject:`, `Reply-To:`, `Sender:`, alle MIME-Header, alle Content-Header und den eigentlichen Inhalt der E-Mail (*Body*) zu signieren. Denn falls einem Angreifer eine E-Mail mit gültiger Signatur in die Hand fallen sollte, kann er alle nicht signierten Teile verändern, ohne dass die Signatur ungültig wird. Eine E-Mail bei der nur `From:` signiert ist, entspäche dann einem Blanko-Scheck und sollte daher vermieden werden. Im Intra2et System stehen mehrere Listen mit zu signierenden Kopfzeilen vordefiniert im Menü "Dienste > E-Mailfilter > DKIM > Headers" zur Verfügung.

Außer der Liste der signierten Teile enthält der `DKIM-Signature:`-Header auch den sog. *Selector*. Der Selector ist der Name des Eintrags des öffentlichen Schlüssels im DNS und kann frei gewählt werden. Anhand des Selectors weiß der Empfänger, woher er den Schlüssel zur Prüfung der Signatur bekommt. Es können mehrere Selectoren für eine Domain gleichzeitig genutzt werden. Dies macht z.B. während einer Umstellung oder bei Nutzung mehrerer E-Mail-Server Sinn.

15.8.3. Weitere Standards

SPF: ist ein alternativer Standard um Absender einer E-Mail zu verifizieren. Dabei wird eine Liste der IP-Adressen im DNS hinterlegt, die E-Mails für eine Domain versenden dürfen. Dies führt aber zu mehreren Problemen:

- E-Mails können nicht mehr normal weitergeleitet werden, da der weiterleitende Server nicht auf der Liste der erlaubten IPs steht. Als Workaround ist das Sender Rewriting Scheme (SRS) vorgesehen, welches das Problem aber nur teilweise löst und neue Probleme mit sich bringt.

- SPF prüft nur den auf SMTP-Ebene übertragenen *Envelope Sender*, nicht den `From:`-Header der vom E-Mail-Programm des Empfängers angezeigt wird. Der *Envelope Sender* ist für den Empfänger nur über Umwege wie z.B. die Quelltext-Anzeige einsehbar.

Intra2net rät auf Grund dieser Nachteile von der Nutzung von SPF ab und empfiehlt DKIM zu verwenden.

DMARC: ist ein Standard, über den der Administrator einer Domain kommunizieren kann, dass alle von dieser Domain legitim versendeten E-Mails mit DKIM signiert sind oder die SPF-Anforderungen erfüllen müssen. Dies kann vom Empfänger genutzt werden, um alle E-Mails, die das nicht erfüllen abzulehnen. DMARC baut daher auf DKIM und/oder SPF auf.

15.8.4. Voraussetzungen zur Nutzung

Ein wichtiger Teil bei der Umsetzung von DKIM ist sicherzustellen, dass Außenstehende nicht in der Lage sind, sich gültige DKIM-Signaturen zu erschleichen. Dies ist vor allem denkbar im Zusammenhang mit E-Mail-Weiterleitungen, Sortierregeln, Verteilern, Webformularen und ähnlichem. Um dies zu verhindern, blockiert das Intra2net System auto-

matisch alle von nicht vertrauenswürdigen Systemen eingehenden E-Mails ohne gültige DKIM-Signatur mit der eigenen Domain als Absender. Dadurch wird auch gleichzeitig die Fälschung der Absenderadresse für die eigene Domain verhindert.

Dies bedeutet aber, dass vor der Einführung von DKIM für alle legitimen E-Mail-Pfade die korrekte Signierung bedacht werden muss. Bedenken Sie hier vor allem externe Nutzer, die direkt auf den E-Mail-Provider zugreifen, Geräte wie Scanner und Drucker im lokalen Netz, E-Mails mit Status- oder Fehlerinformationen von Diensten wie Backupservern, NAS, USVs, Gebäudeautomatisierung und ähnlichem, automatisierte Reports wie z.B. von Arbeitszeiterfassung, Warenwirtschaft, Buchhaltung etc., sowie E-Mails von externen Webservern, wie z.B. Webshop, Kontaktformular und ähnlichem.

Über folgende Wege können E-Mails signiert werden:

- Einlieferung der E-Mail am Intra2net System aus dem lokalen Netz per SMTP, Verschlüsselung der Verbindung mit TLS, Authentifizierung mit einem gültigen Benutzer. Der Benutzer muss Mitglied einer Gruppe sein, die das Recht zur SMTP-Authentifzierung aus dem lokalen Netz hat.

- Einlieferung der E-Mail am Intra2net System aus dem lokalen Netz per SMTP, die IP des SMTP-Clients hat das Recht "E-Mail Relaying erlaubt" (siehe z.B. "Netzwerk > Intranet > Rechner"). TLS und Authentifizierung sind dann optional.

- Einlieferung der E-Mail an einem anderen E-Mail-Server im lokalen Netz. Dieser Server macht zwar selbst keine DKIM-Signierung, leitet ausgehende E-Mails aber an das Intra2net System weiter.

- Einlieferung der E-Mail am Intra2net System aus dem Internet per SMTP, Verschlüsselung der Verbindung mit TLS, Authentifizierung mit einem gültigen Benutzer. Der Benutzer muss Mitglied einer Gruppe sein, die das Recht zur SMTP-Authentifzierung aus dem Internet hat.

- Einlieferung der E-Mail am Intra2net System per Activesync. Der Benutzer muss Mitglied einer Gruppe sein, die das Recht zur Nutzung von Activesync hat.

- Einlieferung der E-Mail an einem anderen Server oder Dienst der auch E-Mails per DKIM signiert. Solche Dienste werden von einigen Webhosting- oder E-Mail-Providern angeboten. Dieser kann einen anderen gültigen DKIM-Selector verwenden als das Intra2net System. Ein solcher Dienst muss zwingend per DKIM signieren, die Nutzung von SPF ist nicht ausreichend, damit die E-Mails vom Intra2net System akzeptiert werden.

Stellen Sie sicher, dass jede E-Mail, die die eigene Domain im Absender verwendet, immer über einen der genannten Wege versendet wird.

15.8.5. Konfiguration

Gehen Sie wie folgt vor um E-Mails mit DKIM zu signieren:

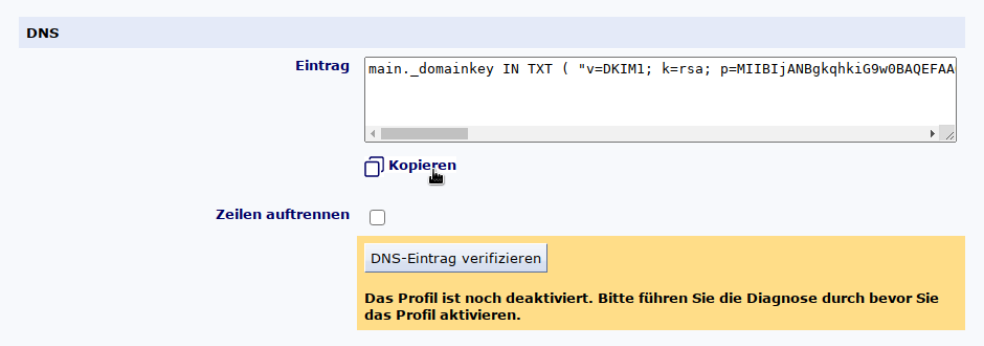
1. Stellen Sie sicher, dass die Voraussetzungen aus Abschnitt 15.8.4, „Voraussetzungen zur Nutzung“ erfülllt sind und prüfen dazu alle legitimen E-Mail-Pfade für die eigene Domain.

2. Legen Sie im Menü "System > Schlüssel > Eigene Schlüssel" einen neuen Schlüssel vom Typ "DKIM" an. Wählen Sie einen beliebigen Namen bei "Selector", beschränken sich aber auf Kleinbuchstaben und verwenden keine Leer- oder Sonderzeichen außer dem

Bindestrich. Als Schlüssellänge wird 2048 Bit als guter Kompromiss zwischen Sicherheit, Rechenzeit und Datengröße im DNS empfohlen.

3. Legen Sie im Menü "Dienste > E-Mailfilter > DKIM > Profile" ein neues Profil an. Wählen Sie die eigene Domain als Absenderdomain aus und verwenden den eben erstellten DKIM-Schlüssel. Als Liste der zu signierenden Header wird empfohlen mit der Standardliste zu beginnen.

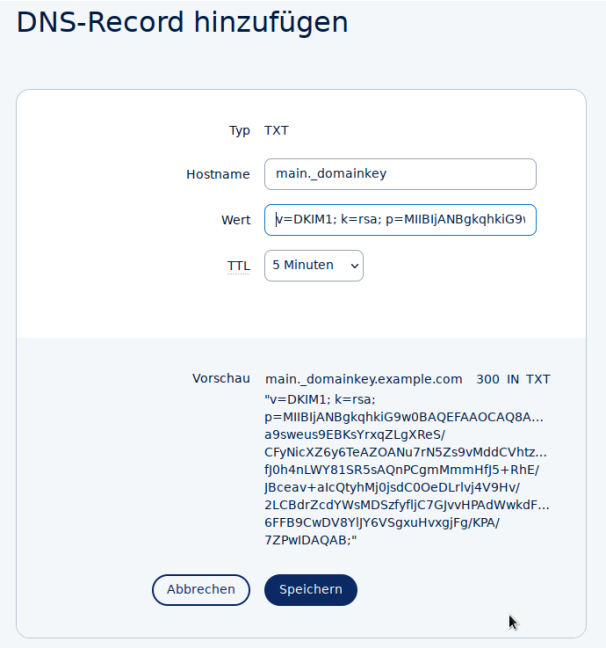
4. Lassen Sie das Profil unbedingt zuerst deaktiviert und speichern die Einstellungen. Nach dem Speichern wird im unteren Bereich des Menüs der nötige DNS-Eintrag für den Selector angezeigt.



5. Gehen Sie in das Verwaltungsportal des für die Domain zuständigen Providers. Meist ist dies der Provider, der auch für das Webhosting zuständig ist. Öffnen Sie dort die DNS-Verwaltung für die gewählte Absenderdomain.

6. Fügen Sie einen neuen Eintrag, Hostname oder Record vom Typ `TXT` hinzu. Der Name für den Eintrag ist dabei der Selector mit `._domainkey` angehängt, so wie es im Menü des Intra2net Systems unter "Eintrag" vorne angezeigt wird.

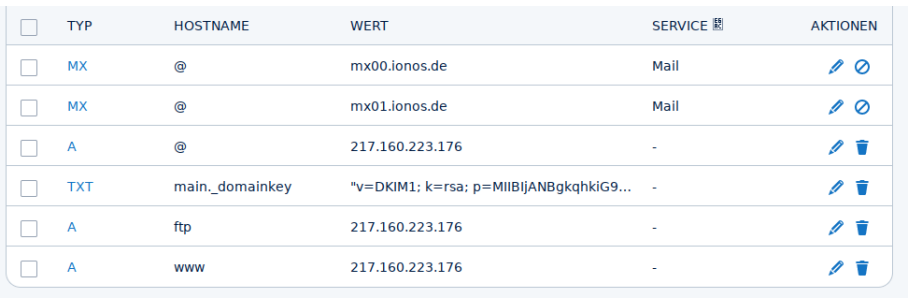
7. Den Inhalt des Eintrags kopieren Sie auch aus der Anzeige des Intra2net Systems. Das genau geforderte Format unterscheidet sich hierbei zwischen den DNS-Providern. Denn der nötige Eintrag ist länger als 255 Zeichen und muss daher nach dem DNS-Standard aufgetrennt werden. Einige DNS-Provider nehmen diese Auftrennung selbst vor, bei anderen muss der Nutzer dies übernehmen. Über die Schaltfläche "Zeilen auftrennen" können Sie sich beide Varianten im Intra2net System anzeigen lassen. Auch ob die Anführungszeichen mit angegeben werden müssen oder nicht unterscheidet sich zwischen den DNS-Providern.



Menü eines DNS-Providers als Beispiel. Die Gestaltung variiert je nach DNS-Provider.

8. Wenn der DNS-Provider Ihnen die Möglichkeit dazu gibt, dann verwenden Sie zuerst eine kurze *TTL* (Time-to-Live, Gültigkeitsdauer) für den DNS-Eintrag aus, z.B. 5 Minuten bzw. 300 Sekunden. Dies ermöglicht Ihnen im Fall eines Konfigurationsfehlers diesen sofort zu korrigieren, ohne zuerst die lange Gültigkeitsdauer des falschen Eintrags abwarten zu müssen.

9. Speichern Sie den neuen DNS-Eintrag in der Oberfläche des DNS-Providers und warten bis der neue Eintrag auf den DNS-Servern publiziert ist. In den meisten Fällen ist dies nach wenigen Minuten abgeschlossen, die genaue Dauer variiert aber je nach DNS-Provider.



10. Klicken Sie im Intra2net System auf "DNS-Eintrag verifizieren" und starten die DKIM-Diagnose. Damit prüft das Intra2net System, ob der DKIM-Eintrag korrekt im DNS abrufbar ist. Im Fall eines Fehlers siehe Abschnitt 15.8.5.1, „Lösen von DKIM-Konfigurationsfehlern“.

11. Wenn die Diagnose erfolgreich durchgelaufen ist, können Sie das neue DKIM-Profil im Menü "Dienste > E-Mailfilter > DKIM > Profile" aktivieren. Ab dann werden alle E-Mails mit der eingestellten Absenderdomain signiert und unsignierte Mails von dieser Domain blockiert wenn Sie nicht von einem vertrauenswürdigen System kommen.

15.8.5.1. Lösen von DKIM-Konfigurationsfehlern

Sollte die Diagnose fehlschlagen, dann prüfen Sie abhängig von der genau angezeigten Fehlermeldung folgende Punkte.

Der DNS-Eintrag wurde nicht gefunden:

- Prüfen Sie als erstes, ob der Eintrag evtl. vom DNS-Provider noch nicht aktualisiert wurde. Abhängig vom DNS-Provider kann dies zwischen wenigen Sekunden bis zu mehreren Stunden dauern. Dies sollte in der Dokumentation oder Verwaltungsoberfläche des DNS-Providers beschrieben sein.

- Kontrollieren Sie als nächstes, ob die Absenderdomain auch lokal genutzt wird oder dorthin eine Weiterleitung besteht. In diesem Fall wird Ihnen der zuständige lokale DNS-Server in der Diagnoseausgabe mit angezeigt. Es empfielt sich den DKIM-Eintrag dann in diesem lokalen DNS-Server zusätzlich zu hinterlegen. Die Diagnose kann aber in diesem Fall ausschließlich den Eintrag im lokalen DNS-Server überprüfen und nicht den für andere im Internet sichtbaren.

- Vergleichen Sie als nächstes die genaue Schreibweise des Eintrags / Hostnamens und den korrekten Typ "TXT" zwischen der Anzeige im Intra2net System und den Daten beim DNS-Provider.

Syntaxfehler oder falscher öffentlicher Schlüssel:

- Vergleichen Sie den Inhalt des DNS-Eintrags zwischen den im Intra2net System angezeigten Daten und denen beim DNS-Provider. Die Daten dort müssen identisch sein. Achten Sie vor allem auf den Anfang und das Ende sowie auf Leerzeichen.

- Wenn die Verwaltungsoberfläche des DNS-Providers mehrere Zeilen vorsieht, dann verwenden Sie Darstellung mit aufgetrennten Zeilen, wenn sie nur eine Zeile vorsieht dann ohne.

- Probieren Sie Anführungszeichen am Anfang und Ende wegzulassen oder hinzuzufügen.

- Evtl. bietet die Verwaltungsoberfläche des DNS-Providers die Möglichkeit zur Diagnose die komplette DNS-Zonendatei anzeigen zu lassen oder herunterzuladen. Dies kann hilfreich sein um Übertragungsfehler zu erkennen. Eine standardkonforme Zonendatei sollte den Eintrag exakt in der Form enthalten, wie sie im Intra2net System mit aktiviertem "Zeilen auftrennen" angezeigt wird.

Beachten Sie, dass wenn Sie einen einmal beim DNS-Provider erstellten Eintrag abrufen und danach dort wieder ändern, der alte Wert normalerweise noch im DNS-Cache für die hinterlegte TTL / Gültigkeitsdauer zwischengespeichert bleibt. Warten Sie daher erst den Ablauf der TTL ab, bevor Sie die Diagnose erneut starten.

Abhängig von den verwendeten DNS-Servern können Sie diese Wartezeit umgehen, indem Sie den DNS-Cache des Intra2net Systems im Menü "Netzwerk > DNS > Einstellungen" leeren. Das ist aber nur möglich wenn das Intra2net System als eigentständiger DNS-Resolver die Root Nameserver befragt und nicht andere DNS-Resolver verwendet.

15.8.6. Filterung und Quarantäne

Nach der Aktivierung von DKIM für eine Absenderdomain muss das Intra2net System alle E-Mails, die vorgeben von dieser Domain zu kommen, aber nicht DKIM-signiert sind oder

von einem vertrauenswürdigen System stammen, blockieren. Dies ist notwendig, um das Erschleichen von Signaturen zu verhindern, siehe Abschnitt 15.8.4, „Voraussetzungen zur Nutzung“.

Auf diese Weise blockierte E-Mails landen standardmäßig in der DKIM/DMARC-Quarantäne. Diese Quarantäne ist unter "Dienste > E-Mailfilter > Quarantäne > DKIM/DMARC" zu finden. Dort können die E-Mails eingesehen, untersucht und fälschlicherweise gefilterte E-Mails wieder freigegeben werden.

Unter "Dienste > E-Mailfilter > Einstellungen" können Sie das Verhalten des Filters steuern. Es wird empfohlen, diese E-Mails für einige Wochen nach Einführung von DKIM zuerst unter Quarantäne stellen zu lassen. Während dieser Zeit kann der Administrator sicherstellen, dass tatsächlich alle E-Mail-Pfade der eigenen Domain korrekt konfiguriert sind, ohne dass E-Mails versehentlich abgelehnt und gelöscht werden. Im Fehlerfall können diese E-Mails dann über einen der in Abschnitt 15.8.4, „Voraussetzungen zur Nutzung“ beschriebenen Wege umgeleitet werden.

Ruft das Intra2net System von außen eingehende E-Mails per POP von einem E-Mail-Provider ab (siehe Menü "Dienste > E-Mail > Abholen"), dann muss die Quarantäne dauerhaft genutzt werden, da die zu blockierenden E-Mails schon durch den E-Mail-Provider angenommen wurden wenn sie am Intra2net System ankommen. Um sie auf SMTP-Ebene abzulehnen ist es dann schon zu spät.

Werden von extern eingehende E-Mails dagegen per SMTP empfangen und zeigt der MX-Eintrag der E-Mail-Domain auf das Intra2net System, dann empfiehlt es sich, nach einer Einführungzeit von einigen Wochen die Aktion für unsignierte E-Mails auf Ablehnen umzustellen. Dann fallen die Benachrichtigungsemails für unter Quarantäne gestellte E-Mails an den Administrator weg.

15.8.7. Headerlisten und Ausnahmen

Unter "Dienste > E-Mailfilter > DKIM > Headers" können Listen mit den zu signierenden E-Mail-Kopfzeilen konfiguriert werden. Normalerweise empfiehlt es sich das vordefinierte Standardprofil zu verwenden, da dort alle relevanten Header enthalten sind und es damit einem potentiellen Angreifer sehr schwer gemacht wird, E-Mails zu verfälschen oder bestehende Signaturen zu missbrauchen.

Allerdings kann es vorkommen, dass ein Server zwischen Absender und bestimmten Empfängern E-Mails legitim verändert und dadurch die Prüfung der DKIM-Signatur dann beim endgültigen Empfänger der E-Mail fehlschlägt. Dies passiert z.B. wenn Kennzeichnungen wie "[extern]" in den Betreff eingefügt werden oder eine Mailingliste genutzt wird, die ihren Namen in den Betreff einfügt oder eine Kurzanleitung zur Nutzung an den E-Mail-Text anhängt. Für diese Fälle bietet das Intra2net System die Möglichkeit für bestimmte Empfänger Ausnahmereglen zu definieren und dort weniger Header zu signieren.

Wählen Sie dafür zuerst unter "Dienste > E-Mailfilter > DKIM > Headers" eine passende Liste von Headern aus oder legen eine neue an. Gehen Sie danach ins Menü "Dienste > E-Mailfilter > DKIM > Profile" und legen ein neues Empfänger-Profil an. Tragen Sie entweder eine gesamte Empfänger-Domain ein oder eine einzelne Empfänger-E-Mail-Adresse. Wählen Sie die gewünschte Header-Liste aus und speichern.

Dann wird für alle E-Mails, die an die eingestellte Empfänger-E-Mail-Adresse oder -Domain gehen sollen und deren Absenderadresse in einer Domains liegt, für die ein DKIM-Profil

aktiv ist, die im Empfänger-Profil hinterlegte Einstellung übernommen. Diese hat also Vorrang vor den Einstellungen für die Absenderdomain.

Da der Absenderserver die Liste der zu signierenden Header frei auswählen kann, ist hierfür keine Änderung im DNS oder dem Selector nötig.

15.8.8. Schlüssel rotieren

Der zu einem DKIM-Selector gehörende Schlüssel kann prinzipiell zeitlich unbegrenzt verwendet werden. In einigen Fällen sollte der Schlüssel aber unverzüglich durch einen neuen ersetzt werden:

- Es wird Missbrauch des Schlüssels durch andere eindeutig erkannt oder vermutet
- Ein Server, auf dem der private Schlüssel gespeichert war, wurde von nicht autorisierten Personen infiltriert oder dies zumindest vermutet
- Ein Mitarbeiter, der Zugriff auf den privaten Schlüssel hatte, hat das Unternehmen verlassen
- Einem Dienstleister, wie z.B. IT-Dienstleiser, Webhosting-Provider oder E-Mail-Provider, bei dem der private Schlüssel gespeichert war, wurde gekündigt

Über diese Ereignisse hinaus empfiehlt es sich die Schlüssel alle 1 bis 5 Jahre zu rotieren, um ein Brechen des Schlüssels mit viel Rechenleistung zu verhindern und die Schlüssellänge an den jeweiligen Stand von Wissenschaft und Technik anzupassen.

Gehen Sie zum Rotieren des Schlüssels wie folgt vor:

1. Legen Sie im Menü "System > Schlüssel > Eigene Schlüssel" einen neuen Schlüssel vom Typ "DKIM" an. Verwenden Sie einen anderen Selector als beim bisherigen Schlüssel.
2. Legen Sie im Menü "Dienste > E-Mailfilter > DKIM > Profile" ein neues Profil an. Tragen Sie die selbe Absenderdomain ein, verwenden Sie den neuen Schlüssel und lassen das neue Profil unbedingt zuerst deaktiviert.
3. Konfigurieren Sie den neuen DNS-Eintrag zusätzlich beim DNS-Provider, lassen dort den bisherigen DNS-Eintrag bestehen und starten danach die DKIM-Diagnose. Siehe Abschnitt 15.8.5, „Konfiguration“ für eine detaillierte Beschreibung.
4. Wenn die Diagnose erfolgreich war, aktivieren Sie die Warteschlange im Menü "System > Warteschlange".
5. Deaktivieren Sie das bisherige DKIM-Profil und aktivieren das neue. Lassen Sie das bisherige Profil weiterhin bestehen und löschen es noch nicht. Beide Änderungen werden zuerst in der Warteschlange vorgemerkt und noch nicht sofort wirksam.
6. Führen Sie jetzt die Warteschlange aus, um nahtlos vom alten auf das neue Profil umzuschalten.
7. Da noch mit dem alten Profil signierte E-Mails unterwegs sein können und später vom Empfänger geprüft werden können müssen, muss das Profil und der zugehörige DNS-Eintrag weiterhin bestehen bleiben. Im Menü "Dienste > E-Mailfilter > DKIM > Profile" wird das frühestmögliche Löschdatum angezeigt.

15.9. Archivierung

15.9.1. Schnittstelle

Im Menü "Dienste > E-Mail > Archivierung" kann die Archivierungsschnittstelle des Intra2net Systems 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 `X-Envelope-To` abgelegt.
POP3-Sammelpostfach (MailStore)	Von jeder E-Mail wird eine Kopie in einem speziellen Sammelpostfach abgelegt, aus dem eine Archivierungs-Software sie per POP3 abholen kann. Bei E-Mails mit mehreren Empfängern wird für jeden Empfänger eine separate E-Mail im Sammelpostfach abgelegt. Der Absender wird in der Kopfzeile `X-Envelope-From`, der Empfänger in der Kopfzeile `X-Envelope-To` 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 `RCPT-TO`-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 `X-Envelope-From`, der Empfänger in der Kopfzeile `X-Envelope-To` abgelegt.
MailStore Proxy	Die einzelnen E-Mails werden in Dateien kompatibel zum Format des MailStore Proxys abgelegt. Damit kann das Intra2net System wie ein MailStore Proxy an den MailStore Server angebunden werden. Hinweise zur Einrichtung finden Sie in Abschnitt 15.9.2, „Anbindung des MailStore Servers“.

Ist der Spamfilter des Intra2net Systems 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.

15.9.2. Anbindung des MailStore Servers

Der MailStore Server [https://www.mailstore.com/] kann genutzt werden, um alle E-Mails zu archivieren, die durch das Intra2net-System geleitet werden. Zu diesem Zweck gibt es zwei Archivierungsarten: Per Sammelpostfach oder per Mailstore-Proxy. Da die Mailstore Proxy Schnittstelle seitens Mailstore abgekündigt wurde, wird die Anbindung per POP3-Sammelpostfach empfohlen.

15.9.2.1. Anbindung des MailStore Servers per POP3-Sammelpostfach

Der MailStore Server [https://www.mailstore.com/] wird über ein separates POP3-Sammelpostfach im Intra2net System angebunden. Dabei wird von jeder E-Mail, die durch das Intra2net System läuft, eine Kopie in dem POP3-Sammelpostfach angelegt. Der Mailstore Server ruft dieses Sammelpostfach regelmäßig ab und archiviert die E-Mails. Das Zusatzprogramm "Mailstore Gateway" wird nicht benötigt.

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:

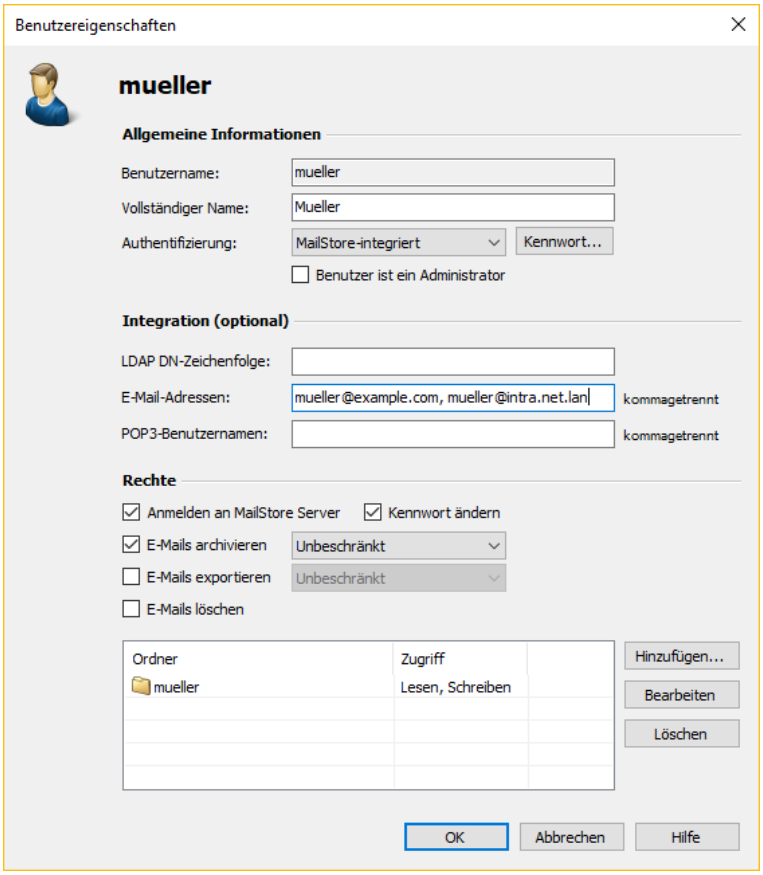
1. Installieren Sie den MailStore Server wie im Handbuch des Herstellers beschrieben: http://de.help.mailstore.com/.

2. Stellen Sie den Archivierungsmodus des Intra2net Systems im Menü "Dienste > E-Mail > Archivierung" auf "POP3-Sammelpostfach (MailStore)" und legen ein Passwort für das Archivpostfach an.

   Notieren Sie sich den Login (z.B. **`mailarchive`**).

3. Öffnen Sie den MailStore Client, loggen sich mit Administrationsrechten ein und öffnen das Menü "Verwaltung".

4. 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.

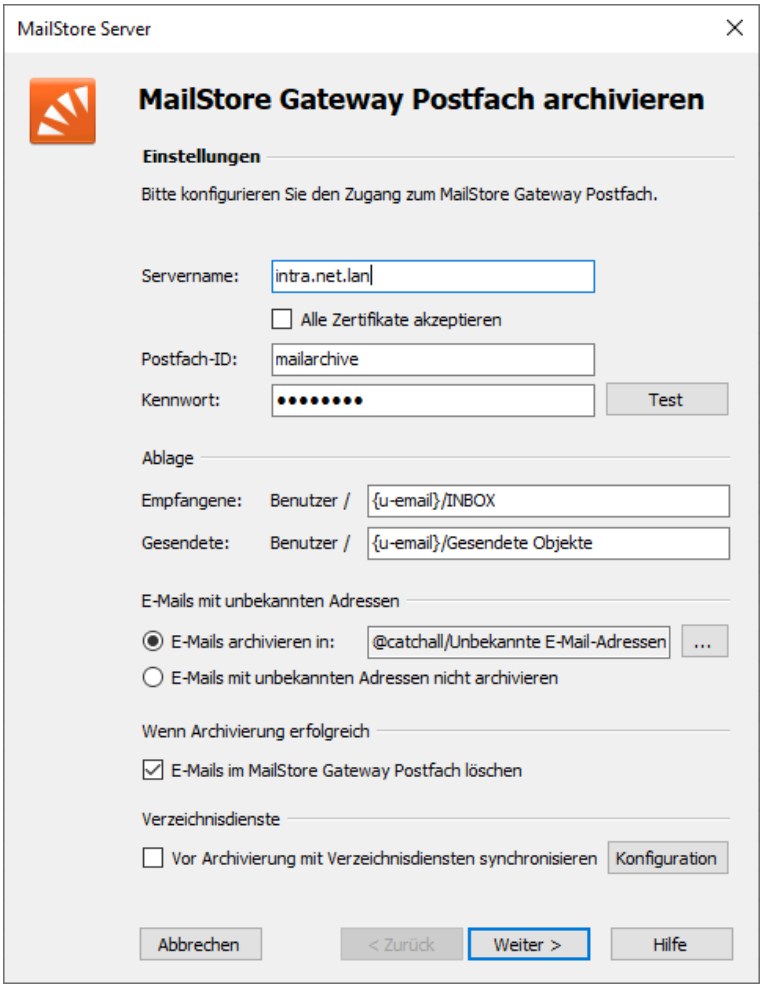


5. Wählen Sie im Menü "E-Mails archivieren" den Punkt "E-Mail-Server" und anschließend die Option "Mailstore Gateway Postfach".

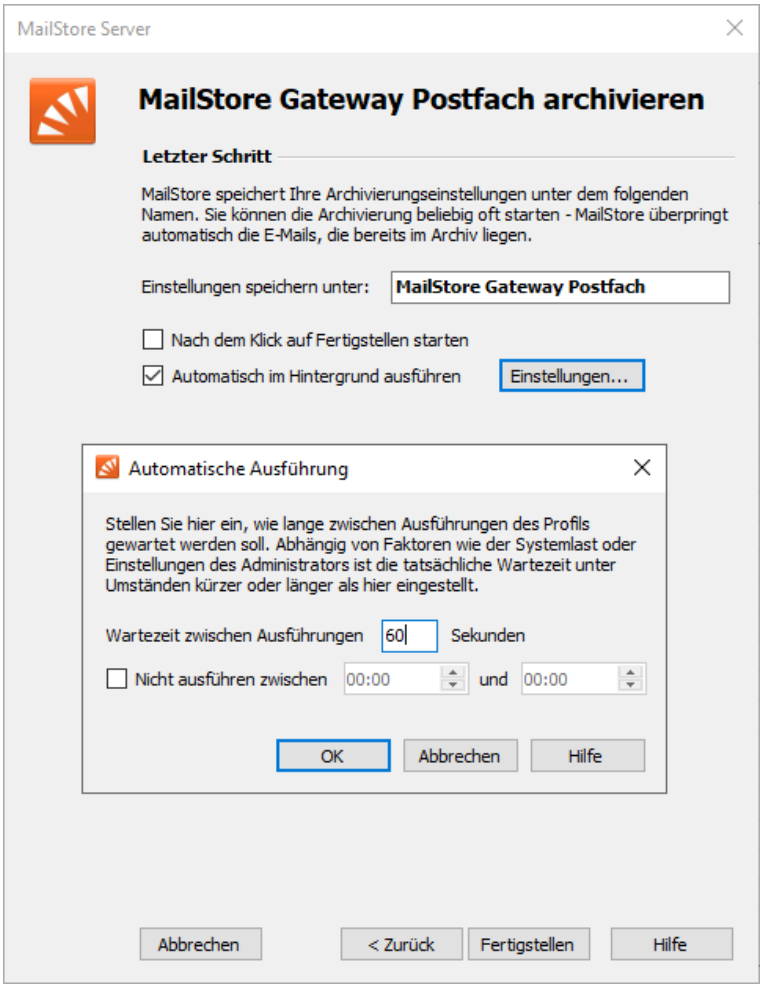
6. Wählen Sie die Option "Anderer E-Mail Server".

7. Geben Sie den Servernamen und das vergebene Kennwort ein. Als Postfach-ID verwenden Sie den unter 2. im Intra2net-System aufgeführten Login (z.B. **`mailarchive`**).

   Lassen Sie die E-Mails im Gateway Postfach löschen, wenn die Archivierung erfolgreich war (wichtig!).



8. Lassen Sie das Profil automatisch alle **60** Sekunden im Hintergrund ausführen.



9. Speichern Sie die Konfiguration.

15.9.2.2. Anbindung des MailStore Servers über die Proxy-Schnittstelle

Die Anbindung des Mailstore Servers über die Proxy Schnittstelle wurde abgekündigt. Wir empfehlen stattdessen Abschnitt 15.9.2.1, „Anbindung des MailStore Servers per POP3-Sammelpostfach“.

Der MailStore Server [https://www.mailstore.com/] wird über die im Intra2net System vorhandene MailStore Proxy Schnittstelle angebunden. Dabei wird von jeder E-Mail, die durch das Intra2net System geleitet wird, eine Kopie angelegt und in einem speziellen Format an der Archivschnittstelle des Intra2net Systems 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.

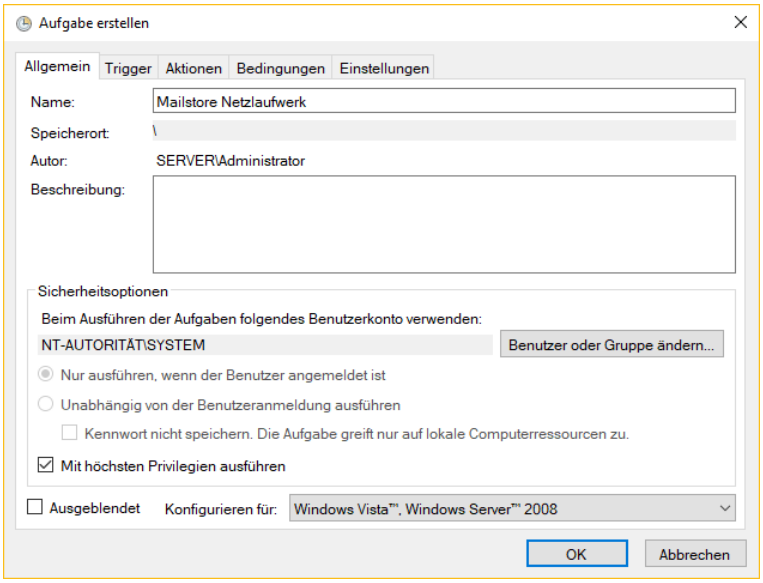
Gehen Sie bei der Installation wie folgt vor:

1. Installieren Sie den MailStore Server wie im Handbuch des Herstellers beschrieben: http://de.help.mailstore.com/.

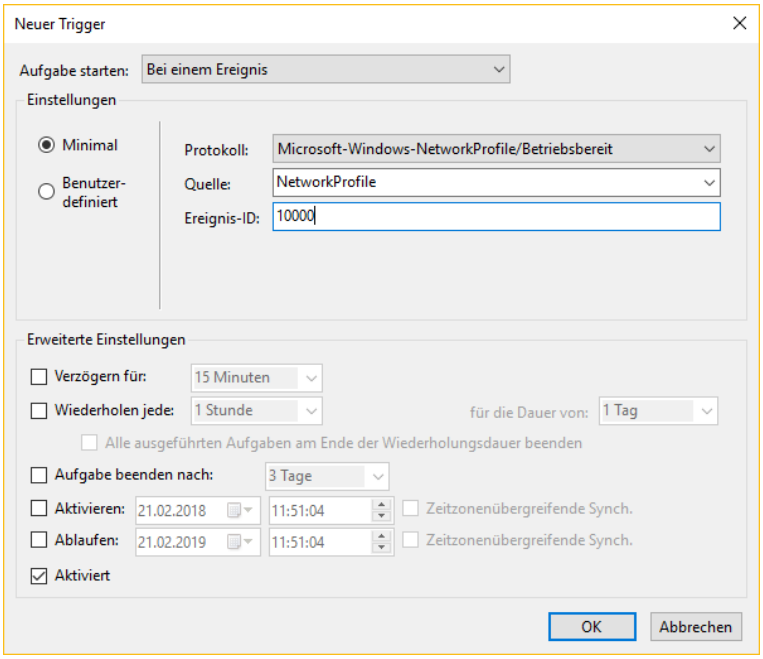
2. Stellen Sie den Archivierungsmodus des Intra2net Systems im Menü Dienste > E-Mail > Archivierung auf "MailStore Proxy" und geben Zugangsdaten für den Freigabepfad an.

3. Öffnen Sie auf dem Rechner mit dem MailStore Server die Windows-Aufgabenplanung aus der Windows-Verwaltung.

4. Legen Sie eine neue Aufgabe an. Lassen Sie die Aufgabe mit dem Benutzerkonto **`SYSTEM`** und mit höchsten Privilegien ausführen.

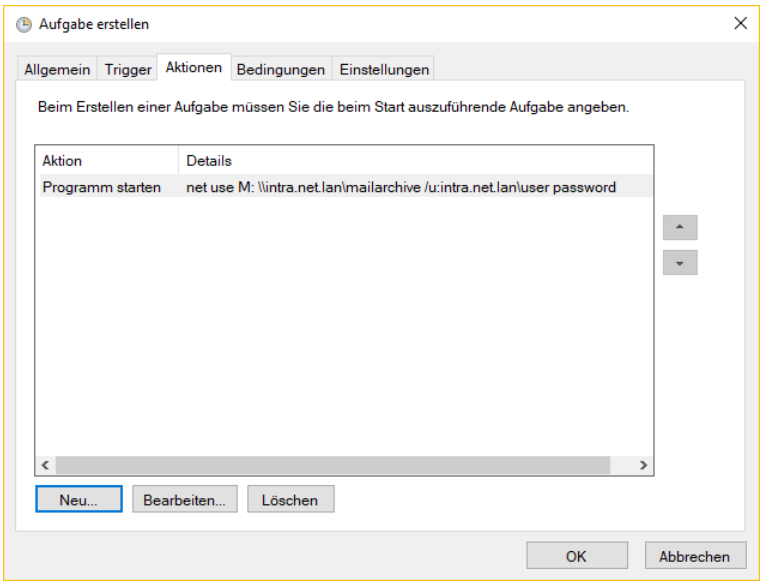


5. Fügen Sie einen neuen Trigger für die Aufgabe hinzu. Lassen Sie die Aufgabe bei einem Ereignis starten und wählen das Protokoll "Microsoft-Windows-NetworkProfile/Betriebsbereit". Die Quelle ist "NetworkProfile" und als Ereignis-ID geben Sie ein **`10000`**. Damit wird die Aufgabe gestartet, sobald das Netzwerksystem funktionsfähig ist.



6. Fügen Sie eine neue Aktion hinzu. Lassen Sie das Programm **`net`** starten und geben ihm als Argumente **`use M: \\intra.net.lan\mailarchive /u:intra.net.lan\user password`** mit. Verwenden Sie dabei den Namen Ihres Intra2net Systems und die von

Ihnen gewählten Zugangsdaten an Stelle von "user" und "password". Sollte der Laufwerksbuchstabe M: auf Ihrem Rechner schon anderweitig vergeben sein, so verwenden Sie einen anderen. Beachten Sie das Leerzeichen zwischen **`M:`** und **`\\intra.net.lan\...`**.

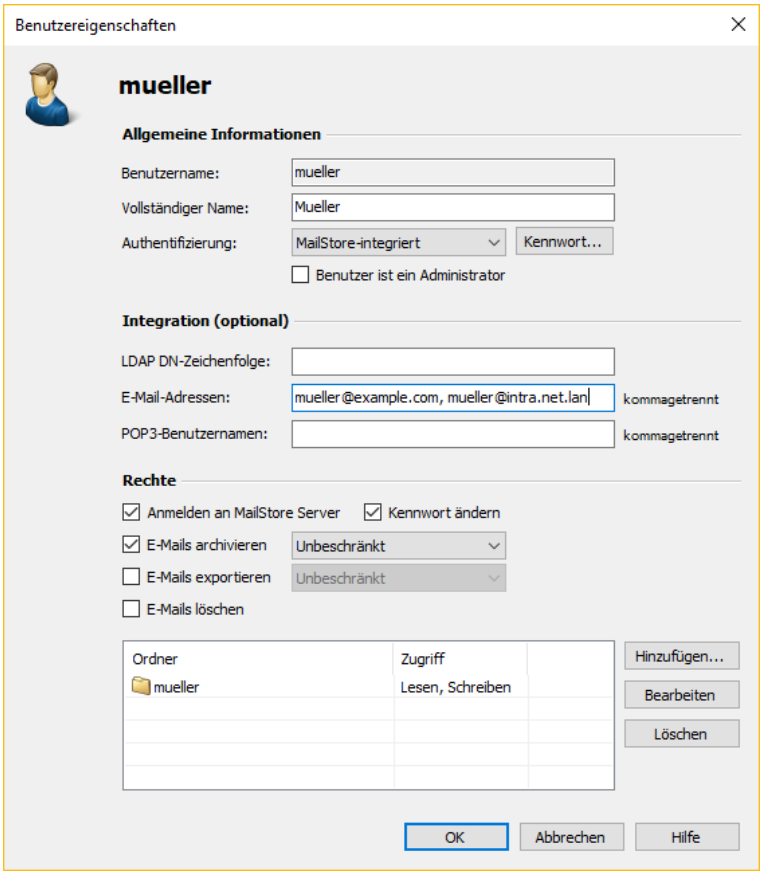


7. Speichern Sie die neue Aufgabe und starten danach den Rechner mit dem MailStore Server neu.

8. Kontrollieren Sie, ob das Netzlaufwerk M: nach dem Systemstart korrekt verbunden wurde. Beachten Sie dabei, dass nur der Windows-Systembenutzer Zugriff auf das Netzlaufwerk hat. Alle anderen Benutzer bekommen den Zugriff verweigert, bzw. sehen ein "Nichtverbundenes Netzlaufwerk". Wenn Sie das angezeigt bekommen, funktioniert die Verbindung korrekt. Nur wenn gar kein Netzlaufwerk angezeigt werden sollte liegt ein Fehler vor.

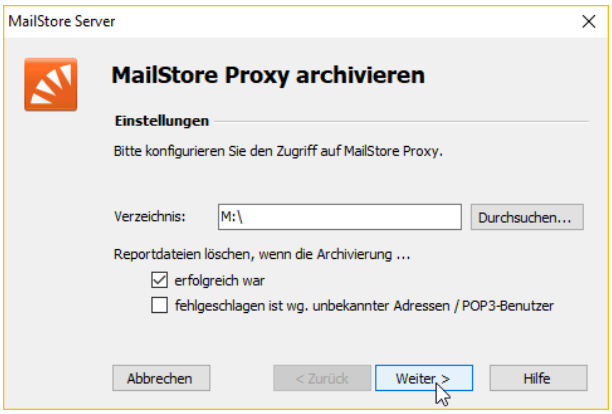
9. Öffnen Sie den MailStore Client, loggen sich mit Administrationsrechten ein und öffnen das Menü "Verwaltung".

10. 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.

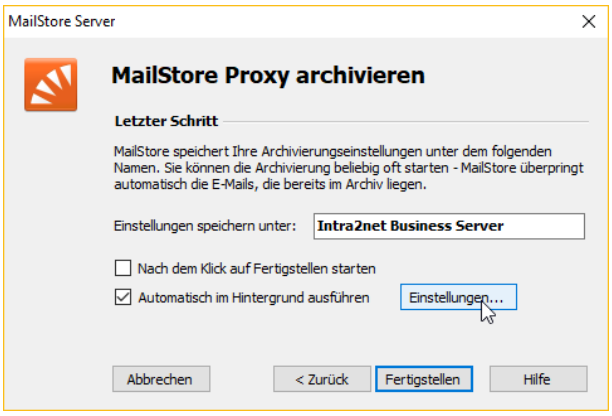


11. Öffnen Sie das Menü "E-Mails archivieren" und konfigurieren ein neues Archivierungsprofil vom Typ "MailStore Proxy".

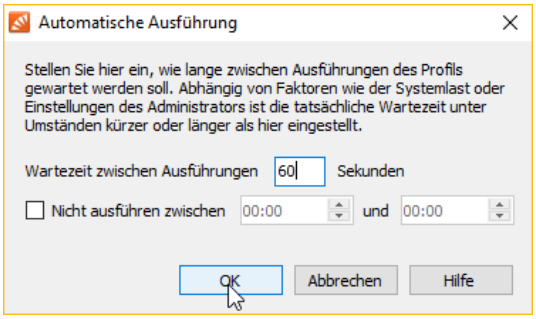
12. Wählen Sie den eben verknüpften Laufwerksbuchstaben als Verzeichnis und lassen die Reportdateien löschen, wenn die Archivierung erfolgreich war (wichtig!).



13. Lassen Sie das Profil Automatisch im Hintergrund ausführen.



14. Lassen Sie das Profil alle **60** Sekunden ausführen und speichern das Profil.



15.10. Automatischer Transfer

Das Intra2net System 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 das Intra2net System Online ist, werden E-Mails immer sofort versendet.

15.11. Verteiler

Das Intra2net System 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 das Intra2net System 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.

15.12. 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.

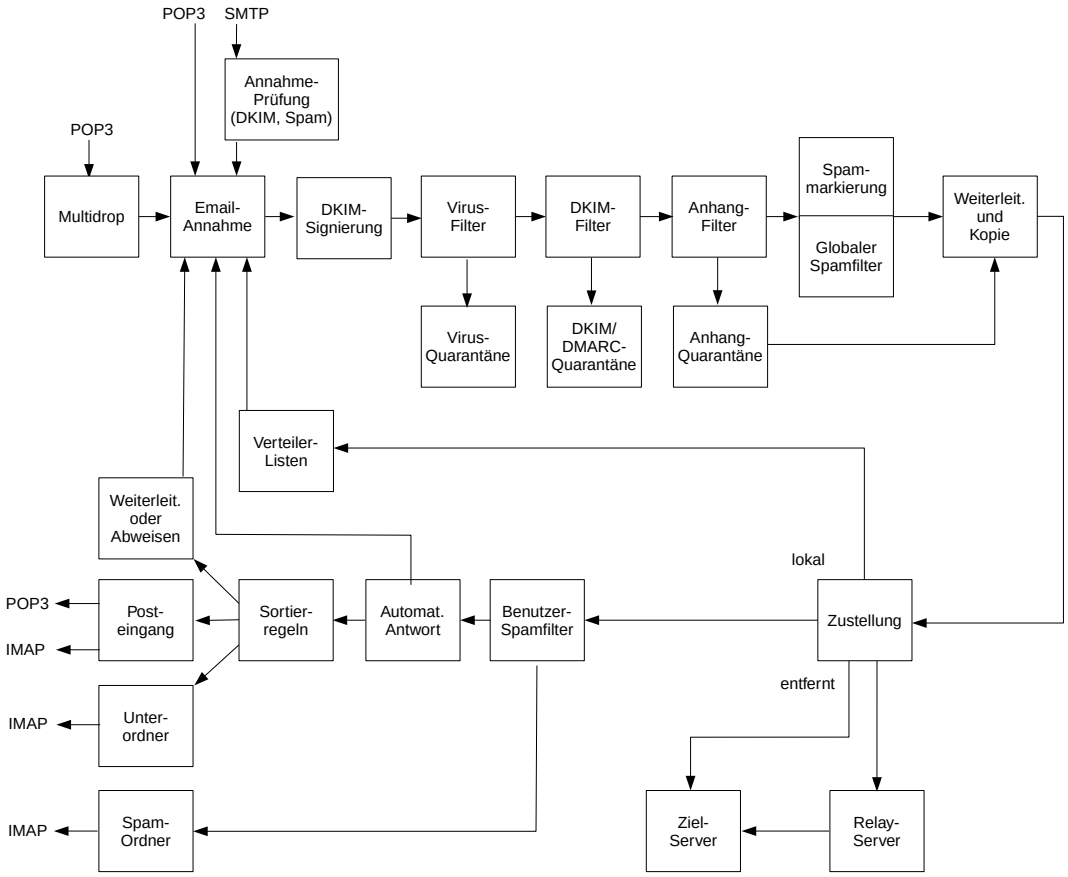
15.13. Warteschlange

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.

15.14. Aufbau des Mailsystems



15.15. Unterschiede zwischen den Lizenzen

Intra2net 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
- DKIM-Signieren und -Filtern
- Schnittstelle zur E-Mail-Archivierung

Intra2net Lizenzen mit Mail Server ermöglichen zusätzlich:

- Dauerhaftes Speichern von E-Mails auf dem Intra2net System

- E-Mail-Abruf durch Clients (wie z.B. Outlook) vom Intra2net System per POP3 und IMAP
- Abwesenheitsschaltung
- E-Mail-Sortierung
- Benutzerbasierter Spamfilter
- Verteilerlisten
- Webmail und Web-Groupware
- ActiveSync

16. Kapitel - Dienste

16.1. Zeitserver

Das Intra2net System hält seine eigene Uhrzeit aktuell, indem es sich, sobald es 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 das Intra2net System 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 das Intra2net System bei den Eigenschaften der Uhr als Internetzeitserver eintragen. Um das SMB-Protokoll zu verwenden, müssen Sie regelmäßig (z.B. bei jedem Systemstart) folgenden Befehl mit Administratorrechten ausführen:

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

Dabei müssen Sie natürlich den lokalen Namen oder die IP-Adresse Ihres Intra2net Systems verwenden.

16.2. Überwachung per SNMP

Unter Dienste > Überwachung > SNMP kann man konfigurieren, ob und wie das Intra2net System Daten für die Überwachung per SNMP bereitstellen soll. Diese Daten können dann von einem zentralen SNMP-Überwachungsdienst abgefragt und ausgewertet werden.

Das Intra2net System 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 Intra2net System angegeben werden.

Es ist sinnvoll, den Überwachungsdienst sich nicht nur beim Intra2net System 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 Intra2net Systems abfragen zu können.

Soll das Intra2net System 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 das Intra2net System über das Internet überwacht werden, richten Sie eine VPN-Verbindung zwischen dem Überwachungsserver und dem Intra2net System ein. Über diese können dann die Daten abgefragt werden.

Das Intra2net System bietet über SNMP u.a. verschiedene Informationen zu CPU- und Speicherauslastung, I/O-Last, Festplattenbelegung, Netzwerkauslastung, Anzahl von Fehlermeldungen, Intra2net Software 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.

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 Intra2net 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

Das Intra2net System aktualisiert seine Systemzeit sobald es Online ist. Wich die Systemzeit während der Installation stark ab, kann es sein, dass der Zeitraum für die Demolizenz falsch berechnet wird. Installieren Sie in diesem Fall das Intra2net System erneut.

17.1.2. Lizenzcode

Haben Sie eine Lizenz erworben, können Sie diese in das System einspielen und damit aktivieren. Dafür benötigt das Intra2net System 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 Intra2net System 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 Virenscannerupdates 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 Intra2net System funktionieren aber auch die Updates für den Virenscanner 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

Das Intra2net System enthält ein Updatesystem, mit dem es 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" das Intra2net System 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. Das Intra2net System 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.

Das Intra2net System 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 das Intra2net System nicht während des Updatevorgangs aus!

Die aktuelle Version der Intra2net Software kann unter Information > Version eingesehen werden.

Das Update der Virendatenbanken wird separat von den Intra2net System-Updates durchgeführt. In der Standardkonfiguration prüft das Intra2net System stündlich auf neue Virendatenbanken und installiert diese dann vollautomatisch.

Zusätzlich zu den stündlichen Abfragen auf neue Virendatenbanken gibt es die Option, dass das Updatesystem per Push-Verfahren über DNS innerhalb weniger Minuten nach der Freigabe neuer Virendatenbanken informiert wird und diese dann auf dem normalen Weg herunterlädt und automatisch installiert. Wenn Sie diese Option nutzen, empfehlen wir die normalen, stündlichen Updates parallel weiter laufen zu lassen. Denn die Übertragung der Versionsinformation per DNS ist nicht kryptographisch abgesichert und kann daher leichter gestört werden als die vollständig per HTTPS abgesicherte Kommunikation zu den Updateservern von Intra2net.

Auch die Spammerkmals-Datenbank wird unabhängig von den Intra2net System-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 Vertriebspartner mit einer größeren Anzahl von Intra2net Systemen sehr bequem. Voraussetzung dafür ist das aktivieren der Funktion "Update-Fernsteuerung zulassen" unter System > Update > Einstellungen auf dem Gerät selbst. Die Freischaltung im Partnerweb erfolgt ca. 5 Minuten nach dem Speichern auf dem Gerät.

Im Partnerweb wählen Sie einzelne Intra2net Systeme 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.

17.2.2. Rettungssystem

Bevor bei einem Updatevorgang des Systems neue Programmteile eingespielt werden, wird eine Kopie des aktuellen Stands der Systempartition erzeugt. Erst danach beginnt der eigentliche Updatevorgang. Diese Kopie wird Rettungssystem genannt und kann bei Bedarf statt dem normalen System gestartet werden. Sie enthält immer den Stand vor dem letzten Update.

Das Rettungssystem wird automatisch gestartet wenn ein Update nicht vollständig eingespielt werden konnte. Z.B. weil ein Hardwarefehler auftrat oder der Benutzer das Gerät während des Updatevorgangs abgeschaltet hat.

Das Rettungssystem kann bei Bedarf auch manuell gestartet werden, z.B. wenn ein Update Fehler in der Funktion verursacht. Dafür kann auf der Konsole, also mit an das Gerät angeschlossenem Monitor und Tastatur, kurz nach dem Start des Geräts im Menü des Bootmanagers das Rettungssystem ausgewählt werden.

Im Rettungssystem kann das System in den allermeisten Fällen normal verwendet werden. Es gibt aber Einschränkungen in der Funktion: Es können keine neuen Benutzer angelegt, gelöscht oder umbenannt werden. Außerdem können vom Rettungssytem aus keine Updates eingespielt werden. Es wird daher empfohlen das Problem, was zur Aktivierung des Rettungssystems führte, so bald wie möglich zu beheben und wieder auf das Primärsystem umzustellen.

Wurde das Rettungssystem durch einen Fehler während des Einspielen eines Updates aktiviert, so gibt es folgende Möglichkeiten um wieder auf das Primärsystem umzustellen und das Update erneut versuchen zu können:

- Sie wenden Sich an den Intra2net Support. Per Fernwartung kann dann das Primärsystem wieder zurückgesetzt werden.
- Sie legen aus dem Rettungssystem heraus ein Backup an, kopieren es auf einen externen Speicher, installieren das System neu und spielen dann das Backup zurück. Gehen Sie dabei vor wie in Abschnitt 17.3.5, „Vorgehen bei Festplattenschaden oder Hardwaretausch“ beschrieben.

17.3. Backup

Das Intra2net System enthält sowohl die aktuellen Konfigurationsdaten als auch alle E-Mails und Groupwaredaten sowie Statistiken, Logdateien und die E-Mail-Anhangquarantäne. Daher ist ein regelmäßiges Backup wichtig.

Da die E-Mails und Groupwaredaten schnell ein großes Volumen annehmen können, dauert ein vollständiges Backup unter Umständen viele Stunden. Daher bietet das System die Möglichkeit nicht nur Vollbackups, sondern auch differenzielle Backups anzulegen. Diese enthalten dann nur alle Änderungen seit dem letzten Vollbackup. Sie können wesentlich schneller erstellt werden und erlauben daher mehrfach am Tag die Daten zu sichern.

In der Standardkonfiguration legt das Intra2net System einmal wöchentlich am Samstag um 22h ein Vollbackup an und an allen Tagen außer Sonntag 3x am Tag um 6:30h, 12:30h und 19h ein differenzielles. Dadurch kann das Vollbackup bei Bedarf den ganzen Sonntag über laufen ohne durch erhöhte Systemlast die Mitarbeiter zu stören. Gleichzeitig bieten

die drei Backups pro Tag ein nur geringes Fenster für Datenverlust falls es jemals zu schwerwiegenden Störungen kommen sollte.

Diese Standardeinstellungen können Sie im Menü System > Backup > Einstellungen an Ihre Bedürfnisse anpassen oder auch ein Backup manuell anstoßen.

Soll manuell oder über die hinterlegte Zeitsteuerung ein differenzielles Backup erstellt werden, es ist aber bisher noch kein Vollbackup vorhanden, so wird statt dessen automatisch ein Vollbackup erstellt.

Die Backups enthalten alle E-Mails, Groupwaredaten, die Konfiguration, die Lizenz, die verschiedenen E-Mail-Quarantänen, die Statistikdaten und die Logdateien des Proxyservers. Nicht im Backup enthalten sind insbesondere die E-Mail-Warteschlange, die E-Mail-Archivierungsschnittstelle und die Logdateien des Systems. Außerdem werden für einzelne E-Mails per IMAP gesetzte Flags nicht im Backup gespeichert. E-Mail-Flags sind Informationen wie "gelesen"/"ungelesen", "markiert", als auch benutzerdefinierte Flags die von manchen E-Mail-Clients außer Outlook angeboten werden. Dies betrifft u.a. Kategorien in Thunderbird.

17.3.1. Schutz der Backups

Die Backups enthalten alle E-Mails, Groupwaredaten und die Konfiguration mit Passwörtern u.a. von E-Mail-Abholungen. Sie müssen daher unbedingt vor dem Zugriff Unbefugter geschützt werden.

Als Basisschutz der Backups kann der Zugriff auf einen Rechner oder Benutzer beschränkt werden. Im Auslieferungszustand ist der Zugriff auf die Backups auf einen Benutzer mit einem per Zufallsgenerator erzeugten Passwort beschränkt. Ändern Sie dieses Passwort um zugreifen zu können.

Für einen erweiterten Schutz können die Backups verschlüsselt werden. Es kommt dafür das symmetrische Verfahren AES-128-GCM zum Einsatz. Das eingegebene Passwort wird direkt nach der Eingabe mit dem scrypt-Verfahren zu einem Schlüsselblock umgewandelt und nur dieser in der internen Konfigurationsdatenbank hinterlegt. Dadurch kann das verwendete Passwort nachträglich nicht mehr aus der Konfigurationsdatenbank ausgelesen werden.



Achtung

Achten Sie unbedingt darauf das Passwort sicher zu verwahren und kontrollieren die genaue Schreibweise über die Augen-Schaltfläche neben dem Eingabefeld. Bei Verlust des Passworts gibt es auch für Intra2net keine realistische Möglichkeit das Backup wieder lesbar zu machen.

Für ein optimales Schutzniveau wird empfohlen das Passwort mindestens alle 5 Jahre zu ändern. Zum einen werden bei Bedarf die scrypt-Parameter an aktuelle Bedrohungsszenarien angepasst und zum anderen wird durch einen regelmäßigen Tausch die Wiederverwendung von Initialisierungsvektoren verhindert.

17.3.2. Aufbewahrungsdauer

Backups werden immer ausschließlich auf der lokalen Festplatte des Systems erstellt und danach zuerst auch lokal vorgehalten. Dies dient vor allem der schnellen Wiederherstellung

im in der Praxis erfahrungsgemäß häufigsten Fall, dem versehentlichen Löschen wichtiger E-Mails durch einen Benutzer.

Die Backups der letzten drei Tage werden in der Standardkonfiguration auf dem System selbst aufbewahrt. Bei differenziellen Backups wird immer auch das zugehörige Vollbackup mit aufbewahrt, auch wenn dieses älter als der eingestellte Zeitraum ist.

Wurden die ersten Backupsätze auf einem System erstellt, finden Sie im Menü System > Backup > Einstellungen eine Statistik über den Zeit- und Platzbedarf. Verwenden Sie diese Daten um die Häufigkeit und Aufbewahrungsdauer an Ihre Bedürfnisse und vorhandenen Speicherplatz anzupassen.

17.3.3. Auslagern

Selbstverständlich reicht es nicht aus, das Backup nur auf dem Intra2net System abzulegen, da z.B. die Festplatte kaputt gehen könnte.

Deshalb können die Backupsätze per HTTPS oder SMB/CIFS (Windows Freigabe) vom Intra2net System auf einen anderen Rechner heruntergeladen werden. Dies kann z.B. durch eine automatisch gestartete Batchdatei geschehen oder indem das Verzeichnis auf dem Intra2net System in ein bestehendes Backupprogramm mit aufgenommen wird.

Eine andere Möglichkeit ist das automatische entfernte Ablegen. Ist diese Funktion aktiv, lädt das Intra2net System die Backupdateien automatisch auf einen Zielserver hoch sobald sie erstellt wurden. Dies kann über das FTP- oder SMB-Protokoll geschehen. Per SMB kann das Intra2net System auch automatisch alte Backupsätze löschen.

17.3.4. Rücksichern

Zum Rückspielen von Backups werden die Backupsätze per SMB/CIFS auf das Intra2net System in die `restore`-Freigabe hochgeladen.

Für diese Freigabe gelten die selben Zugriffsschutzeinstellungen wie für auf dem System erzeugte Backups, siehe Abschnitt 17.3.1, „Schutz der Backups“. Möchten Sie ein differenzielles Backup wiederherstellen, sind sowohl die Dateien des differenziellen, als auch die des zugehörigen Vollbackups zu kopieren.

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 Unterorder 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.

Das Intra2net System 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.

17.3.5. Vorgehen bei Festplattenschaden oder Hardwaretausch

Nach einem Festplattenschaden oder beim Tausch der für das Intra2net System verwendeten Hardware empfehlen wir nach der folgenden Liste vorzugehen. Wir raten dringend

davon ab, die Daten des Intra2net Systems 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. Planen Sie den Hardwareumzug und die dafür nötige Zeit. Schauen Sie dafür im Menü "System > Backup > Einstellungen" auf den Punkt "Vorhersage". Verdoppeln Sie die dort angegebene Zeit um Backup und Wiederherstellen zu berücksichtigen.

   Ziehen Sie abhängig von der geschätzten Dauer die in Abschnitt 17.3.6, „Hardwareumzug mit Unterstützung von Intra2net“ beschriebene Variante in Betracht.

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

3. Backup starten

4. Wenn E-Mail-Archivierung in Verwendung: Kontrollieren ob die Archivierungsschnittstelle vollständig abgerufen und geleert wurde

5. Fertiges Backup auf anderen Rechner kopieren

Bei Defekt und Hardwareumzug

6. Aktuelles Installations-Image für das Intra2net System von www.intra2net.com [https://www.intra2net.com] herunterladen und auf USB-Speichermedium installieren

7. Vom USB-Speichermedium booten und Intra2net System installieren

8. Tragen Sie in der Installations-Maske den IP-Bereich Ihres lokalen Netzes ein

9. Verfügt die neue Hardware über 2 Festplatten, aktivieren Sie jetzt über die Weboberfläche, Menü System > Hardware > RAID, die Festplattenspiegelung. Aktivieren Sie das RAID unbedingt an dieser Stelle, nach Wiederherstellen des Backups dauert es wesenlich länger.

10. Öffnen Sie die Weboberfläche des Intra2net Systems und setzen ein neues Passwort für die Backup-Freigabe (Menü System > Backup > Einstellungen)

11. Kopieren Sie das Backup vom anderen Rechner auf die Restore-Freigabe des Intra2net Systems

12. Spielen Sie das Backup mit Konfiguration und E-Mails auf das Intra2net System zurück

13. Aktivieren Sie das E-Mail- und Groupwaresystem wieder, sofern Sie dieses vorher deaktiviert hatten

14. Konfiguration, E-Mails und Statistikdaten sind wiederhergestellt und funktionsfähig wie vorher

Beim Wiederherstellen von E-Mail- und Groupwaredaten aus einem Backup müssen zur Erhaltung der Datenintegrität die internen Kennungen (*UIDVALIDITY*) aller E-Mail-Ordner geändert werden. Die meisten IMAP-basierten E-Mail-Clients erkennen dies und synchro-

nisieren alle Daten neu vom Server. Wenn viele Clients dies gleichzeitig machen, kann das zu erhöhter Systemlast führen. Auch können E-Mail-Clients dadurch für eine Zeit nur eingeschränkt nutzbar sein. Hinweise wie dies beim Intra2net Groupware Client gehandhabt wird, finden Sie in Abschnitt 25.10.1, „Gesicherte Daten nach Wiederherstellung".

17.3.6. Hardwareumzug mit Unterstützung von Intra2net

Bei einem geplanten Tausch der Hardware können Sie vorgehen wie in Abschnitt 17.3.5, „Vorgehen bei Festplattenschaden oder Hardwaretausch" beschrieben. Allerdings ist das System bei diesem Vorgehen während der Erstellung des Backups und dann beim Zurückspielen nicht nutzbar. Bei einem größeren Volumen an E-Mails kann es sich um mehrere Stunden handeln und damit zum Problem werden. Zusätzlich ist auch noch der Punkt mit der Änderung der UIDVALIDITY der E-Mail-Ordner und das dadurch nötige Resynchronisieren der E-Mails durch die Clients zu beachten.

Daher bietet Intra2net eine Alternative, die diese Nachteile umgeht. Mit Unterstützung des Intra2net Supports kann die neue Hardware im Hintergrund und ohne Störung der Benutzer auf den aktuellen Datenstand gebracht werden. Dieser Vorgang läuft dann z.B. über Nacht. Am nächsten Tag müssen nur noch die seit dem geänderten Daten übertragen und die Konfiguration übernommen werden. Daher beschränkt sich die Nichterreichbarkeit auf ca. 15 bis 30 Minuten. Auch bleibt die UIDVALIDITY der E-Mail-Ordner erhalten, die E-Mail-Clients müssen daher nicht neu synchronisieren.

Bereiten Sie dafür Folgendes vor:

1. Neue Hardware im selben lokalen Netz wie das bisherige Intra2net System

2. Hat dort zuerst eine andere IP-Adresse konfiguriert als das bisherige System (die IP des bisherigen Systems wird dann später übernommen)

3. Internetzugang über ein Providerprofil vom Typ "Router im lokalen Netz", Router ist das bisherige Intra2net System im LAN

4. Es ist die selbe Version des Intra2net Systems installiert wie auf dem bisherigen System

5. Monitor und Tastatur für den Zugriff auf die Konsole stehen bereit

6. Es ist *keine* zusätzliche oder geänderte Lizenz nötig, die bisherige Lizenz kann problemlos auf die neue Hardware übernommen werden.

Wenden Sie sich dann an den Intra2net Support, um einen Termin für den Hardwareumzug auszumachen. Beachten Sie dass es sich hierbei um Consulting handelt und die für den Umzug tatsächlich benötigte Zeit lt. Preisliste berechnet wird.

Das Einrichten der Datenübertragung ist vollständig per Fernwartung möglich. Für die Umstellung am 2. Tag sollte ein geschulter IT-Techniker vor Ort sein um u.a. die Netzwerkkarten korrekt zu identifizieren und die Verkabelung anzupassen.

17.3.7. Standby-Systeme

Um die Wiederherstellungszeit im Fehlerfall zu reduzieren, kann man ein Standby-System vorhalten. Hier sind 2 Varianten möglich:

17.3.7.1. Cold-Standby

Ein Cold-Standby-System ist ein System im lokalen Netz, welches zeitnah die Funktion, Konfiguration und Daten eines ausgefallenen Primärsystems übernehmen kann. Dafür wird ein geeignetes Gerät im lokalen Netz vorrätig gehalten. Das Intra2net System ist dort in der passenden Version installiert und alles ist zur schnellen Übernahme der Daten vorbereitet.

Im Gegensatz zum Hot-Standby-System werden aber die Nutzerdaten nicht im Abstand von wenigen Minuten auf das Cold-Standby-System synchronisiert.

17.3.7.1.1. Einrichten und Umschalten

Konfigurieren Sie das System wie folgt:

- Achten Sie bei der Auswahl der Hardware darauf, dass das Standby-System
  - über die gleiche oder eine höhere Anzahl an Netzwerkkarten verfügt
  - über die gleiche oder eine größere Festplattenkapazität verfügt
- Installieren Sie die aktuelle Version des Intra2net Systems
- Sie benötigen eine separate Lizenz für das Standby-System. Diese ist unabhängig von der Lizenz des Primärsystems immer ein Intra2net Network Security (I2N-INS-100)
- Wenn 2 Festplatten verfügbar sind, richten Sie den RAID-Verbund bereits fertig ein
- Vergeben Sie dem System eine IP im lokalen Netz des primären Intra2net Systems
- Richten Sie ein Providerprofil vom Typ "Router im lokalen Netz" ein und verwenden die IP des primären Intra2net Systems als Router IP
- Der Versionsstand auf dem Standby-System muss immer identisch oder höher als der des primären Systems sein. Installieren Sie also am besten ein Update immer zuerst auf dem Standby-System und starten das Update des Primärsystems erst, wenn das auf dem Standby-System erfolgreich abgeschlossen ist
- Konfigurieren Sie auf dem Primärsystem das entfernte Ablegen des Backups so, dass dieses automatisch direkt in die `restore`-Freigabe des Standby-Systems kopiert wird

Beim Ausfall des Primärsystems gehen sie wie folgt vor:

1. Schalten Sie das Primärsystem aus
2. Sollte das Primärsystem in diesem Moment wieder angeschaltet und verbunden werden, kann es zu Netzwerkstörungen sowie Verlust von E-Mail- und Groupwaredaten kommen.

   Sichern sie daher das Primärsystem gegen versehentliches Wiedereinschalten, z.B. durch Entfernen des Netzkabels und Verkleben der Stromversorgungsbuchse mit einem entsprechend beschrifteten Klebeband.
3. Stellen Sie den letzten, durch das Primärsystem hochgeladenen Backupsatz vollständig auf dem Standby-System wieder her (Menü System > Backup > Wiederherstellen, Wiederherstellungsart "Konfiguration, Statistik, E-Mails und Groupwaredaten")

4. Werden Sie vom System zur Auswahl der einzuspielenden Lizenz gefragt, so wählen Sie die Lizenz des Primärsystems

5. Stecken Sie zusätzliche Netzwerkkabel (z.B. Internetverbindung) vom Primärsystem auf das Standby-System um

6. Warten Sie, bis das Standby-System das Backup vollständig wiederhergestellt und sich automatisch neu gestartet hat

7. Sollte es zu Netzwerk-Verbindungsproblemen kommen, so ist es möglich, dass die Zuordnung der Netzwerkkarten des Standby-Systems anders ist als auf dem Primärsystem.

   Schließen Sie in diesem Fall Monitor und Tastatur an, loggen sich mit einem Benutzer aus der Administratorengruppe an der Konsole ein und überprüfen die Zuordnung der Netzwerkkarten im Menü "Netzwerkkarten Einstellungen". Entfernen Sie dazu ein Netzwerkkabel. Daraufhin wird die Verbindung an der zugehörigen Netzwerkkartennummer im Menü als getrennt angezeigt. Sie können danach über die entsprechende Option die Zuordnung zwischen 2 Netzwerkkarten tauschen.

17.3.7.2. Hot-Standby

Das Cold-Standby hat, vor allem bei einem Intra2net Business Server mit größerem gespeichertem E-Mail-Volumen, den Nachteil, dass dieses auf die Festplatte wiederhergestellt werden muss und dieser Schritt die Wiederherstellungszeit verlängert.

Bei einem Hot-Standby wird dieses Problem umgangen, indem die E-Mail- und Groupwaredaten kontinuierlich auf das Standby-System synchronisiert werden. Außerdem wird durch die kontinuierliche Synchronisation der maximal mögliche Zeitraum zwischen letzter Datensicherung und Ausfall drastisch verkürzt.

Ein Hot-Standby-System kann durch Techniker von Intra2net per Fernwartung eingerichtet werden. Bei Interesse wenden Sie sich bitte an Ihren Fachhändler oder den Intra2net Vertrieb.

17.4. Betrieb hinter einer Firewall

Betreiben Sie das Intra2net System 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 vorher 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 Intra2net System zu den entsprechenden Ports ausgehenden Verbindungen freizugeben.

Zu folgenden Zielen müssen Intra2net Systeme Verbindungen aufbauen können (ausgehende Verbindungen):

Ziel	Protokoll	Zielport / Pakettyp	Funktion
update.intra2net.com	TCP	443 (https)	System-Updates, Antispam-Updates, Lizenzen, Koordination der Antivirus-Updates
avupdate.intra2net.com	TCP	443 (https)	Daten der Antivirus-Updates
*.avcloud.intra2net.com	TCP	443 (https)	Antivirus Cloud für die Realtime-Abfrage von Virus-Prüfsummen
avfpc.intra2net.com	TCP	443 (https)	Antivirus Cloud für die Realtime-Abfrage von fälschlich erkannten Viren (False-Positives)
*.intra2net.pool.ntp.org oder von Ihnen gewählte NTP-Server	TCP und UDP	123 (ntp)	Zeitabgleich
support.intra2net.com	TCP	5000 bis 5050	Hersteller-Fernwartung
Ihr DNS-Server	TCP und UDP	53 (dns)	Namensauflösung
Mehrere Server	TCP	2703	Razor Spamerkennung
Mehrere Server	ICMP	Echo-Request (Ping)	Verbindungsüberwachung

Weitere evtl. freizuschaltende Dienste sind E-Mail (POP3 und SMTP) sowie HTTP, HTTPS und FTP für den Proxy des Intra2net Systems.

Wenn Sie die im Folgenden genannte Dienste nutzen wollen, müssen Sie die entsprechenden Ports für aus dem Internet eingehende Verbindungen öffnen:

Protokoll	Zielport	Funktion
TCP	443 (https)	Webgroupware, Activesync, Fernwartung Hinweis: Die für die Webgroupware und Fernwartung genutzte Portnummer kann geändert werden. Activesync funktioniert dagegen nur wenn Port 443 verwendet wird.
TCP	80 (http)	Ausstellen und Verlängern von Zertifikaten mit Let's Encrypt
TCP	25 (smtp)	Empfang von per SMTP eingehenden E-Mails (MX-Record auf externe IP)
TCP	587 (smtp-submission)	Versand von E-Mails durch externe Benutzer
TCP	993 (imaps)	Abruf von E-Mails und Groupwaredaten durch externe Benutzer
UDP	500 und 4500	Eingehende VPN-Verbindungen

17.5. Logdateien

Unter Information > System > Logdateien bietet das Intra2net System Zugriff auf die internen Logdateien des Systems. Sie können entweder heruntergeladen werden oder die letzten Zeilen in einem Livelog angesehen werden.

Die Logfiles werden täglich, oder sobald sie eine gewisse Größe erreicht haben, rotiert. Die Anzahl der alten Logdateien, die auf dem System aufbewahrt werden, kann über die Tage, nach denen spätestens gelöscht werden soll, konfiguriert werden. Die Größe die die Dateien maximal erreichen dürfen, wird automatisch über einen Algorithmus aus vorhandenem Platz, Anteil der betroffenen Datei am gesamten Logvolumen sowie der Anzahl der Tage, für die die Logs aufbewahrt werden sollen, errechnet.

17.6. Logcheck Reports

Unter Information > System > Report kann eingestellt werden, dass das Intra2net System 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. Das Intra2net System 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 das Intra2net System automatisch ausschalten, wenn es 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.

17.8. Prüfung und Reparatur der Dateisysteme

Beim Start prüft das Gerät automatisch die Konsistenz der Dateisysteme. Sollte dabei ein Fehler erkannt werden, bricht der Systemstart ab. Bei Appliances mit LED-Anzeige bleibt die Anzeige des Starts bei Stufe 2 oder 3 stehen, siehe Abschnitt 3.5.1, „Start des Geräts“.

Details dazu werden ausschließlich auf der Konsole angezeigt. Schließen Sie daher Monitor und Tastatur an das Gerät an. Ein Fehler wird mit `Filesystem check failed` eindeutig angezeigt. Drücken Sie eine Taste um das Gerät neu zu starten.

Beim Neustart wird für kurze Zeit der Bootmanager angezeigt. Normalerweise startet dieser nach wenigen Sekunden das normale System. Wählen Sie hier statt dessen die Option "Dateisystem-Reparaturversuch" aus.

In diesem Modus untersucht das System alle Dateisysteme genauer und versucht automatisch alle erkannten Schäden zu reparieren. Wurde ein Dateisystem repariert, zeigt das System für einige Sekunden das Ergebnis an und geht dann zum nächsten Dateisystem über. Am Ende startet das System automatisch neu.

Schalten Sie das System bei laufendem Dateisystem-Reparaturversuch auf keinen Fall aus, da dies zu noch schwereren Schäden an den Dateisystemen führen kann.



Achtung

Führen Sie keinen Dateisystem-Reparaturversuch durch, wenn Verdacht auf eine beschädigte Festplatte besteht. Dadurch könnte das Dateisystem irreparabel beschädigt werden.

Verdacht auf eine beschädigte Festplatte besteht, wenn vorher entsprechende Meldungen auf der Hauptseite des Intra2net Systems oder in den Systemmeldungen angezeigt wurden, der RAID-Status nicht Ok ist oder ungewöhnliche Geräusche von der Festplatte zu hören sind.

Wenden Sie sich bei Verdacht auf eine beschädigte Festplatte am besten an den Intra2net Support. Alternativ können Sie von der defekten Festplatte eine Low-Level-Kopie anfertigen (z.B. mit dd_rescue) und dann mit dieser Kopie den Reparaturversuch durchführen.

Teil 3. Groupware Client

18. Kapitel - Einführung

18.1. Systemvoraussetzungen

Betriebssystem	• Microsoft Windows 11 (64 Bit auf Intel x86-Plattform) • Microsoft Windows 10 (32 und 64 Bit auf Intel x86-Plattform) • Microsoft Windows Server 2016 (64 Bit) • Microsoft Windows 8 / 8.1 (32 und 64 Bit auf Intel x86-Plattform) • Microsoft Windows Server 2012 R2 (64 Bit) • Microsoft Windows 7 (32 und 64 Bit) • Microsoft Windows Server 2008 (32 und 64 Bit) Der Betrieb in Terminal-Server-Umgebungen ist möglich.
Microsoft Outlook	• Microsoft Outlook 2021 • Microsoft Outlook 2019 • Microsoft Outlook 2016 • Microsoft Outlook 2013 • Microsoft Outlook 2010 • Microsoft Outlook 2007 (mindestens SP1) Es werden 32- und 64-Bit-Varianten von Outlook unterstützt.
Server	Intra2net Business Server ab Version 6.0.0



Achtung

Es darf nur eine Version und Bit-Variante 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 ab Outlook 2013 teilweise unterstützt, sog. Side-By-Side-Installationen), können mit dem Groupware Client nicht zuverlässig genutzt werden.

Auch wenn mit Office verwandte Apps (u.a. "Mein Office", "OneNote" und "Office Lens") aus dem Microsoft Store installiert sind, kann dies zu einer inkompatiblen Side-By-Side-Installation führen. Diese Apps sind bei einigen Versionen von Windows vorinstalliert und müssen über den Microsoft Store deinstalliert werden.

Auch von der Verwendung von Click-to-Run-Installationen von Microsoft Office 2013 raten wir ab, da wir bei dieser Version in einigen Fällen Fehlfunktionen im Zusammenhang mit Click-to-Run beobachtet haben. Verwenden Sie statt dessen eine vollständig lokale offline Installation.

18.2. Übersicht der Funktionen

- Gemeinsamer Zugriff auf E-Mails, 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 und E-Mails auf dem Server
- Synchronisation aller Ordner im Hintergrund
- Einstellbarer Synchronisationsrhythmus pro Ordner
- Gleichzeitige Nutzung mehrerer Serverkonten und E-Mail-Adressen innerhalb eines Outlook-Profils
- 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 Intra2net System.
- Webzugriff auf E-Mails, Termine, Kontakte, Aufgaben und Notizen (Funktion des Intra2net Business Servers, siehe 32. Kapitel, „Einführung in die Web-Groupware“)
- Synchronisation der Daten auf mobile Geräte per ActiveSync (Funktion des Intra2net Business Servers, siehe 35. 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 demselben PC ist dagegen problemlos möglich.
- Einschränkungen bei der Handhabung von Einladungen bei der Nutzung des Kontos auf mehreren Geräten oder mit Freigaben.

  Eingehende Einladungs-E-Mails, daraus erstellte Termine und selbst erstellte Termine mit Einladungen sollten ausschließlich mit dem Groupware Client und nur auf einem Gerät angenommen oder bearbeitet werden. Ansonsten kann es zu Verdoppelungen des Termins, fehlerhaften Nachrichten an den Organisator oder falscher Anzeige des Einladungszustands kommen.
- Geänderte Teilnehmer in einem Serienelement eines Serientermins
- Ganztägige Serientermine, die sich über mehrere ganze Tage erstrecken
- Journal-Funktion

- Verknüpfung von Groupware-Objekten untereinander (z.B. zwischen Kontakt und Termin)

- Anhängen von Dateien an Groupware-Objekte (nicht an E-Mails). An Groupware-Objekte angehängte Dateien werden nicht auf den Server geschrieben und sind damit nicht für andere Nutzer oder auf anderen Geräten sichtbar. Wird das Objekt von einem anderen Gerät oder Nutzer verändert, wird der Anhang entfernt. Auch sind sie nicht im Backup enthalten.

- Verarbeitung von per E-Mail eingehenden Aufgabenzuweisungen nicht möglich

- Die Markierung von E-Mails zur Nachverfolgung mit Datumsangabe wird nicht auf den Server geschrieben und ist damit nicht für andere Nutzer oder auf anderen Geräten sichtbar. Auch ist sie nicht im Backup enthalten. Verwenden Sie daher statt der Markierung zur Nachverfolgung die in Abschnitt 26.4, „Erinnerungen und Nachverfolgen von E-Mails“ beschriebene Methode.

- Wird eine E-Mail sowohl beantwortet als auch weitergeleitet, wird nur einer der beiden Punkte in Outlook als Status angezeigt.

- Umbenennen von freigegebenen Ordnern anderer Benutzer ist nicht möglich. Nur der Eigentümer kann Ordner umbenennen.

- Kein automatisches Ausführen von clientseitigen Sortierregeln in Outlook. Verwenden Sie statt dessen serverseitige Sortierregeln wie in Abschnitt 25.3, „Serverseitige Einstellungen bearbeiten“ beschrieben.

- Die "Rückgängig"-Funktion von Outlook wird nicht unterstützt.

- Automatische Antwort auf vom Absender einer E-Mail erbetene Lesebestätigungen (*Message Disposition Notification* (MDN)). Siehe Abschnitt 26.5, „Lesebestätigungen“.

- Der Groupware Client ist ausgelegt für bis zu 500 Ordner, 50.000 Objekte pro Ordner und E-Mail und Groupwaredaten von bis zu 10 GB (in einer Datendatei verbundene Konten, gemessen auf dem Server, z.B. über das Menü "Information > Statistik > Benutzer").

  Werden diese Werte überschritten, kann es zu Störungen kommen. Unter anderem, aber nicht beschränkt auf, Verzögerungen in der Reaktion auf Nutzereingaben, Verzögerungen in der Synchronisation von Änderungen und sowie Abstürze des Programms.

- Die feste Maximalgröße der Datendatei ist 50 GB (bei Outlook 2007: 20 GB). Die Datendatei enthält alle verbundenen Ordner, unabhängig davon ob es sich um eigene oder freigegebene Ordner fremder Nutzer handelt. Bei Erreichen der Maximalgröße wird die Datendatei irreparabel beschädigt und alle Daten müssen frisch vom Server hereinsynchronisiert werden.

  Über die Option "E-Mails nur als Kopfzeilen abrufen" (siehe Abschnitt 26.1, „E-Mails komplett oder nur Kopfzeilen abrufen“) kann Platz in der Datendatei eingespart werden.

- In der Schnellsuche-Funktion von Outlook (nicht aber bei der erweiterten Suche) erscheinen, während die Suche läuft, Suchtreffer zuerst in zufälliger Reihenfolge. Nach Abschluss der Suche können diese sortiert werden. Außerdem können gelöschte Elemente nicht aus der Schnellsuche ausgeschlossen werden.

- Verwendung des Ordnernamens "Meldungen" (bei englischer Spracheinstellung *Notifications*) auf oberster Ebene der Datendatei nicht möglich.

- Ordnernamen, die sich nur durch Groß- und Kleinschreibung von anderen Ordnernamen auf der selben Ebene unterscheiden sowie Ordnernamen, die mit Leerzeichen beginnen oder enden, werden nicht unterstützt. Dies ist eine Einschränkung von Outlook.

Beachten Sie hierzu auch Abschnitt 31.1, „Synchronisierbare Daten“.

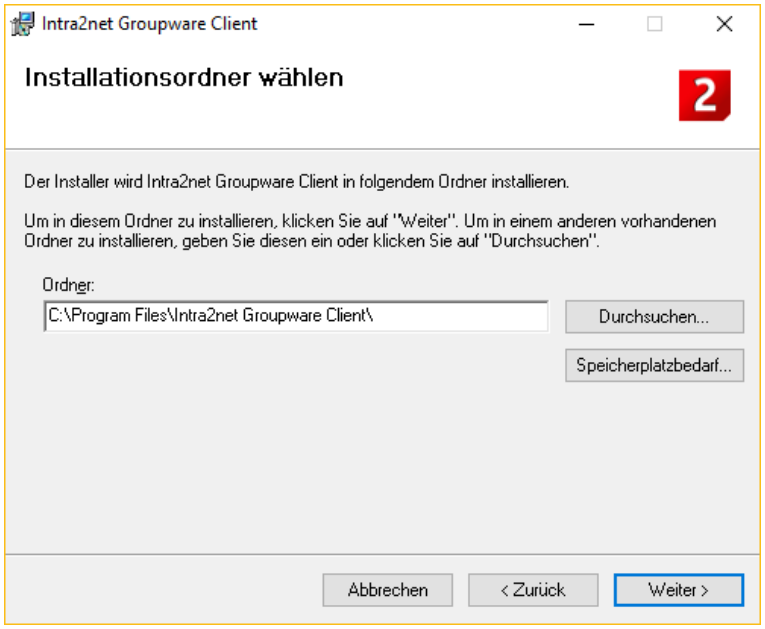
19. Kapitel - Installation

19.1. Installation des Programms

1. Entpacken Sie das ZIP-Archiv, in dem das Programm ausgeliefert wird. Es sind 2 MSI-Dateien enthalten. Wenn ein Outlook in der 32-Bit-Variante installiert ist, verwenden Sie die Datei, die auf `-Win32` endet. Bei der 64-Bit-Variante von Outlook dagegen die, die auf `-x64` endet. Rufen Sie die entsprechende MSI-Datei 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".

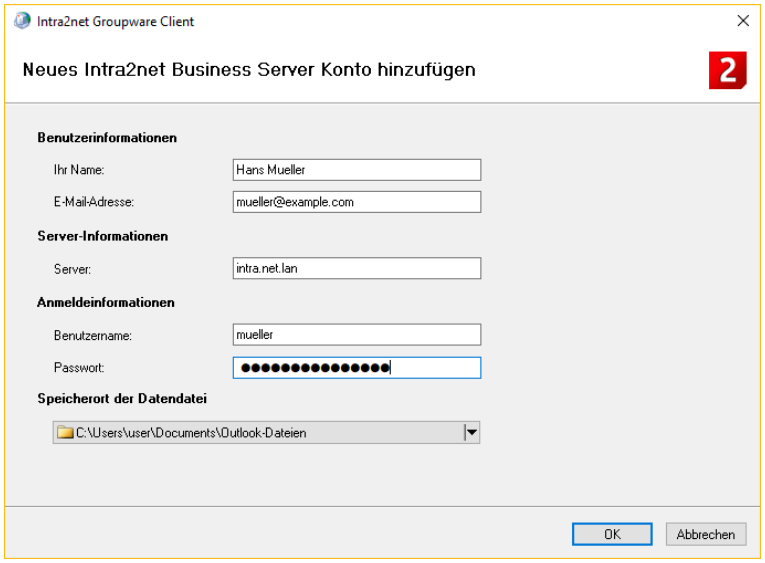


4. War bisher noch kein Outlook-Profil für den Groupware Client angelegt, besteht direkt aus dem Installationsprogramm heraus die Möglichkeit ein passendes Profil anzulegen. Tragen Sie die Nutzer- und Kontodaten ein.

   Tragen Sie unter Server den vollständigen DNS-Namen inkl. Domain Ihres Intra2net Business Servers ein, 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 Intra2net Systems. Verwenden Sie auch hier keine IP-Adresse, sondern registrieren gegebenenfalls für Ihren Server einen DNS-Namen bei Ihrem Domainprovider oder DynDNS-Anbieter.

   Tragen Sie unter Benutzername exakt den Login ein, den Sie auf dem Intra2net Business Server im Menü Benutzermanager > Benutzer vergeben haben. Fügen Sie im Feld Benutzername kein @ und keinen Domainnamen an.

Der Speicherort der Datendatei muss für eine korrekte Funktion unbedingt auf einem lokalen Laufwerk des Client-PCs liegen. Die Verwendung von Netzlaufwerken führt zu Störungen bei der Datensynchronisation sowie dem Versand von E-Mails.



Möchten Sie den Groupware Client erst später konfigurieren, so finden Sie die nötigen Schritte im 20. Kapitel, „Profil einrichten“ beschrieben.

5. Fahren Sie mit der Einrichtung im 21. Kapitel, „Konten konfigurieren“ fort.



Hinweis

Um dem Nutzer alle Optionen bei der Outlook-Profilerzeugung freizuschalten, wird vom Installationsprogramm folgender Wert in der Registry gesetzt:

Schlüssel `HKCU\Software\Policies\Microsoft\Office\16.0\Outlook\setup`, Name `DisableOffice365SimplifiedAccountCreation`, Typ REG_DWORD, Wert 1

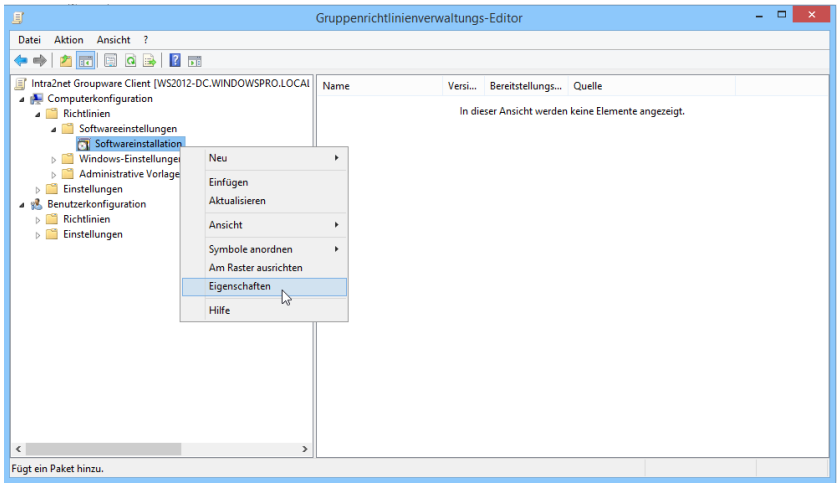
19.2. Verteilung des Programms über Active Directory

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 Benutzerobeflächenoption "Einfach".



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

19.3. Umstieg von 32 Bit auf 64 Bit

Wenn Sie bisher Outlook und den Groupware Client in der 32 Bit Variante installiert haben und jetzt auf die 64 Bit Variante umsteigen wollen oder umgekehrt, gehen Sie bitte wie folgt vor:

1. Schließen Sie Outlook und alle anderen Komponenten von Office
2. Deinstallieren Sie den Groupware Client
3. Deinstallieren Sie Microsoft Office
4. Installieren Sie Microsoft Office in der neuen Bit-Variante
5. Installieren Sie den Groupware Client in der neuen Bit-Variante

Das Outlook-Profil und die Datendatei(en) des Groupware Clients können unverändert weiter verwendet werden. Nur wenn Sie gleichzeitig von einer höheren Outlook-Version auf eine niedrigere umsteigen (also z.B. von Outlook 2019 auf Outlook 2013), müssen Sie Profil und Datendatei neu erstellen um die vollständige Konsistenz der Daten sicherzustellen.

20. Kapitel - Profil einrichten

Für die Nutzung des Groupware Clients muss ein neues Outlook-Profil angelegt werden. Dies ist, weitgehend unabhängig von der installierten Version von Outlook, über die Systemsteuerung möglich und wird im Folgenden beschrieben.

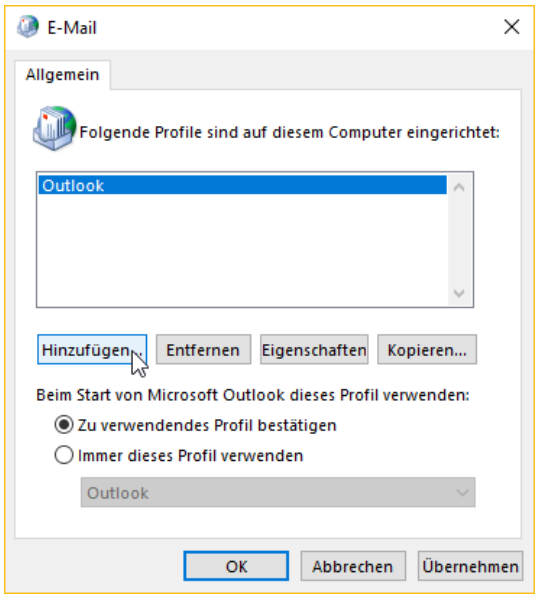
Bestehende Daten können nach der Grundkonfiguration in das neue Profil importiert werden. Dies wird in Abschnitt 21.2, „Bestehende Daten übernehmen“ beschrieben. Vom Hinzufügen des Groupware Clients zu bestehenden Profilen wird abgeraten.

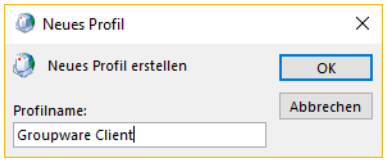
1. Öffnen Sie die Windows-Systemsteuerung, Menüpunkt "Mail (Microsoft Outlook)", bzw. "E-Mail". Die genaue Benennung des Menüpunkts ist abhängig von den verwendeten Versionen von Windows, Outlook sowie der gewählten Systemsprache. Bei manchen Versionen von Windows müssen Sie sich dafür in der Systemsteuerung zuerst alle Elemente anzeigen lassen.

2. Öffnen Sie den Profil-Editor

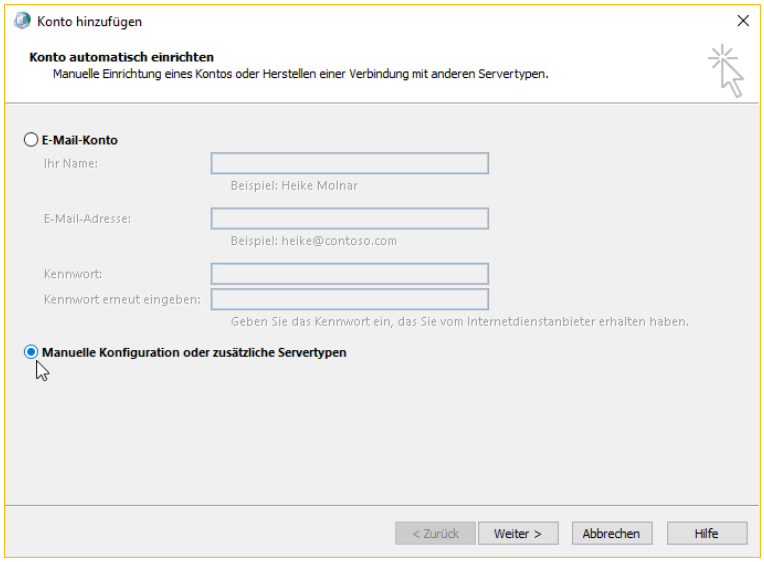


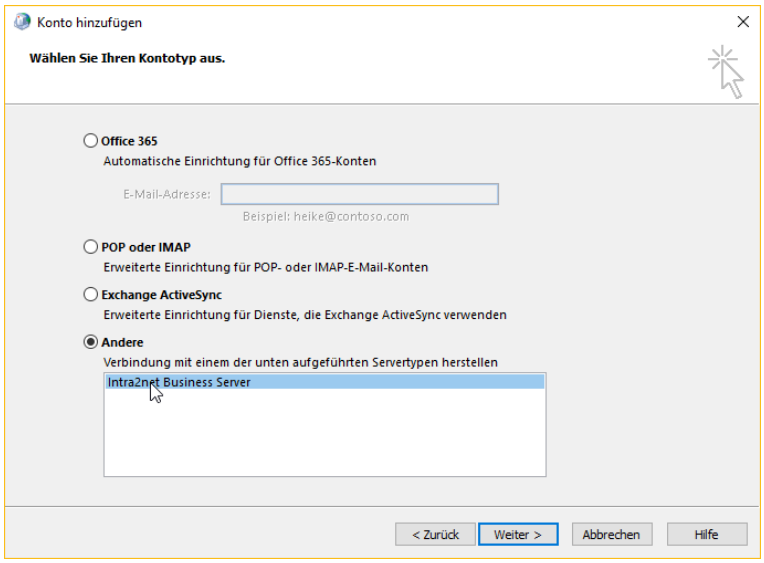
3. Fügen Sie ein neues Profil hinzu und vergeben einen Namen





4. Wählen Sie "Manuelle Konfiguration oder zusätzliche Servertypen" und dann "Andere" und dort "Intra2net Business Server".



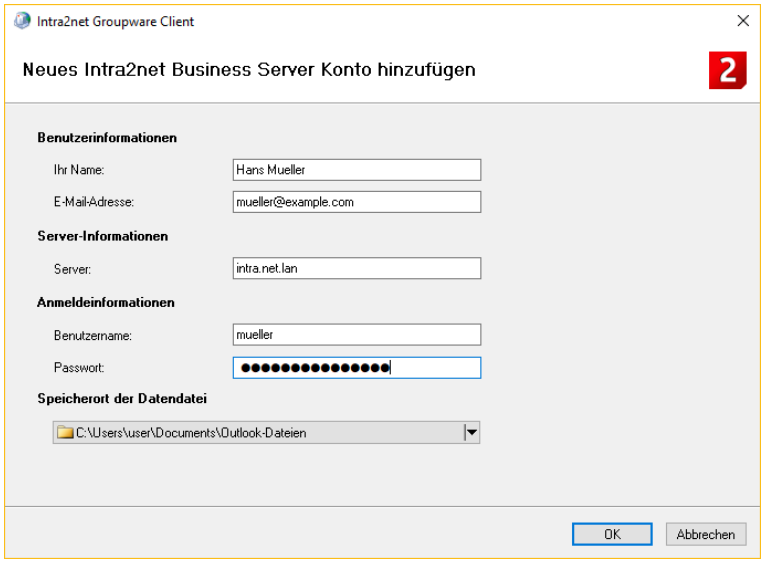


5. Tragen Sie die Benutzer- und Serverdaten ein.

   Tragen Sie unter Server den vollständigen DNS-Namen inkl. Domain Ihres Intra2net Business Servers ein, 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 Intra2net Systems. Verwenden Sie auch hier keine IP-Adresse, sondern registrieren gegebenenfalls für Ihren Server einen DNS-Namen bei Ihrem Domainprovider oder DynDNS-Anbieter.

   Tragen Sie unter Benutzername exakt den Login ein, den Sie auf dem Intra2net Business Server im Menü Benutzermanager > Benutzer vergeben haben. Fügen Sie im Feld Benutzername kein @ und keinen Domainnamen an.

   Der Speicherort der Datendatei muss für eine korrekte Funktion unbedingt auf einem lokalen Laufwerk des Client-PCs liegen. Die Verwendung von Netzlaufwerken führt zu Störungen bei der Datensynchronisation sowie dem Versand von E-Mails.

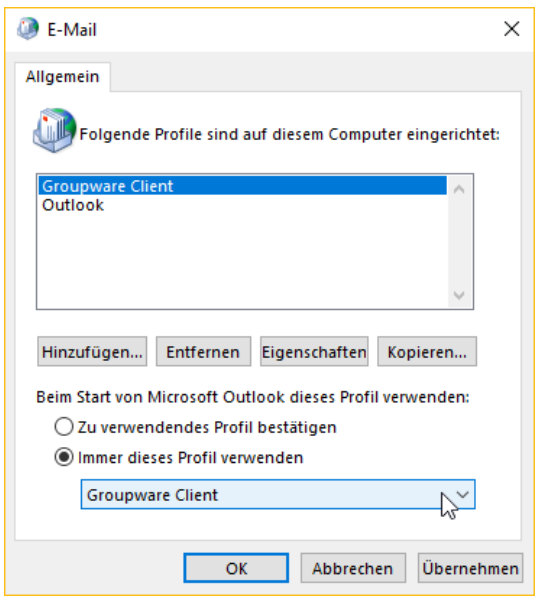


Hinweis

Sollte dieser Dialog nicht angezeigt werden, so ist Microsoft Outlook nicht korrekt oder in einer inkompatiblen Konfiguration installiert. Brechen Sie daher dann an dieser Stelle ab und beheben zuerst das Problem der Outlook-Installation. Beginnen Sie danach wieder mit Schritt 1.

Prüfen Sie zuerst die Abschnitt 18.1, „Systemvoraussetzungen“, insbesondere den Punkt mit Side-By-Side-Installationen ausgelöst durch Apps aus dem Microsoft Store (u.a. "Mein Office", "OneNote" und "Office Lens"). Versuchen Sie danach eine Reparaturinstallation von Microsoft Office.

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



7. Fahren Sie mit der Einrichtung im 21. Kapitel, „Konten konfigurieren“ fort.

21. Kapitel - Konten konfigurieren

21.1. Groupware-Konto

Um die Installation zu vervollständigen, müssen die in den folgenden Abschnitten beschriebenen Einstellungen angepasst werden.

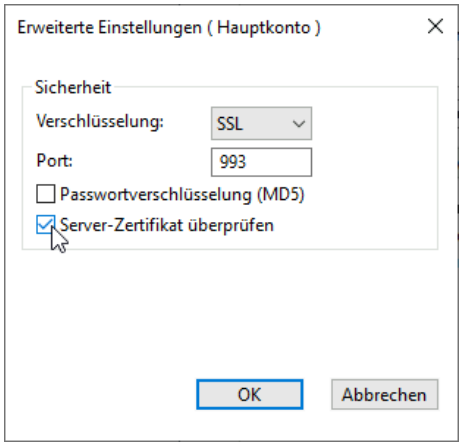
21.1.1. Zertifikatsüberprüfung aktivieren

Aktivieren Sie die Zertifikatsüberprüfung beim Verbindungsaufbau über IMAP. Dadurch wird das Passwort nur über vertrauenswürdige Verbindungen übertragen. Diese Einstellung ist vor allem bei einer Verbindung zum Server über das Internet wichtig.

1. Starten Sie Microsoft Outlook und öffnen das Profil mit dem Intra2net Groupware Client.

2. Öffnen Sie das Menü "Groupware Client", "Kontoeinstellungen".

3. Öffnen Sie das Menü "Erweiterte Einstellungen" und aktivieren die Zertifikatsüberprüfung.

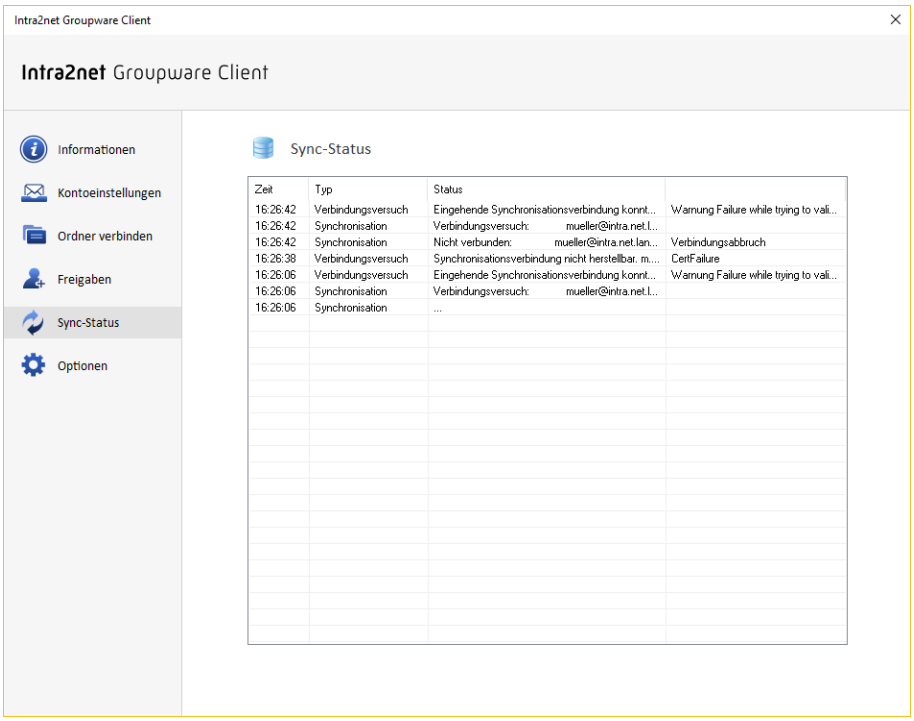


4. Klicken Sie auf "Speichern", um die Kontodaten zu speichern.

5. Öffnen Sie das Menü "Sync-Status" des Groupware Clients und kontrollieren, dass die Verbindung weiterhin erfolgreich aufgebaut werden kann.

21.1.1.1. Vorgehen bei Zertifikatsfehlern

Sollte ein `CertFailure` im Sync-Status angezeigt werden, wird das Zertifikat des Servers nicht als vertrauenswürdig eingestuft.



Prüfen Sie in diesem Fall folgende Punkte:

1. Kontrollieren Sie als erstes, dass Sie den vollständigen DNS-Namen des Server inkl. Domain im Groupware Client hinterlegt haben und nicht eine IP.

2. Handelt es sich beim DNS-Namen um eine lokale Domain oder wurde das Zertifikat nicht von einer externen Zertifizierungsstelle erstellt, muss das Zertifikat in Windows als vertrauenswürdig hinterlegt werden. Gehen Sie dafür vor wie in Abschnitt 10.3, „Zertifikate auf Clients installieren“ beschrieben.

3. Kontrollieren Sie als letztes, dass das Zertifikat des Servers korrekt erstellt wurde, siehe Abschnitt 10.2, „Zertifikate richtig erstellen“

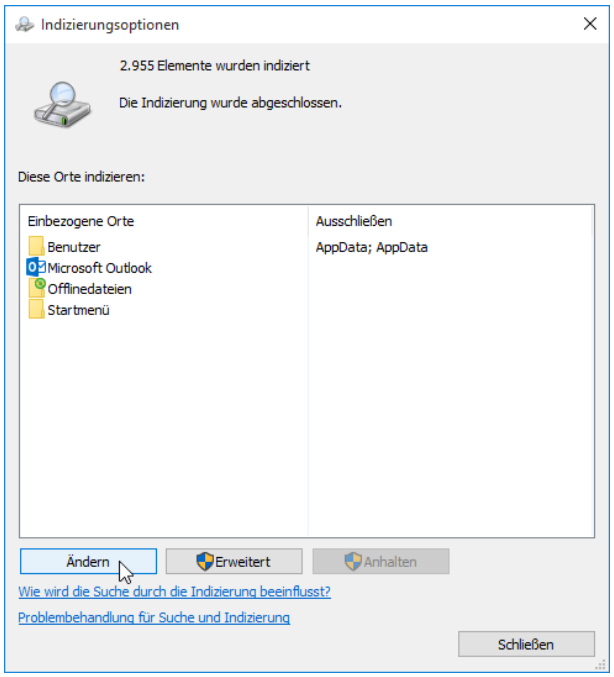
21.1.2. Deaktivieren des Searchindexers

Windows verfügt über einen zentralen Dienst zur Indizierung der Nutzerdaten, welche dann über die systemweite Suchfunktion durchsucht werden können. Dieser Dienst heißt Searchindexer.

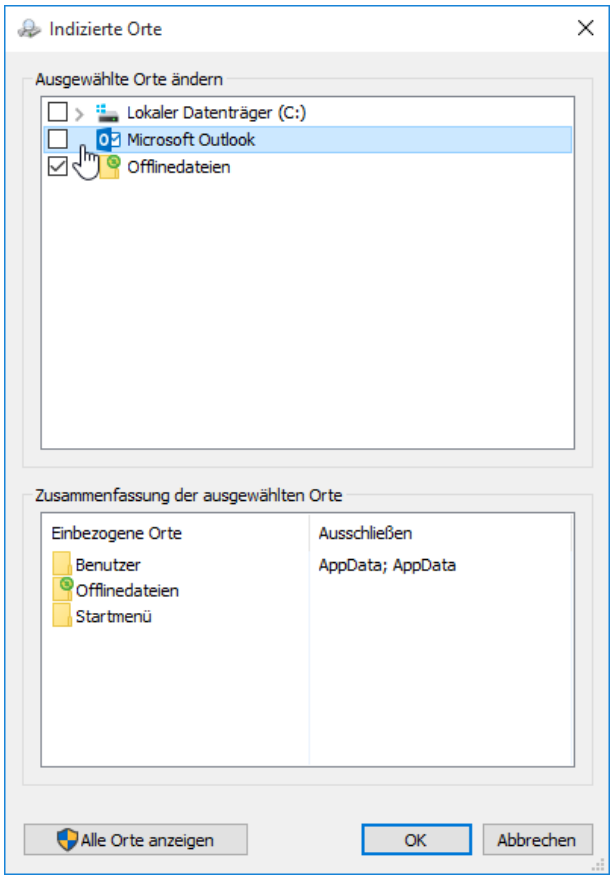
Der Searchindexer versucht standardmäßig auch Daten aus Outlook zu indizieren, was aber vom Groupware Client in der Form nicht unterstützt wird. Dies führt in vielen Fällen zu Performance-Engpässen und einer trägen Reaktion auf Benutzeraktionen in Outlook. Vor allem wird auch der Startvorgang von Outlook verzögert. Daher raten wir dazu, den Searchindexer Outlook nicht indizieren zu lassen. Setzen Sie dies wie folgt um:

1. Öffnen Sie die Windows-Systemsteuerung, Menüpunkt "Indizierungsoptionen".

2. Wählen Sie "Ändern".



3. Entfernen Sie den Haken bei "Microsoft Outlook".



4. Bestätigen Sie die Einstellungen mit "Ok" und schließen die Indizierungsoptionen.

21.2. 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.

Verwenden Sie Outlook bisher mit Microsoft Exchange, so finden Sie den kompletten Migrationsprozess im 30. Kapitel, „Migration von Microsoft Exchange“ beschrieben.

21.2.1. Übernehmen per Outlook-Import

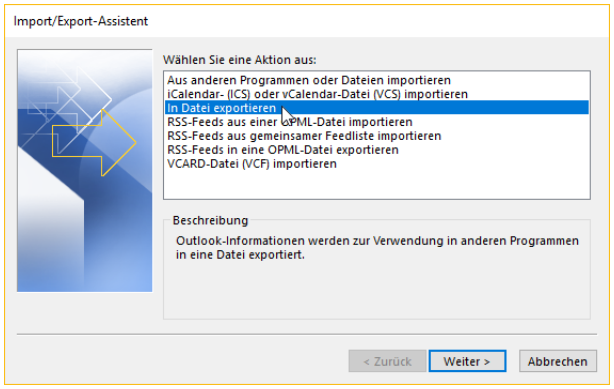
Haben die zu übernehmenden Daten eine Größe von bis etwa 1 GB, können diese mit dem hier beschriebenen Verfahren einfach in den Groupware Client übernommen werden. Haben die zu übernehmenden E-Mails ein größeres Volumen, kann dieses Verfahren weiterhin angewandt werden, braucht aber entsprechend länger. Ein schnellerer Import ist dann meist mit dem in Abschnitt 21.2.2, „Übernehmen größerer Mengen an E-Mails“ beschriebenen Verfahren möglich.

21.2.1.1. Export der bestehenden Daten

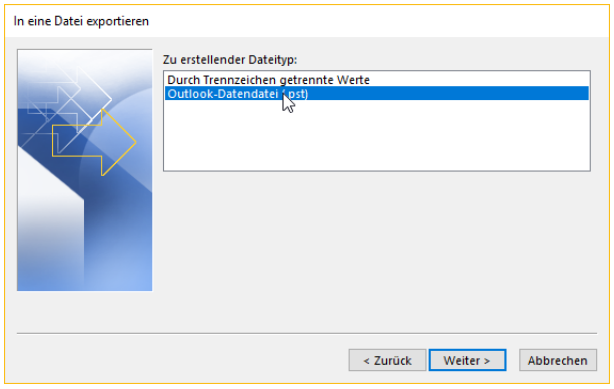
1. Öffnen Sie Outlook mit dem alten Profil welches die zu importierenden Daten enthält. Evtl. müssen Sie das zu öffnende Outlook-Profil über die Windows-Systemsteuerung, Menüpunkt "Mail (Microsoft Outlook)", bzw. "E-Mail" umstellen.

2. Öffnen Sie das Menü "Datei", "Öffnen und Exportieren", "Importieren/Exportieren".

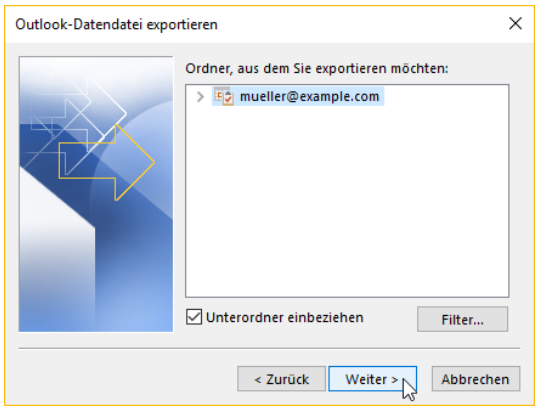
3. Wählen Sie "In Datei exportieren".



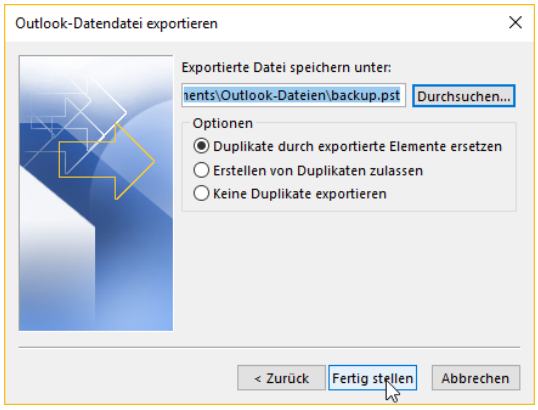
4. Wählen Sie "Outlook-Datendatei (.pst)".



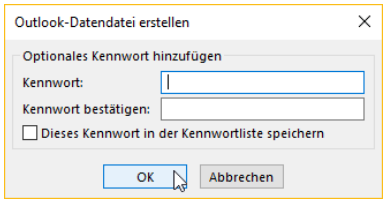
5. Wählen Sie die aktuelle Datendatei inkl. Unterordner.



6. Wählen Sie Verzeichnis und Datei aus, in das die Daten exportiert werden sollen.



7. Ein Kennwort ist nicht erforderlich.



8. Warten Sie bis Outlook alle Daten exportiert hat.

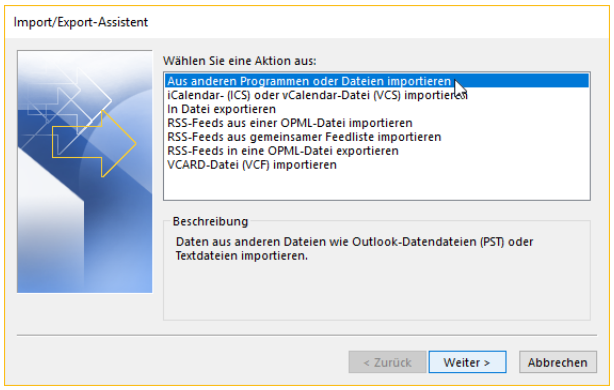
9. Schließen Sie Outlook.

21.2.1.2. Import in den Groupware Client

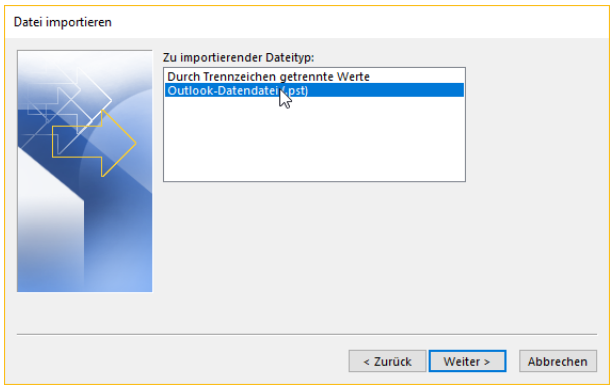
1. Öffnen Sie Outlook mit dem Profil des Groupware Clients. Evtl. müssen Sie das zu öffnende Outlook-Profil über die Windows-Systemsteuerung, Menüpunkt "Mail (Microsoft Outlook)", bzw. "E-Mail" umstellen.

2. Öffnen Sie das Menü "Datei", "Öffnen und Exportieren", "Importieren/Exportieren".

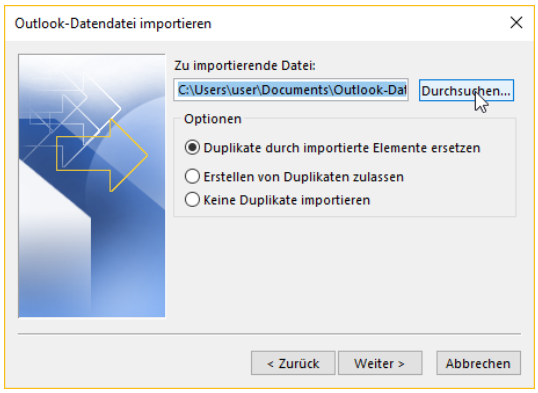
3. Wählen Sie "Aus anderen Programmen oder Dateien importieren".



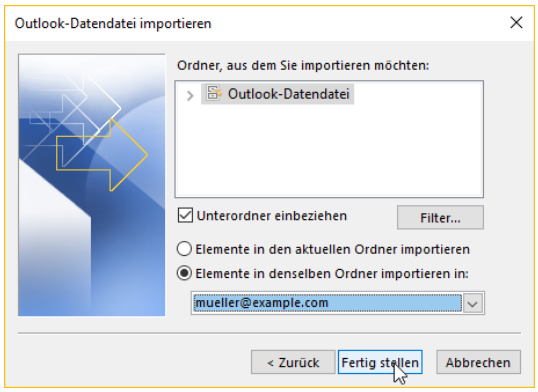
4. Wählen Sie "Outlook-Datendatei (.pst)".



5. Wählen Sie Verzeichnis und Datei aus, in das Sie vorher die Daten exportiert haben.



6. Lassen Sie die Daten inkl. Unterordner in die aktuelle Datendatei in denselben Ordner importieren.



7. Warten Sie bis Outlook alle Daten importiert hat.

8. Der Groupware Client beginnt schon während des Imports im Hintergrund die Daten auf den Server zu schreiben. Dies dauert aber gewöhnlich länger als der Import der Datei in Outlook und läuft daher auch nach dem Abschluss des Imports im Hintergrund weiter. Sie können den Fortschritt im Menü "Groupware Client", "Sync-Status" verfolgen.

21.2.2. Übernehmen größerer Mengen an E-Mails

Wenn Sie bestehende Daten mit dem Groupware Client nutzen wollen und diese größere Mengen an E-Mails enthalten, dann empfiehlt sich das hier beschriebene Verfahren.

Voraussetzung ist, dass sich die E-Mails auf einem per IMAP erreichbaren Server befinden. Die meisten E-Mail-Server sind von Haus aus per IMAP erreichbar oder diese Funktion kann zumindest als Option aktiviert werden. Durch ein Zusatzprogramm werden die E-Mails direkt und ohne Umweg über Outlook vom bisherigen Server auf das Intra2net System kopiert. Per IMAP sind aber nur die E-Mails kopierbar, nicht die Groupwaredaten. Die Groupwaredaten (Kalender, Kontakte, Aufgaben und Notizen) haben aber in den meisten Fällen kein so großes Volumen und können daher über die Import/Export-Funktion von Outlook übertragen werden.

Haben Sie es mit Datenmengen kleiner als etwa 1 GB zu tun oder liegen die E-Mails nicht auf einem per IMAP erreichbaren Server, verwenden Sie statt dessen das in Abschnitt 21.2.1, „Übernehmen per Outlook-Import“ beschriebene Verfahren.

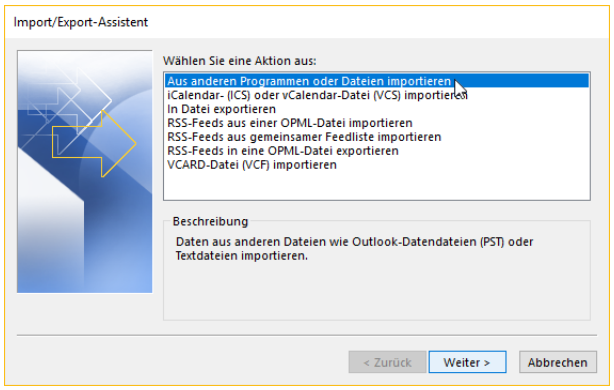
1. Übertragen Sie die E-Mails vom bisherigen Server wie im 29. Kapitel, „Migration von E-Mails mit IMAPCopy“ beschrieben.

2. Exportieren Sie die Daten aus dem bestehenden Outlook-Profil wie in Abschnitt 21.2.1.1, „Export der bestehenden Daten“ beschrieben.

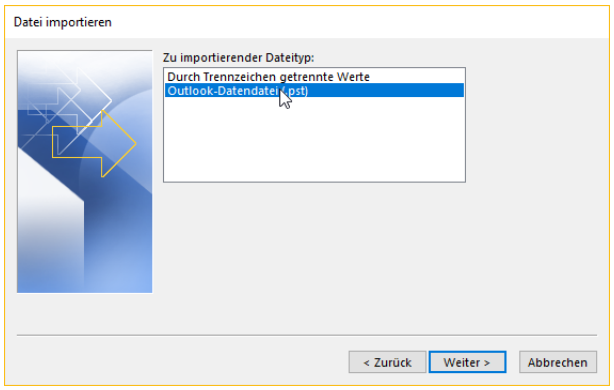
3. Öffnen Sie Outlook mit dem Profil des Groupware Clients. Evtl. müssen Sie das zu öffnende Outlook-Profil über die Windows-Systemsteuerung, Menüpunkt "Mail (Microsoft Outlook)", bzw. "E-Mail" umstellen.

4. Öffnen Sie das Menü "Datei", "Öffnen und Exportieren", "Importieren/Exportieren".

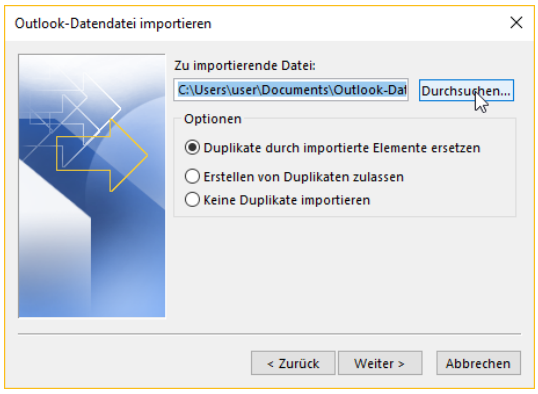
5. Wählen Sie "Aus anderen Programmen oder Dateien importieren".



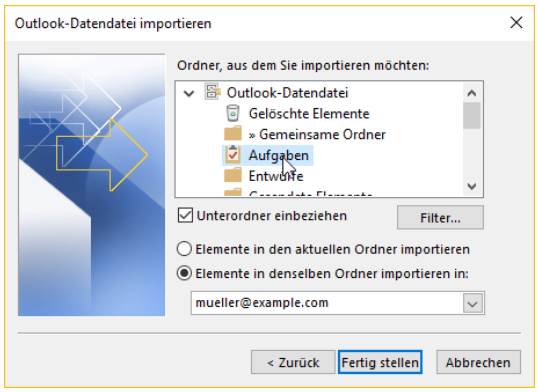
6. Wählen Sie "Outlook-Datendatei (.pst)".



7. Wählen Sie Verzeichnis und Datei aus, in das Sie vorher die Daten exportiert haben.



8. Lassen Sie nicht alle Daten importieren, sondern nur die Ordner mit Groupwaredaten (Kalender, Kontakte, Aufgaben und Notizen). Wählen Sie den ersten Ordner mit Groupwaredaten, hier im Beispiel `Aufgaben`.



9. Wiederholen Sie den Import für alle weiteren Groupwareordner.

21.3. Einrichten mehrerer Konten und E-Mail-Adressen

Sie können mehrere Konten auf dem Server sowie mehrere E-Mail-Adressen gleichzeitig innerhalb eines Outlook-Profils verwenden. Dies ist sinnvoll um z.B. ein firmenweit genutztes Konto wie z.B. "info" anzubinden oder einen Kollegen vollständig vertreten zu können.

21.3.1. Mehrere Serverkonten

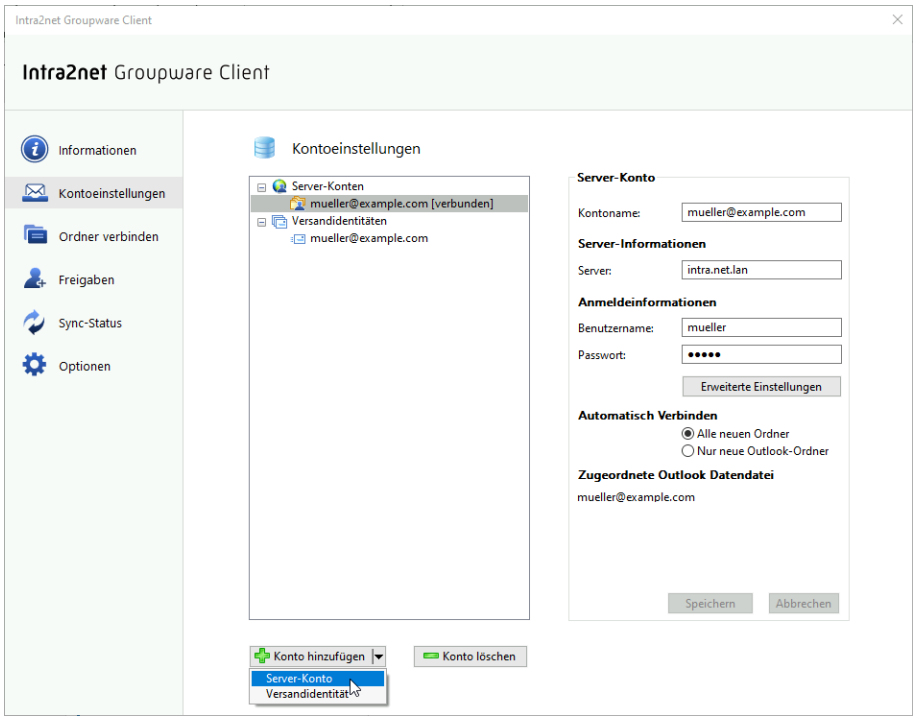


Achtung

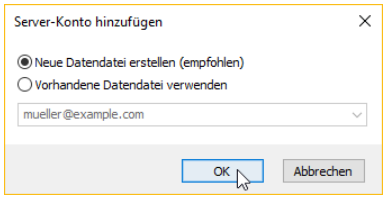
Verwenden Sie ausschließlich die im Folgenden beschriebenen Menüs des Groupware Clients zur Konfiguration von Konten. Verwenden Sie nicht die Kontoeinstellungen von Outlook.

1. Öffnen Sie das Menü "Groupware Client", "Kontoeinstellungen".

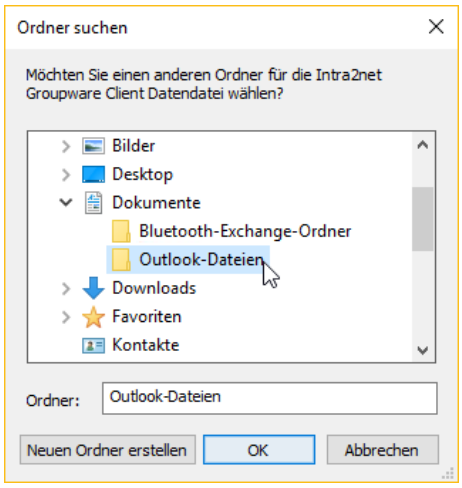
2. Wählen Sie unten "Konto hinzufügen", "Server-Konto".



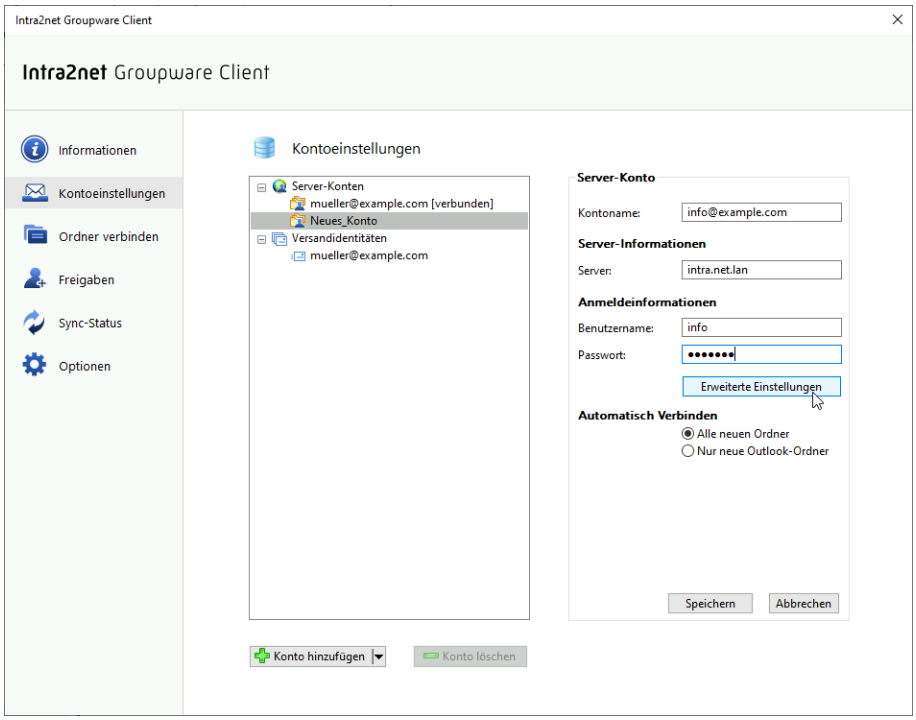
3. Wählen Sie "Neue Datendatei erstellen" wenn Sie das gesamte Konto als zusätzliche Datendatei einfügen möchten. Die Option "Vorhandene Datendatei verwenden" ist gedacht für die Fälle, bei denen nur einzelne Ordner des neuen Kontos unter "Gemeinsame Ordner" verbunden werden sollen.



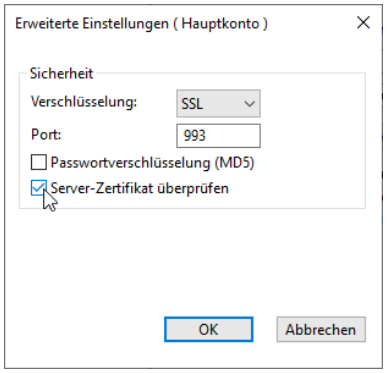
4. Wählen Sie den Ordner, in dem die neue Datendatei abgelegt werden soll.



5. Tragen Sie den vollständigen Servernamen, Login und Passwort ein und vergeben eine Kontobezeichnung.



6. Öffnen Sie die "Erweiterte Einstellungen" und aktivieren Sie die Überprüfung des Server-Zertifikats.



7. Speichern Sie die Einstellungen.

21.3.2. Mehrere Absenderadressen

Sie können, unabhängig von der Anzahl der Serverkonten, beliebig viele verschiedene E-Mail-Absenderadressen konfigurieren. Bei Bedarf können Sie für diese Absenderadressen unterschiedliche Ordner zur Ablage der gesendeten E-Mails festlegen.



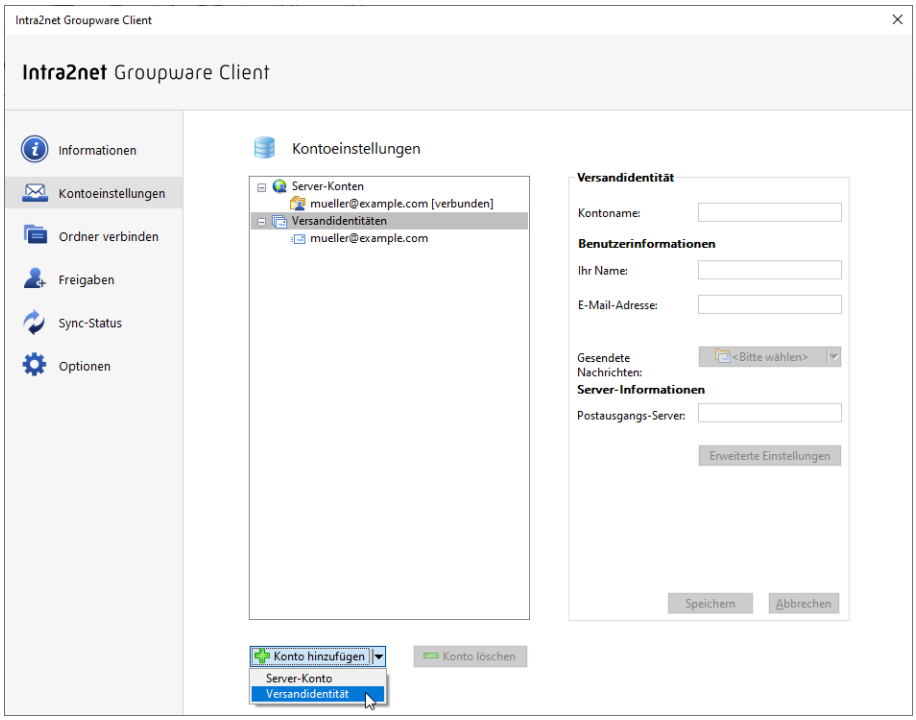
Achtung

Verwenden Sie ausschließlich die im Folgenden beschriebenen Menüs des Groupware Clients zur Konfiguration von Konten. Verwenden Sie nicht die Kontoeinstellungen von Outlook.

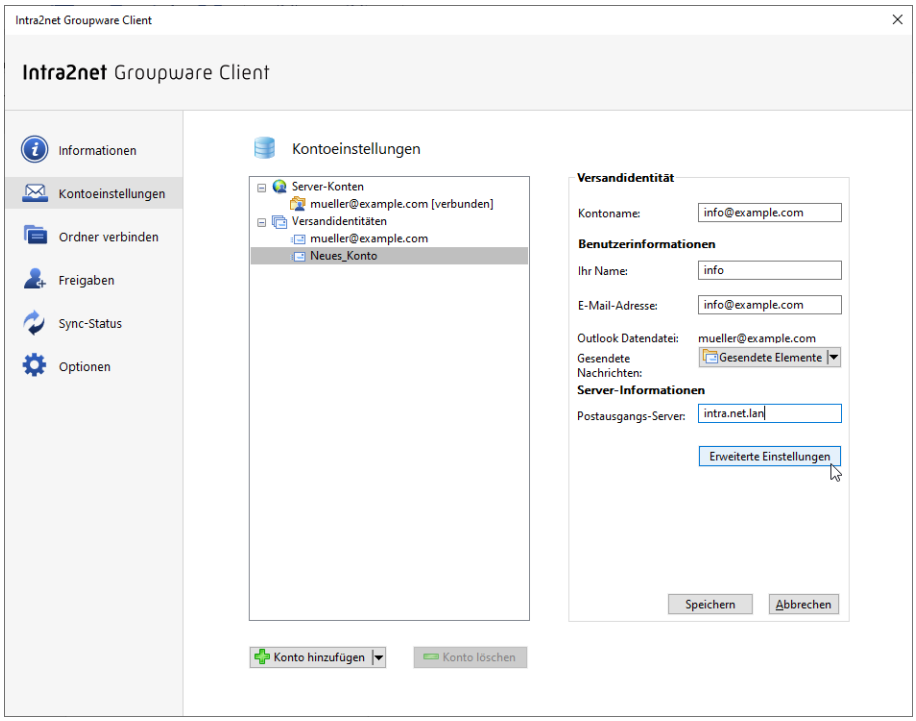
Gehen Sie wie im Folgenden beschrieben vor um neue Absenderadressen anzulegen.

1. Öffnen Sie das Menü "Groupware Client", "Kontoeinstellungen".

2. Wählen Sie unten "Konto hinzufügen", "Versandidentität".

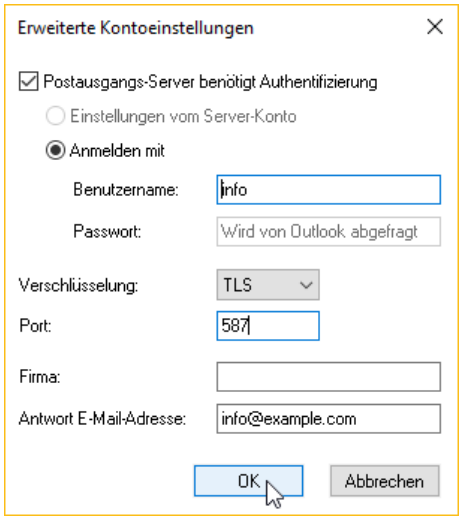


3. Tragen Sie den Benutzernamen, E-Mail-Adresse und Postausgangsserver ein und vergeben eine Kontobezeichnung.

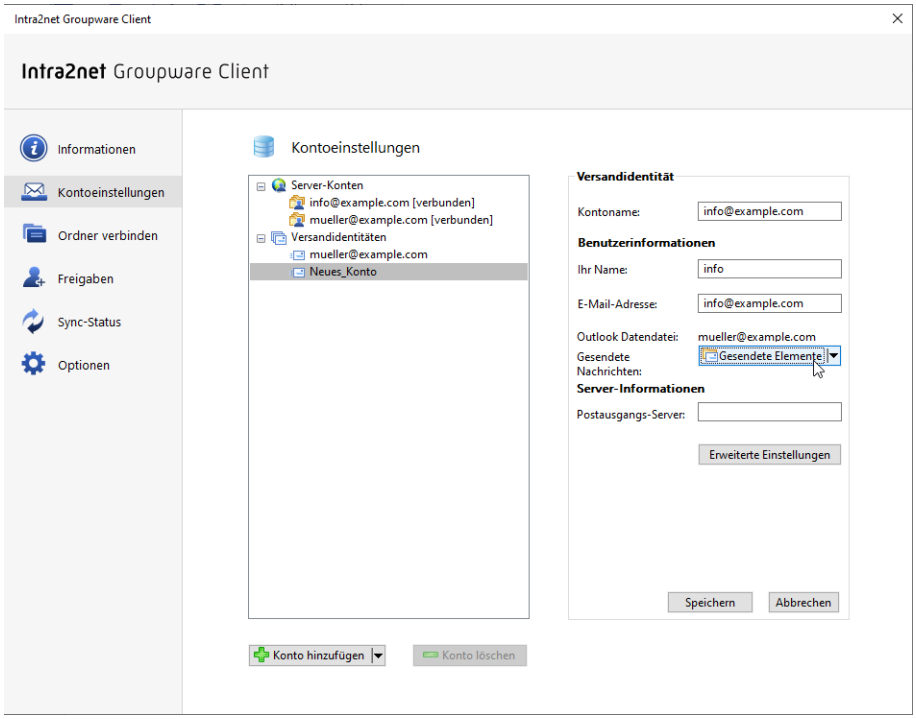


4. Öffnen Sie die "Erweiterte Einstellungen", aktivieren die Verschlüsselung per TLS und stellen den verwendeten Port auf 587.

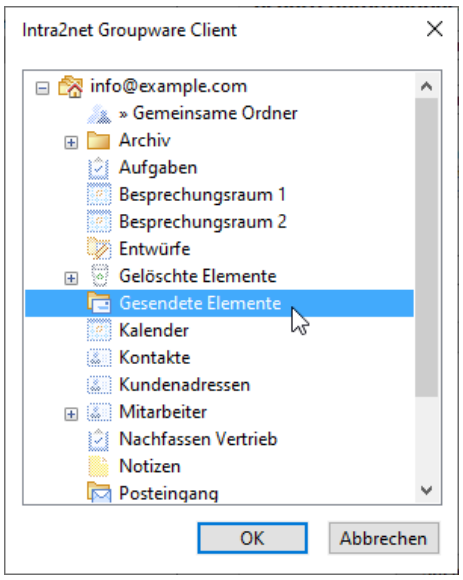
   Bei Bedarf können Sie auch die Authentifizierung aktivieren sowie einen mit den E-Mails versendeten Firmennamen und eine abweichende Antwortadresse hinterlegen.



5. Klicken Sie auf das Auswahlelement hinter "Gesendete Nachrichten".



6. Wählen Sie aus, in welchem Ordner mit dieser Versandidentität gesendete Nachrichten abgelegt werden sollen.



7. Speichern Sie die Einstellungen und starten Outlook neu.

21.3.2.1. Ordnerauswahl für gesendete Nachrichten

Wenn Sie mehrere unterschiedliche Absenderadressen für ein Server-Konto konfiguriert haben, ist es oft sinnvoll, die gesendeten Nachrichten abhängig von der verwendeten Absenderadresse in unterschiedlichen Ordnern abzulegen. Wird eine Absenderadresse von mehreren Nutzern verwendet, macht es oft Sinn auch die gesendeten Nachrichten in einem gemeinsam genutzten Ordner abzulegen. Dafür kann der Ordner für die gesendeten Nachrichten bei jeder Versandidentität unterschiedlich gewählt werden.

Wenn Sie gesendete Nachrichten in einem anderen Ordner als "Gesendete Elemente" ablegen möchten, gelten folgende Besonderheiten:

- Gesendete E-Mails werden zuerst im Ordner "Gesendete Elemente" abgelegt. Wenige Minuten später werden sie dann automatisch in den gewählten Ordner verschoben.
- Der Ordner "Gesendete Elemente" wird automatisch von der Synchronisation zum Server ausgeschlossen. Achten Sie daher darauf, dass andere Nutzer dieses Kontos auf dem Server nicht weiterhin "Gesendete Elemente" verwenden. Die Synchronisation in Gegenrichtung, also vom Server, findet weiterhin statt.
- Es ist nicht möglich, dass eine Versandidentität den Ordner "Gesendete Elemente" verwendet, während eine andere Versandidentität einen anderen Ordner in der selben Datendatei zum Speichern gesendeter E-Mails verwendet.

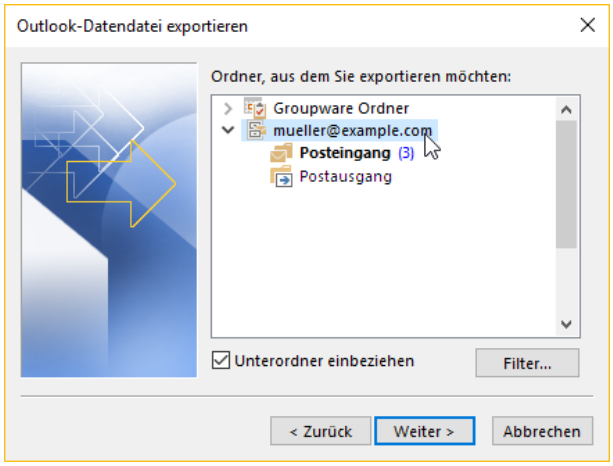
  Stellen Sie in diesem Fall bei allen Versandidentitäten andere Ordner als "Gesendete Elemente" ein.

21.4. Umwandeln bisheriger Installationen des Groupware Clients

Verwenden Sie bisher den Intra2net Groupware Client nur zur Synchronisation der Groupware-Daten und verwenden für E-Mails eine separate, von Outlook verwaltete IMAP-Datendatei, so können Sie bei Bedarf die Verarbeitung auch der E-Mails auf den Groupware Client umstellen.

Im Folgenden wird beschrieben, wie Sie diese Umstellung durchführen.

1. Erstellen Sie über die Import/Export-Funktion eine Sicherheitskopie der lokalen Datendatei für die E-Mails. Die Schritte für den Export finden Sie in Abschnitt 21.2.1.1, „Export der bestehenden Daten“ erklärt. Achten Sie dabei nur darauf, die für E-Mails verwendete Datendatei als Datenquelle auszuwählen.



2. Öffnen Sie die eben exportierte Sicherheitskopie über das Menü "Datei", "Öffnen und Exportieren", "Outlook-Datendatei öffnen" und kontrollieren, ob sie alle E-Mail-Ordner enthält und diese vollständig sind. Schließen Sie sie danach wieder.

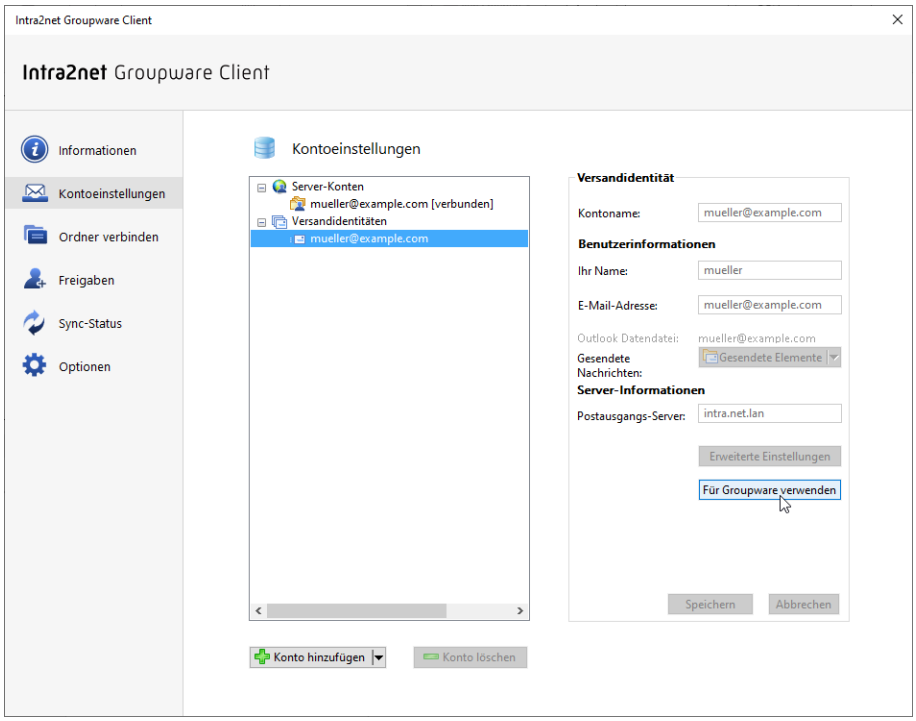


Achtung

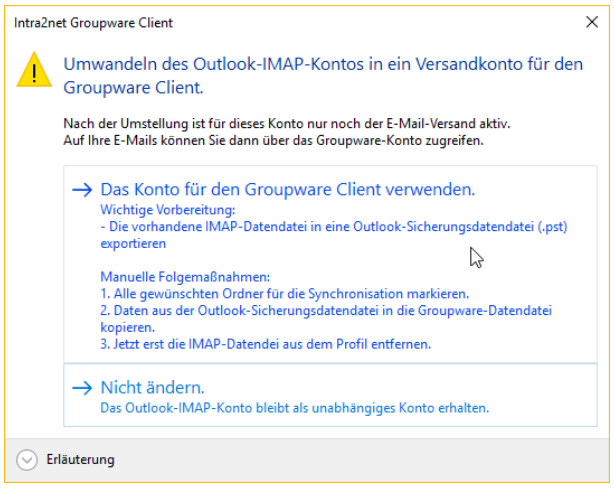
Ohne vollständige Sicherheitskopie kann es zu Verlust von E-Mails kommen.

3. Öffnen Sie das Menü "Groupware Client", "Kontoeinstellungen".

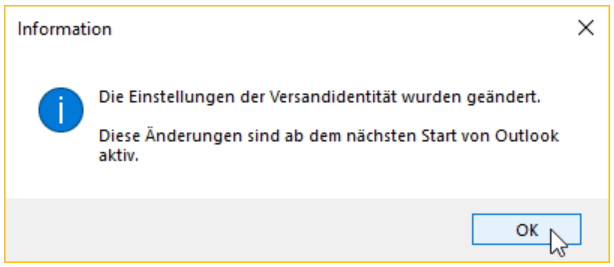
4. Wählen Sie unter "Versandidentitäten" das bisherige IMAP-Konto aus und klicken auf "Für Groupware verwenden".



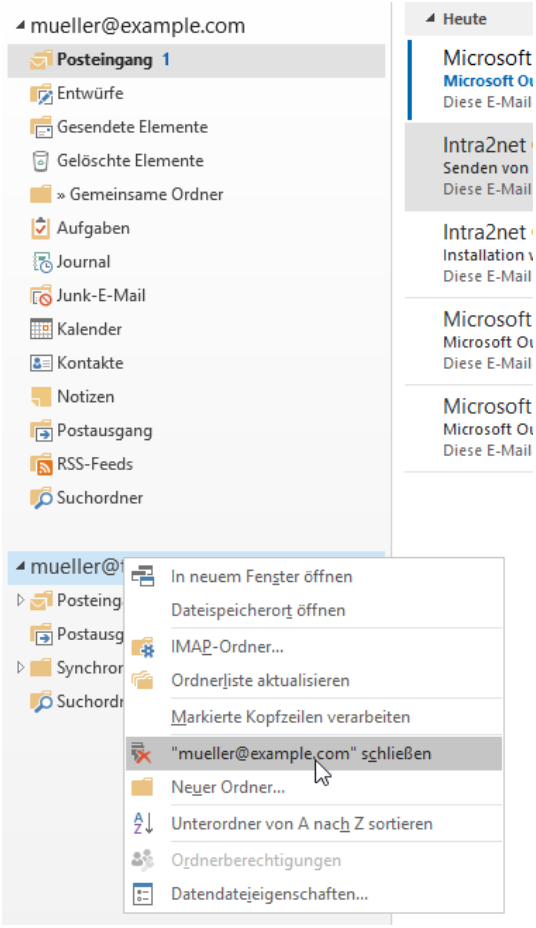
5. Wenn Sie vorher eine Sicherheitskopie der E-Mail-Daten angelegt haben, können Sie die Sicherheitsabfrage mit "Ja" bestätigen.



6. Beenden Sie Outlook, warten bis der Outlook-Prozess wirklich beendet wurde (siehe Taskmanager) und starten es danach neu.

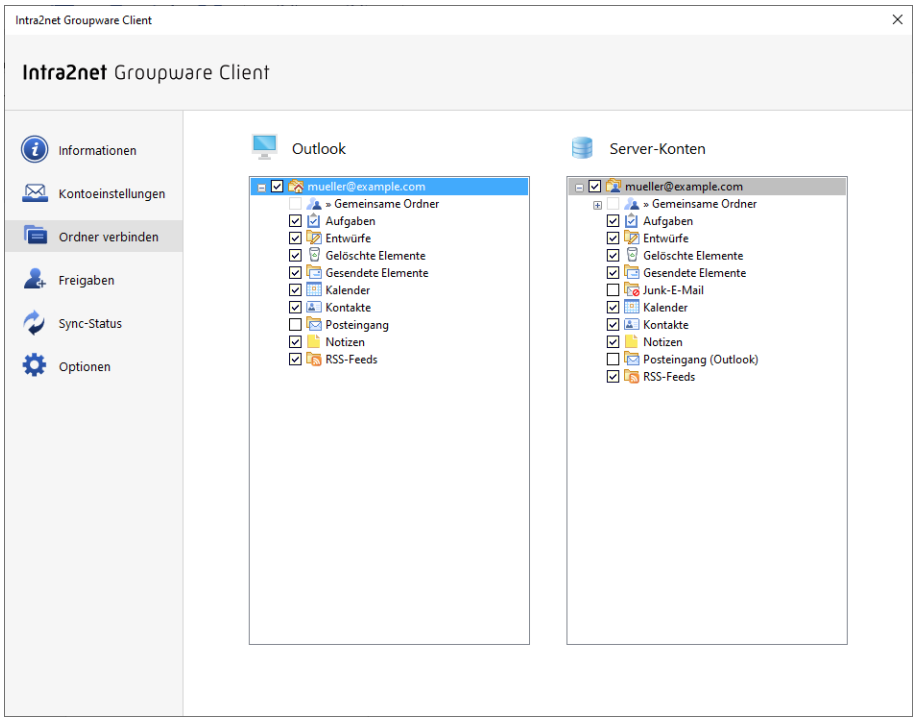


7. Im Ordnerbaum auf der linken Seite von Outlook kann in einigen Konfigurationen weiterhin die Datendatei für das E-Mail-Konto angezeigt werden. Diese muss dann entfernt werden. Klicken Sie dafür mit der rechten Maustaste auf die Datendatei und wählen ""Datendateiname" schließen". Sie erkennen die bisherige IMAP-Datendatei daran, dass Sie *keinen* Ordner "Gemeinsame Ordner" enthält.

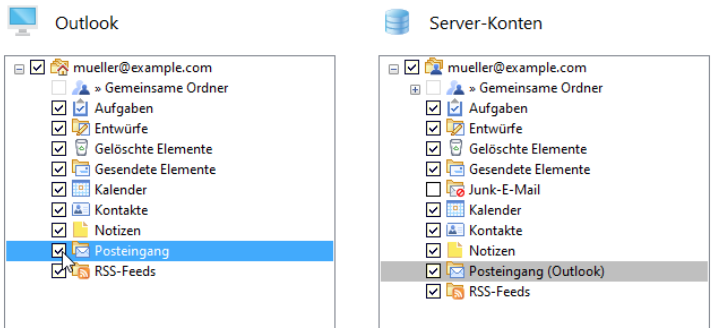


8. Öffnen Sie das Menü "Groupware Client", "Ordner verbinden".

9. Wie man an den fehlenden Häkchen vor den E-Mail-Ordnern erkennt, werden diese bislang nicht vom Groupware Client synchronisiert. Dies wird im Folgenden geändert.



10. Klicken Sie die Checkbox vor dem Ordnernamen auf der linken Seite (Outlook) an und setzen damit das Häkchen.



11. Wiederholen Sie den vorherigen Schritt für alle E-Mail-Ordner.

12. Sie können den Fortschritt im Menü "Groupware Client", "Sync-Status" verfolgen.

13. Nachdem die Synchronisation abgeschlossen ist kontrollieren Sie die E-Mail-Ordner auf Vollständigkeit.

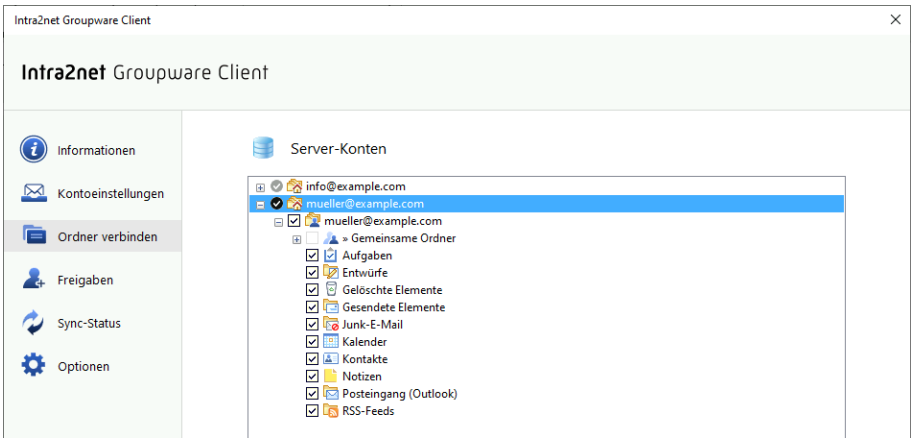
Sollten gesamte Ordner oder einzelne E-Mails fehlen, so können Sie diese aus der anfangs erstellten Sicherheitskopie kopieren. Öffnen Sie dazu die Sicherheitskopie als zusätzliche Datendatei (Menü "Datei", "Öffnen", "Outlook-Datendatei öffnen") und kopieren die fehlenden Daten per Drag&Drop in die andere Datendatei. Verwenden Sie nicht die Import-Funktion von Outlook, da dies in diesem Fall zu Störungen in den importierten Ordnern führen kann.

22. Kapitel - Ordner verbinden

Im Menü "Groupware Client > Ordner verbinden" wird gesteuert welche Ordner auf dem Serverkonto mit dem lokalen Outlook-Datendatei verbunden sein sollen.

In diesem Menü wird immer die Liste der Ordner auf dem Server angezeigt. Verbundene Ordner (durch gesetztes Checkbox-Symbol gekennzeichnet) erscheinen dann an der entsprechenden Stelle in der Ordnerhierarchie auch innerhalb der lokalen Outlook-Datendatei.

Wenn ein Ordner verbunden ist, bedeutet dies, dass alle Inhalte zwischen der lokalen Outlook-Ordner und dem Server-Ordner synchronisiert werden.

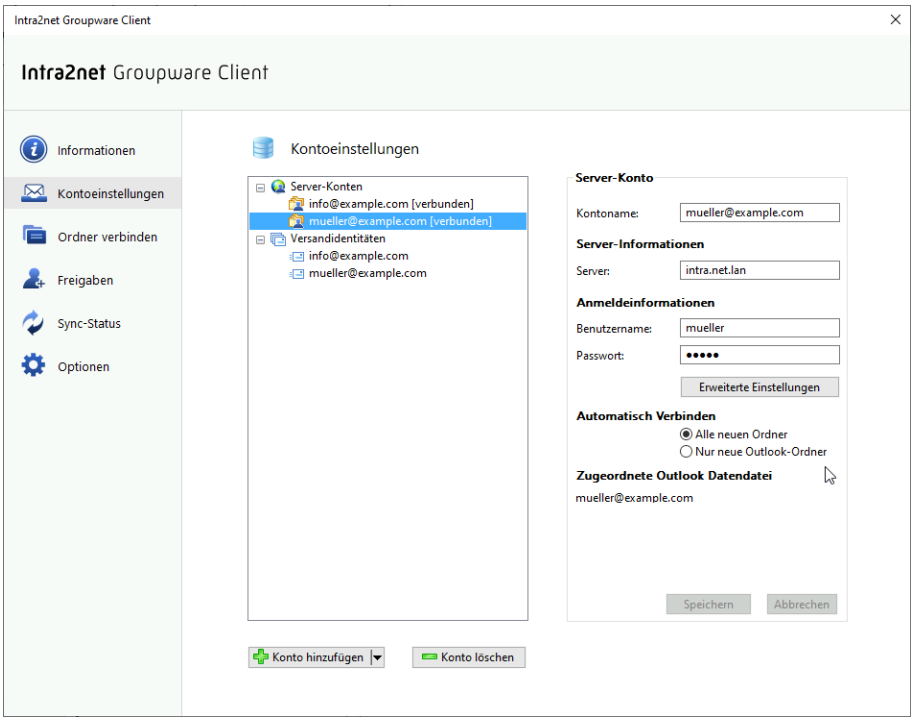


In diesem Kapitel wird der Standardmodus für Ordnerverbindungen beschrieben. Es gibt alternativ auch noch den Expertenmodus, welcher im 24. Kapitel, „Expertenmodus für Ordnerverbindungen“ beschrieben wird.

22.1. Eigene Ordner verbinden

22.1.1. Automatisch verbinden

In der Standardeinstellung werden in der Outlook-Datendatei alle eigenen Ordner des Serverkontos verbunden und umgekehrt alle lokal neu angelegten Ordner auch auf dem Server angelegt und verbunden. Dies entspricht der Option "Alle neuen Ordner" bei "Automatisch verbinden" im Menü "Groupware Client > Kontoeinstellungen".



In manchen Fällen kann es sinnvoll sein, dass neu auf dem Server angelegte Ordner nicht automatisch verbunden und mit der Outlook-Datendatei synchronisiert werden. Z.B. wenn dadurch die Datendatei zu groß werden würde. In diesem Fall können Sie auf "Nur neue Outlook-Ordner" umstellen. Lokal in Outlook neu angelegte Ordner werden dann weiterhin automatisch verbunden, auf dem Server neu angelegte Ordner dagegen nicht mehr. Sie müssen sie im "Ordner verbinden"-Menü dann einzeln anklicken um sie zu verbinden.

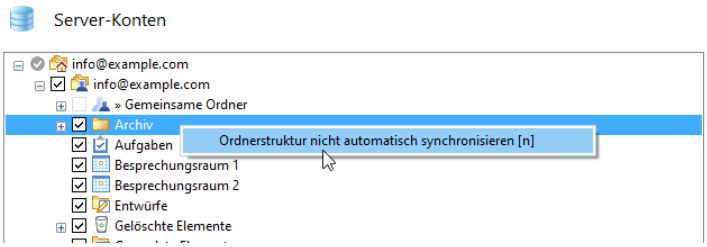
Werden eigene Ordner in Outlook gelöscht, umbenannt oder verschoben, wird diese Änderung immer auch sofort auf dem Server nachvollzogen.

22.1.2. Ordner von der Synchronisation ausschließen

Es kann sinnvoll sein Ordner ausschließlich lokal in der Outlook-Datendatei zu halten und sie nicht mit dem Server zu synchronisieren. Z.B. kann es den Löschvorgang beschleunigen wenn man `Gelöschte Elemente` nicht mit dem Server synchronisiert. Ein anderes Beispiel ist der `Entwürfe`-Ordner, dessen Synchronisation zu Konflikten mit dem automatischen Speichern von zur Bearbeitung geöffneten und noch nicht versendeten E-Mails führen kann.

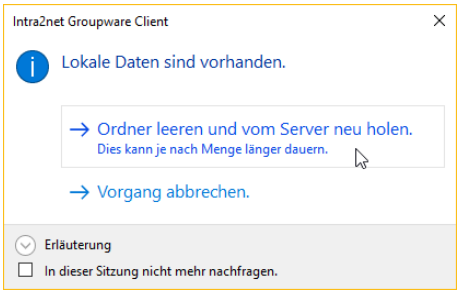
Eine andere gewünschte Konfiguration kann sein, normalerweise neu auf dem Server angelegte Ordner automatisch zu synchronisieren, einige wenige Teile der Ordnerhierarchie aber davon auszuschließen.

Für beides können Sie die Funktion "Ordnerstruktur nicht automatisch synchronisieren" verwenden. Sie finden diese im Menü "Groupware Client > Ordner verbinden" wenn Sie einen Ordner dort mit der rechten Maustaste anklicken.



Beachten Sie, dass ein derart konfigurierter Ordner immer in der lokalen Outlook-Datendatei mit seinem Inhalt vorhanden bleibt, der Ordner und seine Unterordner aber ausschließlich lokal sind und nicht mehr mit dem Server synchronisiert werden. Bei Bedarf können die Unterordner in Outlook gelöscht werden. Der Ordner selbst muss aber bestehen bleiben um die Ausnahme von der Synchronisation zu erhalten. Würde der Ordner aus der lokalen Outlook-Datendatei gelöscht, würde er bei der nächsten Synchronisation der Ordnerstruktur wieder frisch angelegt und sein Inhalt vom Server reinsynchronisiert werden.

Soll die Einstellung wieder rückgängig gemacht werden, setzen Sie die Checkbox des Ordners wieder. Damit die Synchronisation wieder aufgenommen werden kann, müssen zuerst alle lokal vorhandenen Daten und alle Unterordner gelöscht und durch den Inhalt auf dem Server ersetzt werden. Der Nutzer wird darüber in einem Dialog informiert und muss die Löschung starten.



22.1.3. Ordnerliste aktualisieren

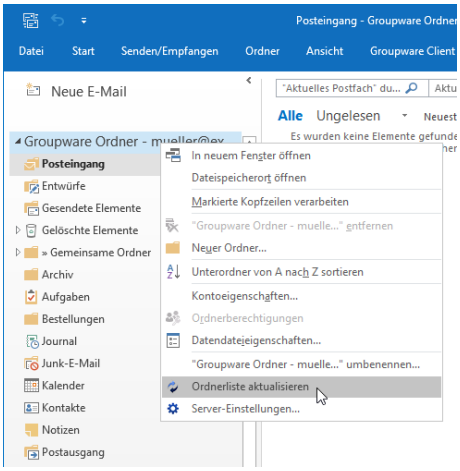
Serverseitige Änderungen an der Ordnerstruktur, also z.B. auf dem Server neu angelegte oder umbenannte Ordner, werden beim Start von Outlook und danach regelmäßig im Hintergrund erkannt und in die lokale Outlook-Datendatei übernommen. Dieser Prozess läuft alle 60 Minuten



Hinweis

Dies betrifft nur die Ordnerstruktur an sich, nicht aber den Inhalt der Ordner. Für die Synchronisation der Inhalte siehe Abschnitt 25.2, „Ordneroptionen“.

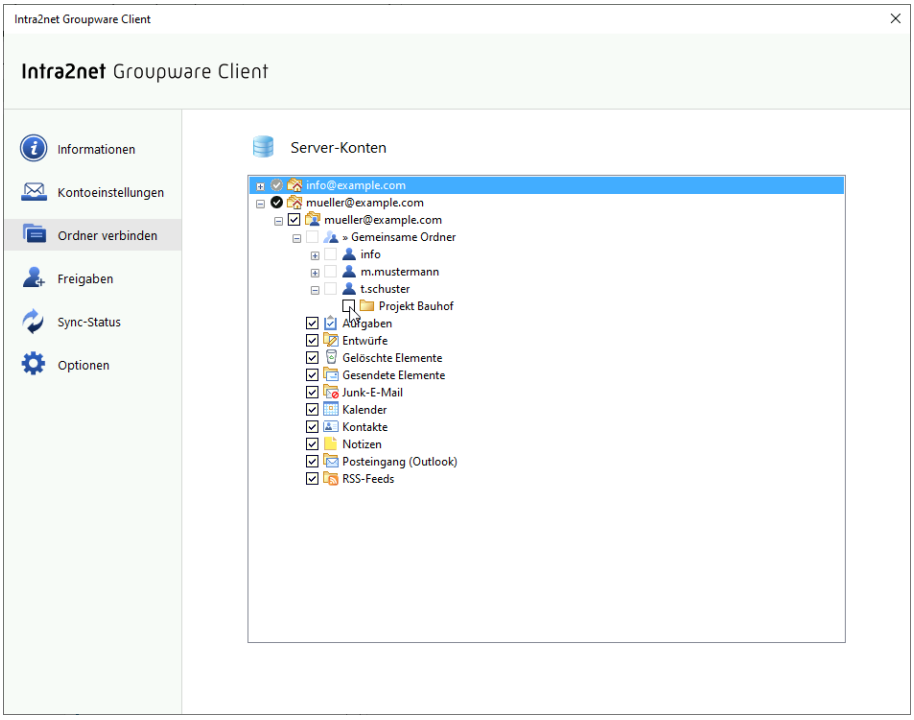
Sie können den Groupware Client anweisen die Ordnerstruktur sofort zu aktualisieren, indem Sie mit einem Rechtsklick in der Ordnerliste das Kontextmenü eines vom Groupware Client verwalteten Ordners öffnen und dort die Option "Ordnerliste aktualisieren" aufrufen. Dadurch wird die Ordnerstruktur der gesamten Outlook-Datendatei aktualisiert.



22.2. Gemeinsame Ordner verbinden

Wurde Ihnen oder einer Gruppe in der Sie Mitglied sind ein Ordner freigegeben, so erhalten Sie beim nächsten Start von Outlook im Posteingang einen Hinweis darauf. Im Gegensatz zu eigenen Ordnern werden neue gemeinsame Ordner nicht automatisch verbunden.

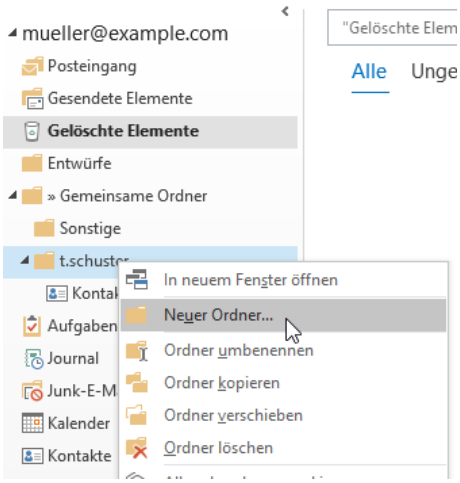
Nutzen Sie das Menü "Groupware Client > Ordner verbinden" und dort den Punkt "»Gemeinsame Ordner" um gemeinsame Ordner zu verbinden und damit in Outlook nutzbar zu machen. Klicken Sie das Checkbox-Symbol an um einen Ordner zu verbinden oder eine Verbindung wieder zu entfernen.



Haben Sie das "Ordner"-Recht auf einen gemeinsamen Ordner, können Sie den Ordner löschen oder neue Unterordner anlegen. Es ist nicht möglich gemeinsame Ordner umzubenennen. Dies kann nur der Eigentümer des Ordners. Zum Löschen von Unterordnern benötigen Sie das "Ordner"-Recht für jeden Unterordner.

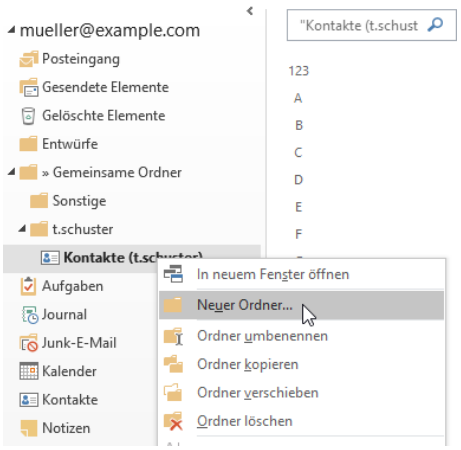
Achtung

Das Anlegen und Verschieben von gemeinsamen Ordnern ist nicht auf der obersten Ordnerebene eines Benutzerkontos möglich. Auch wenn Outlook erlaubt in dieser Ebene Ordner anzulegen, so sind diese nicht mit dem Server verbunden und liegen rein lokal in der Outlook-Datendatei. Beispiel:



Ausschließlich der Eigentümer eines Kontos ist in der Lage Ordner auf der obersten Ordnerebene anzulegen oder dorthin zu verschieben.

Das Anlegen von Ordnern unterhalb eines verbundenen Ordners werden jedoch zum Server synchronisiert. Im Beispiel wird ein neuer Ordner unterhalb von "Kontakte" erstellt.

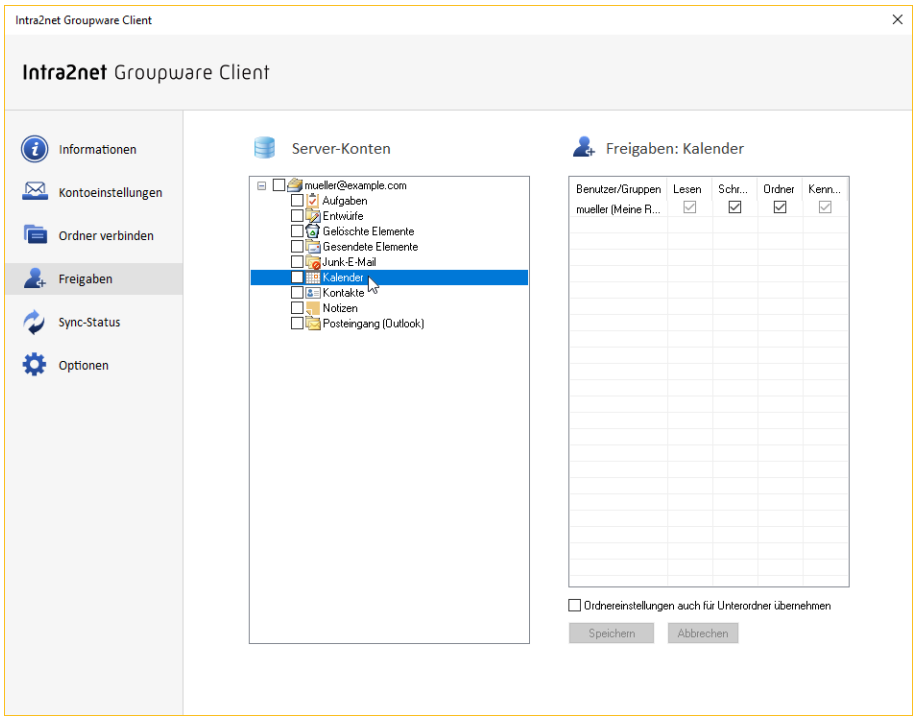


23. Kapitel - Ordner freigeben

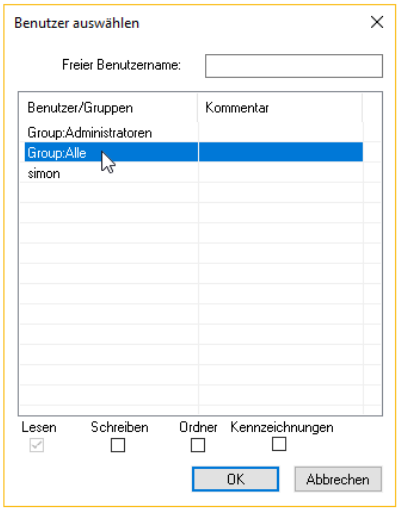
Damit andere Benutzer auf einen Ordner zugreifen können, muss der Eigentümer ihn zuerst wie folgt freigeben:

1. Öffnen Sie das Menü "Groupware Client > Freigaben".

2. Klicken Sie auf der linken Seite (Server-Konten) den freizugebenden Ordner an.



3. Mit einem Doppelklick auf der rechten Seite (Freigaben) öffnen Sie den 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 und schließen den Dialog mit "Ok".

5. Klicken Sie auf "Speichern", um die neuen Rechte auf den Server zu schreiben.

Danach können die anderen Nutzer die freigegebenen Ordner bei sich verbinden wie in Abschnitt 22.2, „Gemeinsame Ordner verbinden“ beschrieben.

Es empfiehlt sich, die Freigaben nicht für einzelne Benutzer, sondern für Benutzergruppen auf dem Intra2net System zu erteilen. Dies vereinfacht die Verwaltung der Freigaben vor allem bei Benutzerfluktuation und Umstrukturierung.

23.1. Rechte

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 für diesen Ordner und darf die Freigaben an andere Benutzer verändern. Zum Löschen von Ordnern mit bestehendem Inhalt benötigt der Benutzer zusätzlich das "Schreiben" Recht.
Kennzeichnungen	Der Benutzer darf die Kennzeichnungen Gelesen, Beantwortet und Markiert 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 exakt so wie beim markierten Ordner eingestellt.

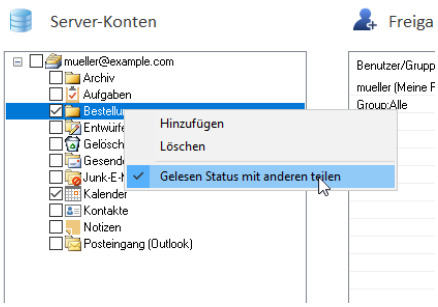
Neu angelegte Ordner übernehmen beim Anlegen immer die Rechte ihres Überordners.

23.2. Gelesen-Status gemeinsam/individuell

Das Intra2net System 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 > Freigaben" eine neue Freigabe an andere Nutzer mit dem Recht "Kennzeichnungen" gesetzt, wird automatisch der gemeinsame Gelesen-Status aktiviert.

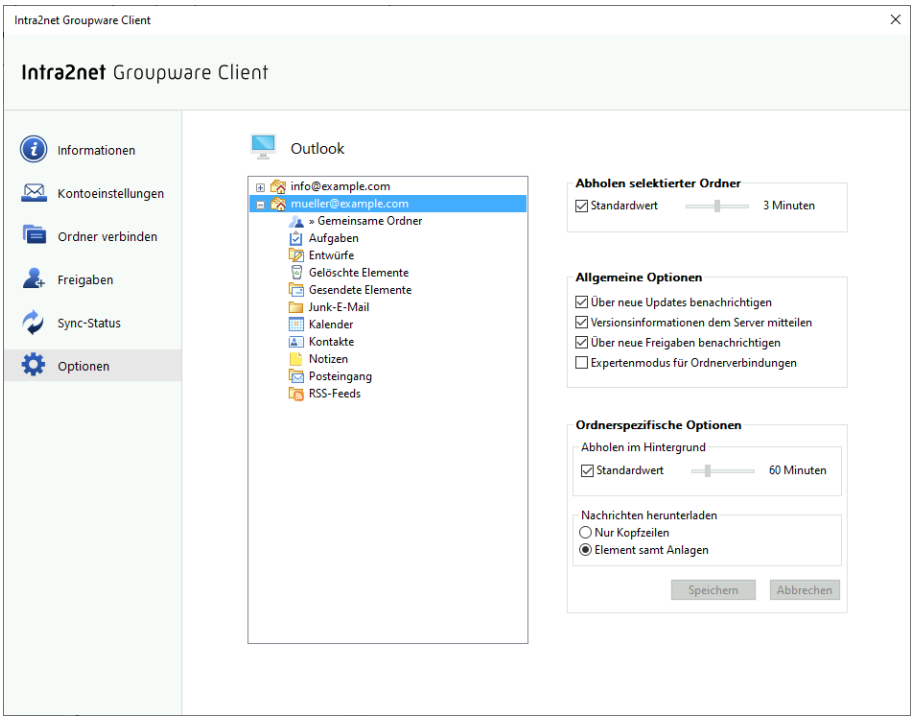
Soll der Gelesen-Status individuell pro Benutzer verwaltet werden, so öffnen Sie das Kontextmenü des Ordners über einen Rechtsklick und schalten die Option "Gelesen Status mit anderen teilen" aus.


Server-Konten
Freiga
mueller@example.com
Archiv
Aufgaben
Hinzufügen
Löschen
Gelesen Status mit anderen teilen
Kalender
Kontakte
Notizen
Posteingang (Outlook)
Benutzer/Grupp
Group:Alle

24. Kapitel - Expertenmodus für Ordnerverbindungen

Der Expertenmodus für Ordnerverbindungen zeigt im Menü "Groupware Client > Ordner verbinden" zwei Ordnerbäume an, einen für das lokale Outlook und einen für die Server-konten. Das ermöglicht sowohl eine feinere Steuerung welche Ordner an welche Stelle verbunden werden sollen, als auch verschiedene Modi beim Umgang mit neuen Unterord-nern.

Der Expertenmodus für Ordnerverbindungen kann über die entsprechende Option im Menü "Groupware Client > Optionen" an- und ausgeschaltet werden:



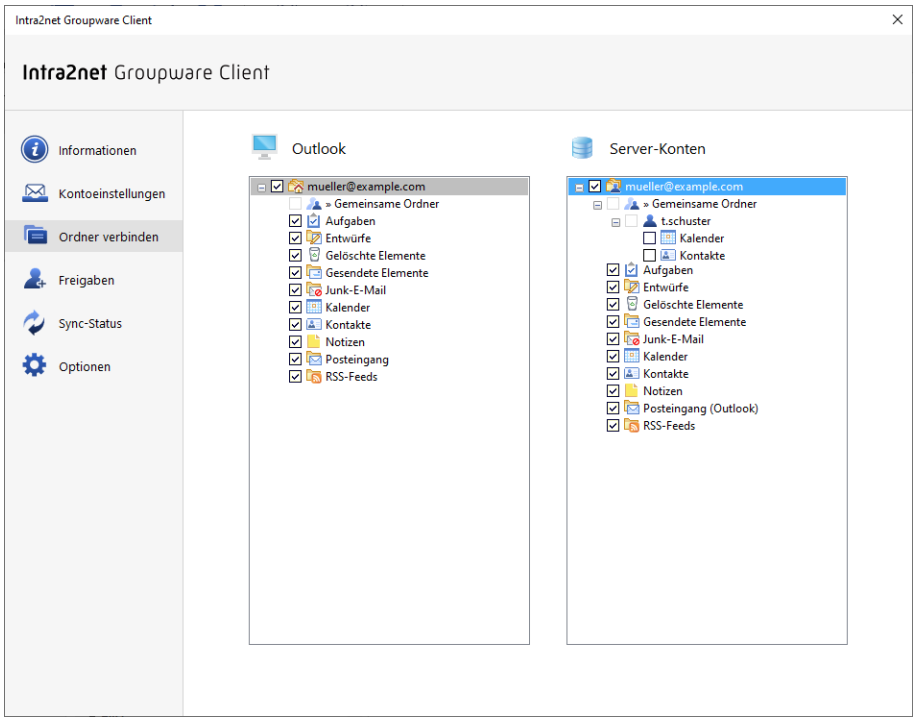
Bis inklusive Intra2net Groupware Client Version 4.0.2 war der Expertenmodus für Ord-nerverbindungen immer aktiv, erst ab Version 5 besteht eine Wahl zwischen den Modi.

24.1. Gemeinsame Ordner verbinden

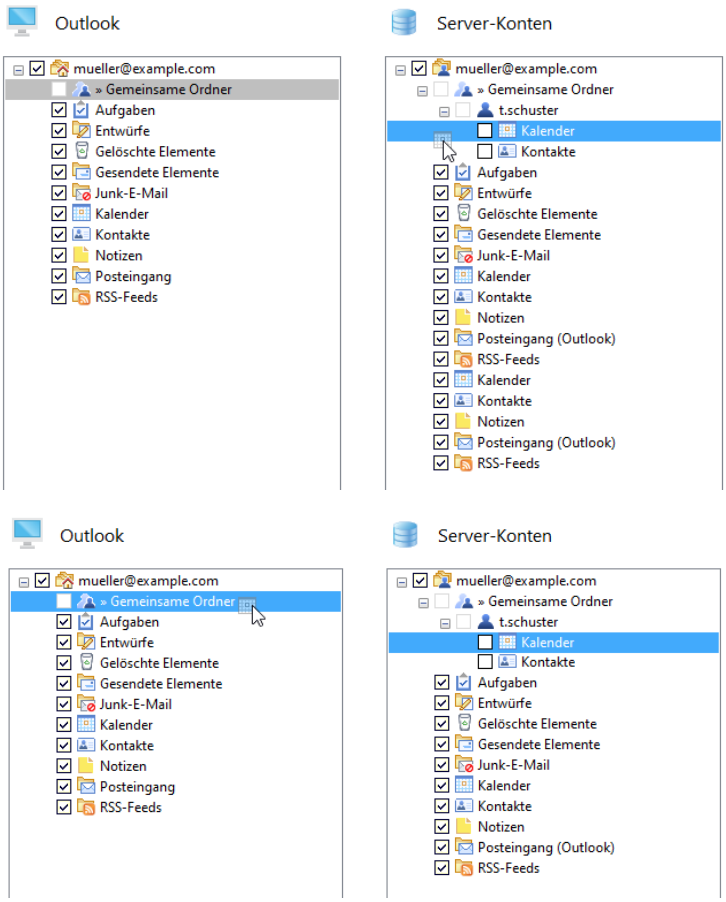
Gehen Sie wie folgt vor, um im Expertenmodus Ordner zu verbinden, die Ihnen andere Benutzer freigegeben haben:

1. Öffnen Sie das Menü "Groupware Client > Ordner verbinden".

2. Auf der rechten Seite (Server-Konten) erscheinen die Ihnen freigegebenen Ordner unterhalb von "»Gemeinsame Ordner".

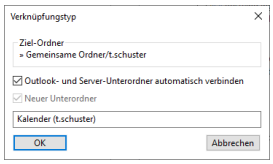


3. Klicken Sie den gewünschten Ordner auf der rechten Seite an und halten Sie die Maustaste gedrückt. Ziehen Sie den Ordner dann mit gedrückter Maustaste auf den Ordner "»Gemeinsame Ordner" auf der linken Seite (Outlook). Lassen Sie dort die Maustaste los.

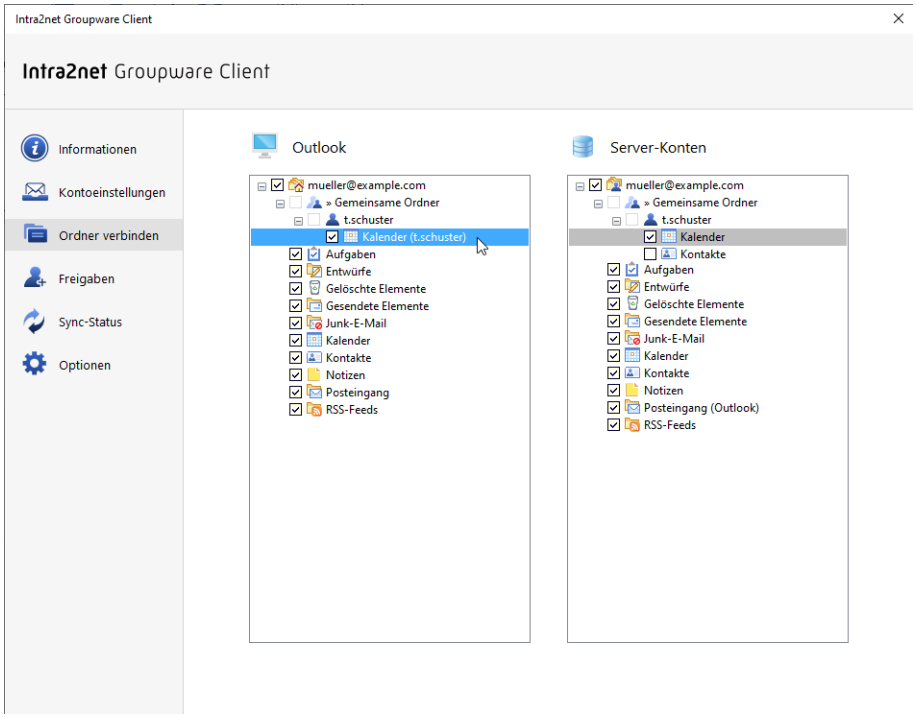


4. Sie werden nun gefragt, wie Sie die Verbindung erstellen möchten. Standardmäßig wird der gewählte Ordner und alle seine freigegebenen Unterordner verbunden. Werden später auf dem Server neue Unterordner erstellt oder freigegeben, werden diese dann auch automatisch verbunden. Alternativ können Sie durch das Abwählen der Option auch nur den einen gewählten Ordner ohne Unterordner verbinden.

   Einige Ordneransichten von Outlook, wie z.B. die Kalenderansicht, zeigen nicht die Ordnerhierarchie an, sondern ausschließlich eine Liste der Ordnernamen. Daher ist es empfehlenwert, diesen Ordnern eindeutige Namen zu vergeben. Der Vorschlag für den Namen des lokalen Ordners enthält daher den Benutzernamen des Eigentümers.



5. Der verbundene Ordner erscheint nun unterhalb von "»Gemeinsame Ordner" und dem Benutzernamen auf der linken Seite (Outlook).



Der Unterschied zwischen Expertenmodus und dem im 22. Kapitel, „Ordner verbinden“ beschriebenen Standardmodus ist, dass die im Expertenmodus verbundenen gemeinsamen Ordner zusätzlich die Möglichkeit bieten auf dem Server neu erstellte Unterordner automatisch mit verbinden zu lassen. Im Standardmodus müssen Sie gemeinsame Ordner immer einzeln verbinden.

Eine weitere Möglichkeit die nur der Expertenmodus bietet ist, den Ordnern lokal einen anderen Namen zu vergeben als auf dem Server. Auch ist es möglich Ordner auf einer anderen Hierarchieebene unterhalb von "»Gemeinsame Ordner" zu verbinden.

Im Expertenmodus ist es auch möglich die Variante der Ordnerverbindung anzulegen wie im Standardmodus. Dafür muss einfach nur die Checkbox vor dem jeweiligen Ordnernamen

auf der Seite "Server-Konten" angeklickt werden anstatt die oben beschriebene Methode per Drag&Drop zu verwenden.

24.2. Ordner manuell verbinden

Normalerweise verbindet der Intra2net Groupware Client die eigenen Ordner automatisch zwischen dem Server und Outlook:

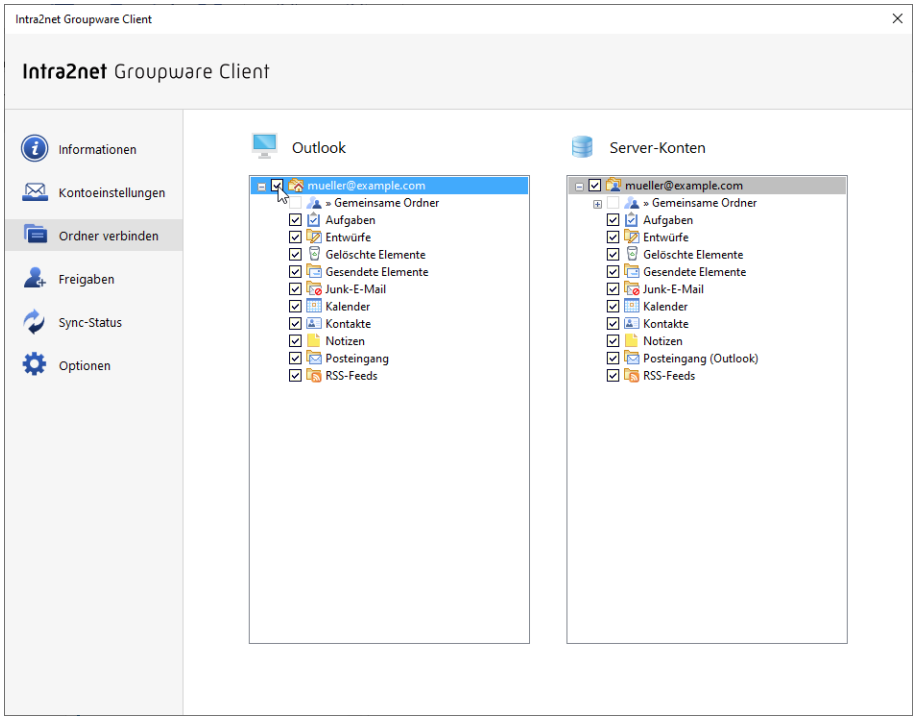
- Auf dem Server neu angelegte eigene Ordner erscheinen automatisch auch in Outlook
- In Outlook angelegte Ordner werden automatisch auf dem Server angelegt und mit diesem verbunden
- Lokal gelöschte Ordner werden auch auf dem Server gelöscht
- Auf dem Server gelöschte Ordner werden auch lokal gelöscht
- 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.

24.2.1. 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 an und entfernen die Checkbox vor dem Namen.



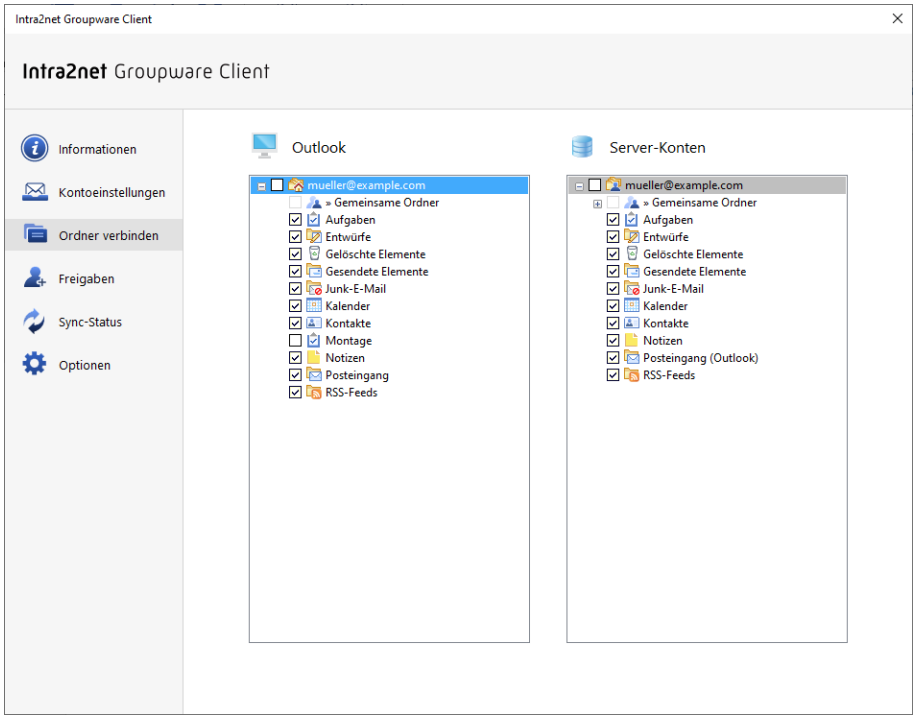
3. Sie werden gefragt ob Sie die Verbindung wirklich aufheben wollen. Antworten Sie mit "OK".

Die einzelnen Unterordner sind zuerst weiterhin verbunden. Und zwar sind die einzelnen Ordner auf der obersten Ordnerebene mit dem Modus "Unterordner automatisch verbinden" verbunden. Wenn lokal oder auf dem Server neue Ordner auf der obersten Ordnerebene anlegt werden, müssen diese 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.

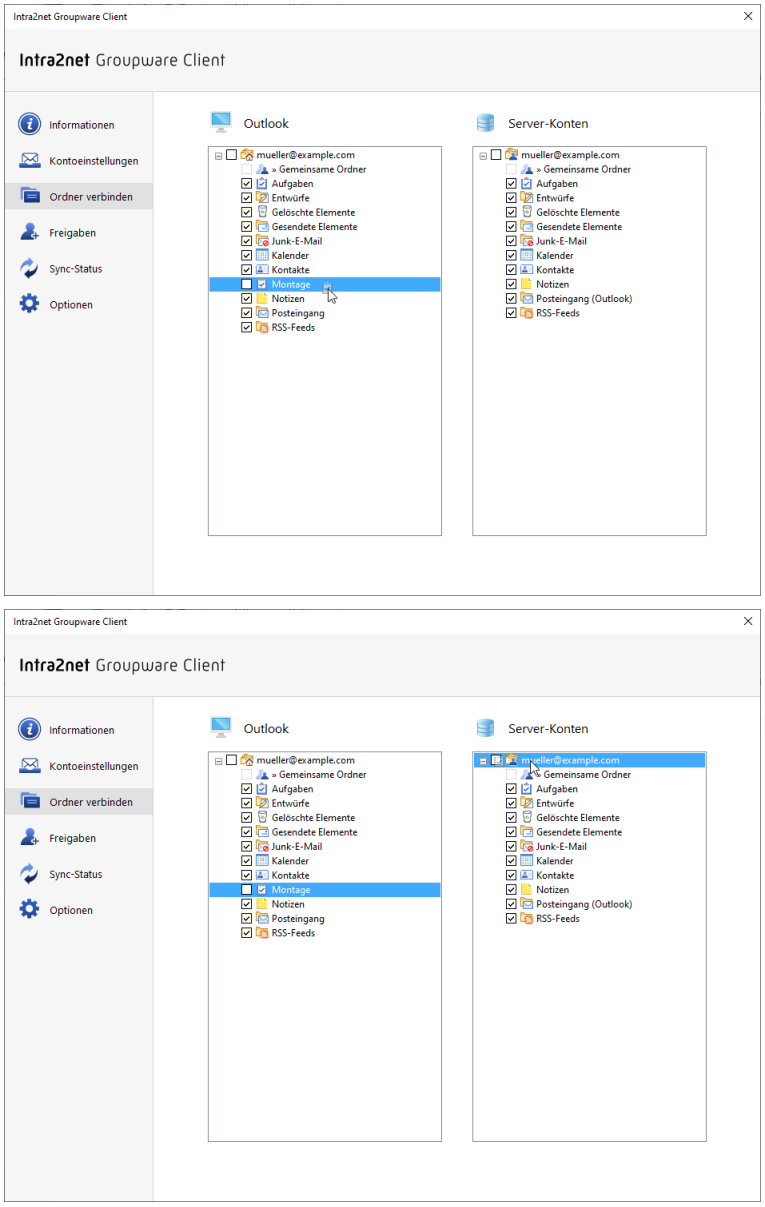
24.2.2. Einen einzelnen Ordner verbinden

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.

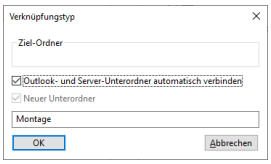


3. Ziehen Sie den gewünschten Ordner auf der Outlook-Seite, hier "Montage", mit gedrückter Maustaste auf den Wurzelordner des Kontos auf der rechten Seite und lassen dort die Maustaste los (Drag & Drop). Befindet sich der zu verbindende Ordner auf dem Server, so ziehen Sie ihn in die andere Richtung.



Sie haben nun die Wahl wie die Verbindung genau gestaltet werden soll:

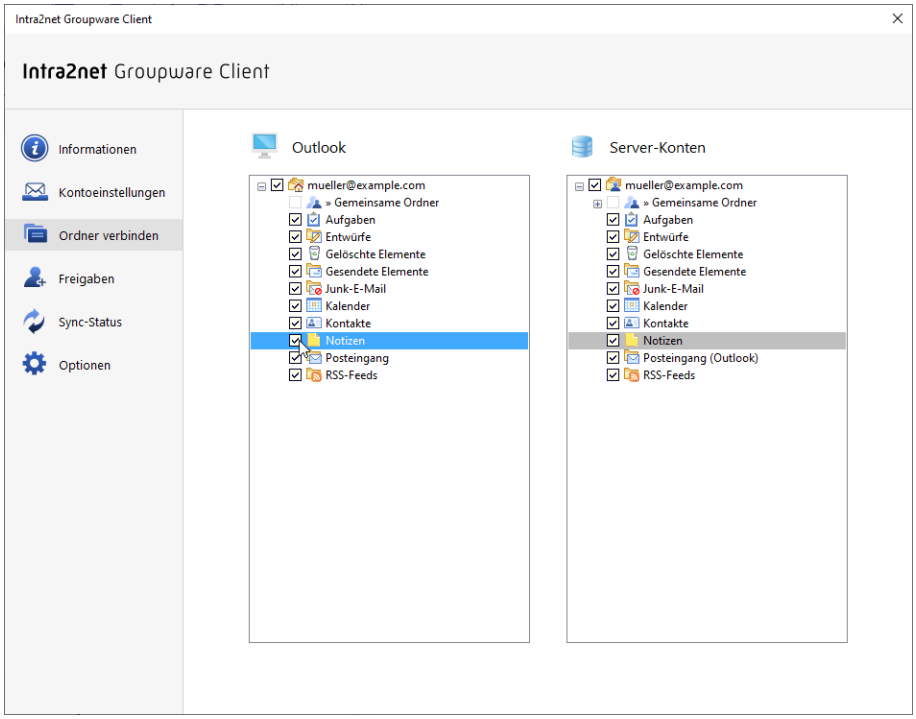
Unterordner automatisch verbinden	Wenn aktiv, wird der Ordner selbst inkl. aller seiner Unterordner verbunden. Werden lokal in Outlook oder auf dem Server neue Ordner hinzugefügt oder gelöscht, wird die Änderung auf die jeweils andere Seite übernommen.
Neuer Unterordner	Wenn aktiviert, wird unterhalb 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 eingestellt werden. Damit können lokal in Outlook und auf dem Server unterschiedliche Namen für denselben Ordner verwendet werden. So kann z.B. der Ordner `Kalender` des Benutzers `meier` lokal in Outlook **`Kalender meier`** genannt werden.



24.2.3. Verbindung eines Ordners aufheben

Um die Verbindung eines Ordners aufzuheben gehen Sie wie folgt vor:

1. Öffnen Sie das Menü "Groupware Client > Ordner verbinden".
2. Klicken Sie auf die Checkbox vor dem Ordnernamen und entfernen den Haken.



3. Bestätigen Sie, dass Sie die Verbindung aufheben wollen.

25. Kapitel - Erweiterte Funktionen

25.1. Ordnerhierarchie und ibx_sub

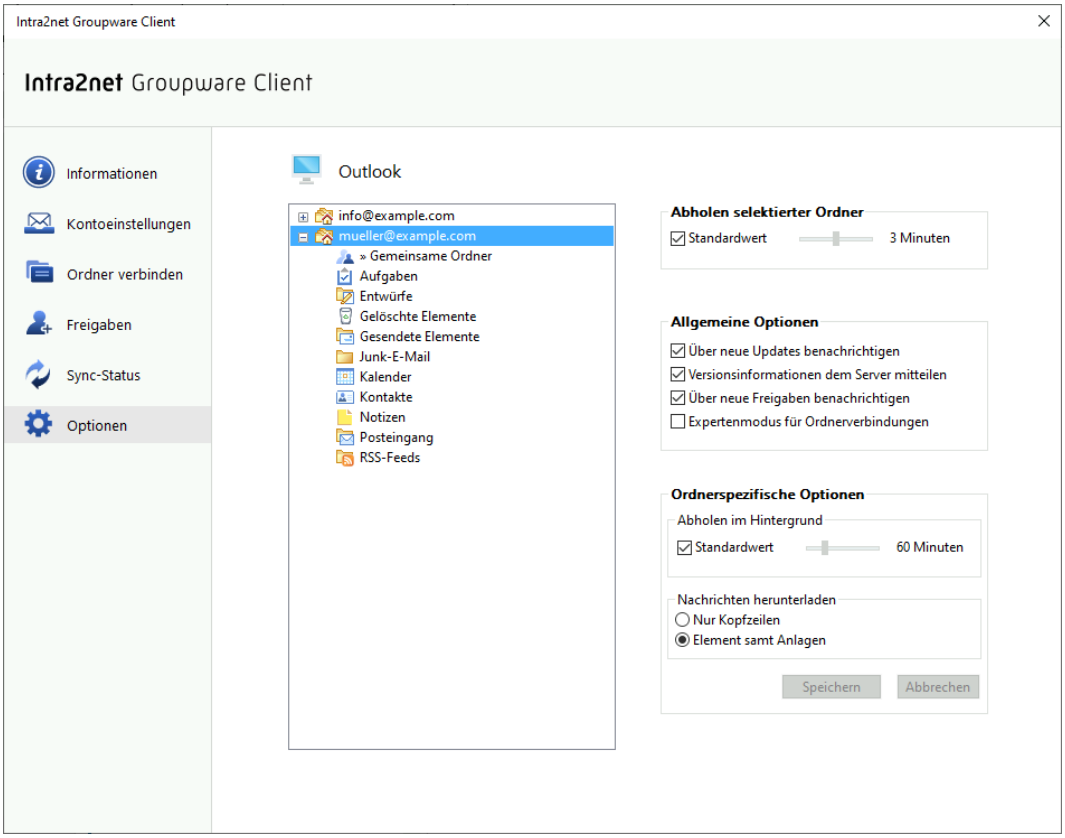
In Outlook wird der Ordner `Posteingang` normalerweise auf derselben Hierarchieebene wie `Kalender`, `Kontakte` etc. angezeigt. Auf dem IMAP-Server ist der `Posteingang` dagegen der Wurzelordner eines Benutzers und alle anderen Ordner wie `Kalender`, `Kontakte` etc. sind Unterordner des Posteingangs.

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.

25.2. Ordneroptionen

Im Menü "Groupware Client > Optionen" können Verbindungsoptionen zu den E-Mail-Konten eingestellt werden. Insbesondere wird hier eingestellt, wie häufig die einzelnen Ordner mit dem Server synchronisiert werden.



Die aktuell in Outlook geöffneten bzw. selektierten Ordner werden standardmäßig im Takt von 3 Minuten aktualisiert. Dieses Intervall kann im Dialog global angepasst werden.

Zusätzlich werden alle Ordner in dem eingestellten Intervall im Hintergrund mit dem Server synchronisiert. Möchten Sie dieses Intervall anpassen, so markieren Sie den Ordner,

deaktivieren die Kontrollfläche "Standardwert" und stellen die gewünschte Zeit ein. Alle Unterordner dieses Ordners übernehmen automatisch die eingestellte Zeit, es sei denn Sie legen explizit einen anderen Wert für einen Unterordner fest.



Achtung

Das Synchronisieren von vielen Ordnern im Hintergrund erzeugt eine deutliche Belastung auf Client und Server. Achten Sie daher unbedingt darauf, dass nur ein oder sehr wenige Ordner pro Benutzer mit kurzem Intervall im Hintergrund synchronisiert werden. Werden alle Ordner im Takt von wenigen Minuten synchronisiert, so kann Outlook träge reagieren sowie der Server bereits von wenigen Benutzern überlastet werden.

Die Einstellungen zu den Updateintervallen hier betreffen nur das Synchronisieren von Änderungen auf dem Server in das lokale Outlook. Lokal in Outlook vorgenommene Änderungen werden zeitnah und ohne Abwarten eines Intervalls auf den Server geschrieben.



Hinweis

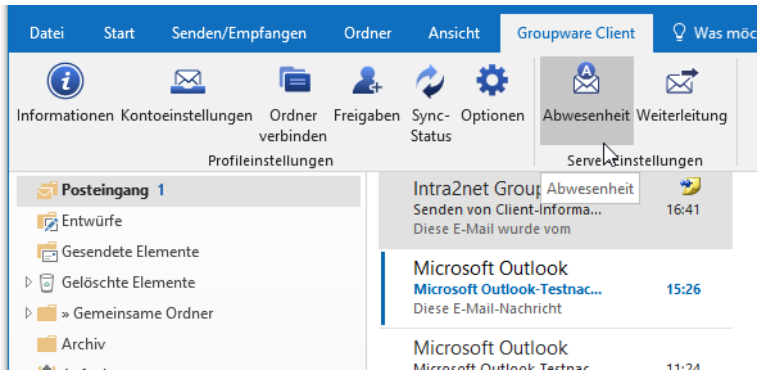
Die Einstellungen zu den Updateintervallen in diesem Menü betreffen nur den Inhalt der Ordner, nicht Änderungen an der Ordnerstruktur. Für die Synchronisation der Ordnerstruktur siehe Abschnitt 22.1.3, „Ordnerliste aktualisieren“.

Über die Registry können noch darüber hinausgehende Einstellungen zur Synchronisation vorgenommen werden. Diese finden Sie in Abschnitt 31.2, „Erweiterte Einstellungen in der Registrierung“ erklärt.

25.3. Serverseitige Einstellungen bearbeiten

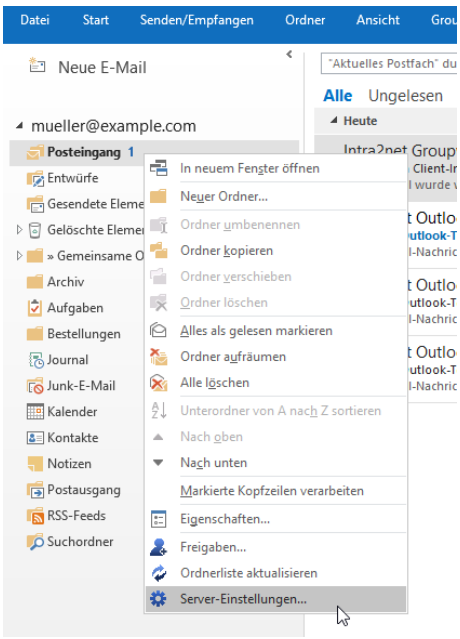
Der Groupware Client bietet eine einfache Möglichkeit für die Benutzer, auf ihre serverseitigen Benutzereinstellungen aus Outlook heraus zuzugreifen. Darüber können u.a. die Funktionen Abwesenheitsschaltung, E-Mail-Weiterleitung, Sortierregeln sowie der benutzerabhängige Spamfilter des Intra2net Systems konfiguriert werden.

Der Zugriff ist über das Office-Menüband "Groupware Client" und dort die entsprechenden Einträge im Bereich "Server-Einstellungen" möglich. Mit diesen Einträgen wird ein Webbrowser geöffnet, der die entsprechenden Menüpunkte auf dem Intra2net System anzeigt. Die Sitzung wird direkt mit den Zugangsdaten des Benutzers geöffnet, ein Login ist nicht notwendig.



Sollten mehrere Server-Konten (Datendateien) konfiguriert sein, wird der Benutzer in einem Dialog gefragt für welches er die Server-Einstellungen öffnen möchte.

Alternativ können die Server-Einstellungen über das Kontextmenü eines jeden Ordners in der Ordnerliste (Rechtsklick auf den Ordnernamen) und dort über die Option "Server-Einstellungen" geöffnet werden.



Bei mehreren Server-Konten werden die Server-Einstellungen für das Konto geöffnet, zu dem der angeklickte Ordner gehört.

Voraussetzung für den Zugriff auf Server-Einstellungen ist natürlich, dass der Administrator des Intra2net Systems 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, indem die Seiten unterhalb von "Benutzermanager > Eigenes Profil" zu den erlaubten Seiten hinzugefügt werden.

Für den Zugriff ist außerdem eine korrekte Konfiguration der SSL-Verschlüsselung notwendig. Gehen Sie bei Fehlern mit der Verschlüsselung wie in Abschnitt 21.1.1.1, „Vorgehen bei Zertifikatsfehlern“ beschrieben vor.

25.4. Kategorien und Farbzuordnung

In Outlook ist es möglich einzelnen Objekten (wie z.B. E-Mails, Terminen oder Kontakten) Kategorien zuzuordnen. Von diesen Kategorien werden zuerst rein die Namen gespeichert und in dieser Form auch durch den Groupware Client auf den Server und andere Outlook-Instanzen synchronisiert. Zusätzlich gibt es in jedem Outlook-Profil eine zentrale (=ordner- und datendateiübergreifende) sog. Hauptkategorienliste. Über diese können den Kategorien Farben zugeordnet werden.

Da jedes Outlook-Profil unterschiedliche Ordner und Konten verbunden haben kann und es somit leicht zu Konflikten zwischen den zugeordneten Farben kommt, ist die Zuordnung von Farben zu den Kategorie-Namen primär eine lokale Konfiguration jedes Outlook-Profils.

Um es dennoch zu ermöglichen auf mehreren Geräten eine weitgehend einheitliche Farbzuordnung zu erreichen, schreibt der Intra2net Groupware Client ab Version 5.0.2 bei neu erstellten oder geänderten Groupware-Objekten die Farbzuordnung mit auf den Server. Beim Hereinsynchronisieren von Groupware-Objekten (nicht E-Mails) mit Katego-

rien und Kategorie-Farbzuordnung vom Server hängt das Vorgehen davon ab, ob der jeweilige Kategorie-Name bereits in der Hauptkategorienliste vorhanden ist oder nicht. Wenn ja, bleibt die bereits bestehende Kategorie unverändert erhalten. Wenn nein, wird die Kategorie neu in der Hauptkategorienliste angelegt und die Farbzuordnung vom Server übernommen.

Diese Vorgehensweise bedeutet, dass die lokale Hauptkategorienliste mit ihrer Farbzuordnung immer Vorrang vor geänderten Farbzuordnungen auf dem Server hat. Der Nutzer kann dadurch eventuelle Farbkonflikte immer leicht bei sich in der lokalen Hauptkategorienliste auflösen.

Außerdem bedeutet es, dass die letztendlich entstehende Farbzuordnung bei Farbkonflikten zwischen verschiedenen Daten auf dem Server von der Reihenfolge abhängt, in der neue Groupware-Objekte mit farbigen Kategorien hereinsynchronisiert werden.

25.4.1. Vorschlag gemeinsame Farbzuordnung

Um für mehrere Arbeitsstationen oder Outlook-Profile eine weitgehend einheitliche Kategorien-Farbzuodnung zu erreichen, wird folgendes Vorgehen empfohlen:

1. Verwenden Sie ein gemeinsam genutztes Konto, siehe z.B. 28. Kapitel, „Konzept für öffentliche Ordner“.

2. Legen Sie darin einen neuen Aufgabenordner an, Name z.B. **`Farbkategorien`**, und geben den Ordner für alle Benutzer zum Lesen frei (siehe 23. Kapitel, „Ordner freigeben“).

3. Legen Sie in diesem Aufgabenordner eine Aufgabe, Titel z.B. **`Standardkategorien`**, an.

4. Machen Sie einen Doppelklick auf die Aufgabe um sie in einem separaten Fenster zu öffnen. Öffnen Sie das Menü der Hauptkategorienliste.

5. Legen Sie alle gewünschten Kategorien mit der jeweiligen Farbzuordnung in der Hauptkategorienliste an.

6. Weisen Sie dieser einen Aufgabe alle gemeinsam genutzten Kategorien zu und speichern sie.

7. Alle Nutzer, die die gemeinsame Farbzuordnung nutzen sollen, verbinden nun in ihrem Outlook-Profil den Aufgabenordner mit den Standardkategorien, siehe 22. Kapitel, „Ordner verbinden“.

Sollten in einigen Outlook-Profilen bereits die in den Standardkategorien abgelegten Kategorie-Namen in der Hauptkategorienliste bestehen, aber andere Farben zugeordnet haben, gehen Sie bei diesen Outlook-Profilen vor wie im nächsten Abschnitt beschrieben um die Farbzuordnung zurückzusetzen.

25.4.2. Lokale Farbzuordnung zurücksetzen

Mit den folgenden Schritten können Sie die komplette Hauptkategorienliste und Farbzuordnung eines Outlook-Profils zurücksetzen und frisch aus einem gemeinsam genutzten Ordner (siehe vorheriger Abschnitt) importieren:

1. Schließen Sie Outlook und warten bis der Outlook-Prozess vollständig beendet ist.

2. Öffnen Sie das Windows Startmenü.

3. Geben Sie als Befehl ein **`outlook.exe /cleancategories`** und führen den Befehl mit Enter aus.

4. Outlook startet in einem speziellen Modus und löscht dabei alle Einträge und Farbzuordnungen aus der Hauptkategorienliste. Die einzelnen Groupwareobjekte behalten ihre Kategoriezuordnungen (also die Kategorie-Namen) unverändert.

5. Öffnen Sie das Menü "Groupware Client > Ordner verbinden".

6. Ist der Ordner mit den gemeinsam genutzten Kategorien (siehe Abschnitt 25.4.1, „Vorschlag gemeinsame Farbzuordnung“) bereits verbunden, so entfernen Sie die Verbindung. Warten Sie kurz bis die Aktion von Outlook vollständig umgesetzt ist.

7. Verbinden Sie den Ordner mit den gemeinsam genutzten Kategorien erneut. Dadurch werden die enthaltenen Daten neu vom Server hereinsynchronisiert und die enthaltenen Kategorien in die Hauptkategorienliste übernommen.

25.4.3. Ändern einer vorhandenen Farbzuordnung

Im Folgenden wird der Prozess beschrieben, mit dem eine bestehende Kategorie-Farbzuordnung netzwerkweit einheitlich für mehrere Benutzer geändert werden kann.

Da es bei unterschiedlichen Farbzuordnungen für die selbe Kategorie wie beschrieben von der Reihenfolge abhängt in der neue Objekte hereinsynchronisiert werden und der Nutzer z.B. beim Einrichten eines neuen Outlook-Profils nur wenig Einfluss auf diese Reihenfolge hat, müssen für eine stabile Farbzuordnung alle Objekte angepasst werden denen die jeweilige Kategorie zugeordnet ist. Das Ändern der Kategorie-Farbzuordnung gilt dabei für Outlook nicht als Änderung der jeweiligen Objekte und löst daher auch kein Schreiben der Objekte mit neuer Farbzuordnung auf den Server aus. Daher sind folgende Schritte notwendig um eine vorhandene Farbzuordnung dauerhaft und auch für neu eingerichtete Outlook-Profile zu ändern:

1. Schließen Sie Outlook auf allen mit dem Intra2net System verbundenen Arbeitsstationen und stellen sicher, dass es geschlossen bleibt. Bedenken Sie dabei auch Homeoffice-Arbeitsplätze, Mobilgeräte und ähnliches.

2. Starten Sie Outlook auf einer Arbeitsstation mit einem Outlook-Profil, welches Schreibzugriff auf den zentralen Farbkategorien-Ordner (siehe Abschnitt 25.4.1, „Vorschlag gemeinsame Farbzuordnung“) hat.

3. Gehen Sie in den zentralen Farbkategorien-Ordner und öffnen dort die Aufgabe für die Standardkategorien mit einem Doppelklick in einem separatem Fenster.

4. Öffnen Sie das Menü der Hauptkategorienliste.

5. Weisen Sie der bestehenden Kategorie die neu gewünschte Farbe zu.

6. Benennen Sie die Kategorie um, indem Sie z.B. eine Zahl an den Namen anhängen.

7. Wiederholen Sie die letzten beiden Schritte für alle anderen Kategorien denen Sie auch eine neue Farbe zuordnen möchten.

8. Verlassen Sie den Kategorienlistendialog mit "Ok". Warten Sie bis Outlook die Umbenennung der Kategorie umgesetzt hat. Die Dauer dafür hängt von der Anzahl der betroffenen Objekte und der Größe der Datendateien ab.

9. Öffnen Sie erneut die Hauptkategorienliste und benennen die Kategorie wieder auf ihren ursprünglichen Namen zurück. Verlassen Sie den Kategorienlistendialog mit "Ok" und warten bis Outlook mit der Umbenennung fertig ist.

10. Warten Sie bis die Änderungen der lokalen Objekte durch den Groupware Client auf den Server geschrieben wurden. Verwenden Sie dafür die Anzeige im Menü "Groupware Client > Sync-Status".

11. Schließen Sie Outlook auf dieser Arbeitsstation und stellen sicher dass es geschlossen bleibt.

Gehen Sie danach eine Arbeitsstation im Netz nach der anderen durch und führen dort folgende Schritte durch. Bedenken Sie dabei auch Homeoffice-Arbeitsplätze, Mobilgeräte und ähnliches.



Achtung

Achten Sie sorgfältig darauf, dass dabei zu jeder Zeit immer nur eine Arbeitsstation Outlook geöffnet haben darf. Ansonsten können dort die umbenannten Kategorien fälschlicherweise mit in die Hauptkategorienlisten übernommen werden.

1. Führen Sie die in Abschnitt 25.4.2, „Lokale Farbzuordnung zurücksetzen“ beschriebenen Schritte durch.

2. Öffnen Sie das Menü der Hauptkategorienliste.

3. Benennen Sie alle Kategorien, denen eine neue Farbe zugewiesen werden soll um, indem Sie z.B. eine Zahl an den Namen anhängen.

4. Verlassen Sie den Kategorienlistendialog mit "Ok". Warten Sie bis Outlook die Umbenennung der Kategorie umgesetzt hat. Die Dauer dafür hängt von der Anzahl der betroffenen Objekte und der Größe der Datendateien ab.

5. Öffnen Sie erneut die Hauptkategorienliste und benennen die Kategorie wieder auf ihren ursprünglichen Namen zurück. Verlassen Sie den Kategorienlistendialog mit "Ok" und warten bis Outlook mit der Umbenennung fertig ist.

6. Warten Sie bis die Änderungen der lokalen Objekte durch den Groupware Client auf den Server geschrieben wurden. Verwenden Sie dafür die Anzeige im Menü "Groupware Client > Sync-Status".

7. Schließen Sie Outlook auf dieser Arbeitsstation und stellen sicher dass es geschlossen bleibt.

Wurde der Vorgang auf der letzten Arbeitsstation abgeschlossen, sind die Farbzuordnungen in allen Outlook-Profilen und in allen Objekten auf dem Server einheitlich angepasst. Jetzt kann Outlook wieder auf allen Arbeitsstationen normal genutzt werden.

25.5. 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.

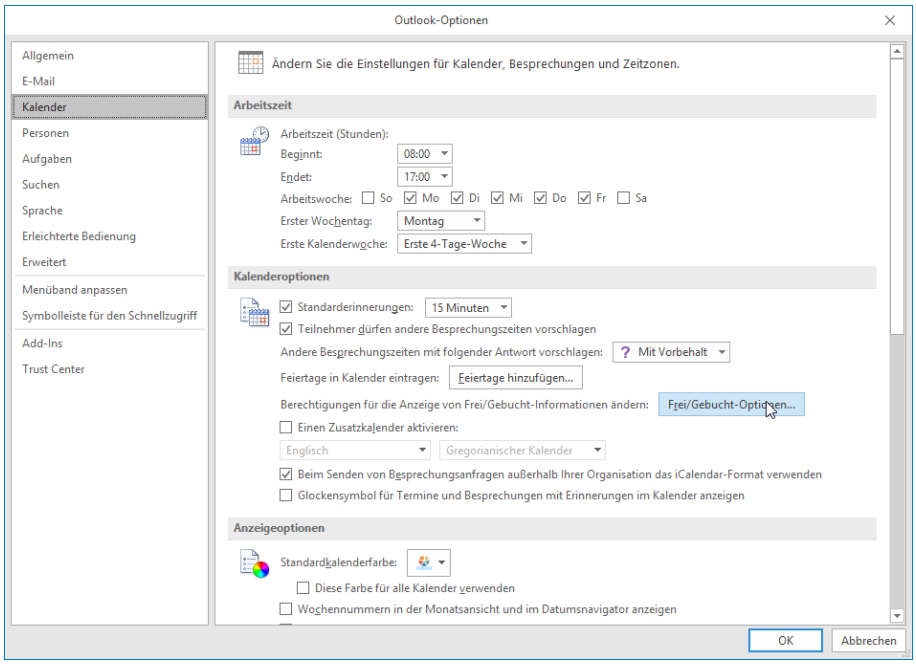
Bevor Sie die Frei-/Gebucht-Daten nutzen können, müssen Sie zuerst die korrekte Adresse zum Abruf der Daten in Outlook hinterlegen. Gehen Sie dazu wie folgt vor:

25.5.1. Outlook 2010 bis 2021

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.

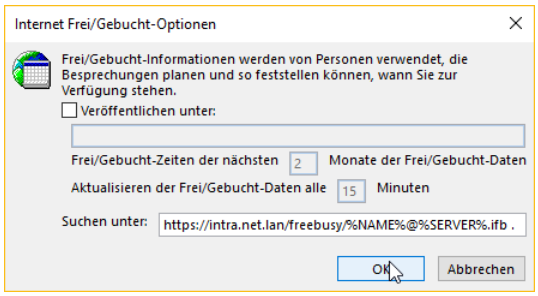


4. Tragen Sie den Suchpfad bei "Suchen unter" ein.

   Die Adresse lautet **`https://intra.net.lan/freebusy/%NAME%@%SERVER%.ifb`**.

   Verwenden Sie den Namen Ihres Intra2net Systems und geben die Adresse ansonsten genau so wie hier gezeigt ein.

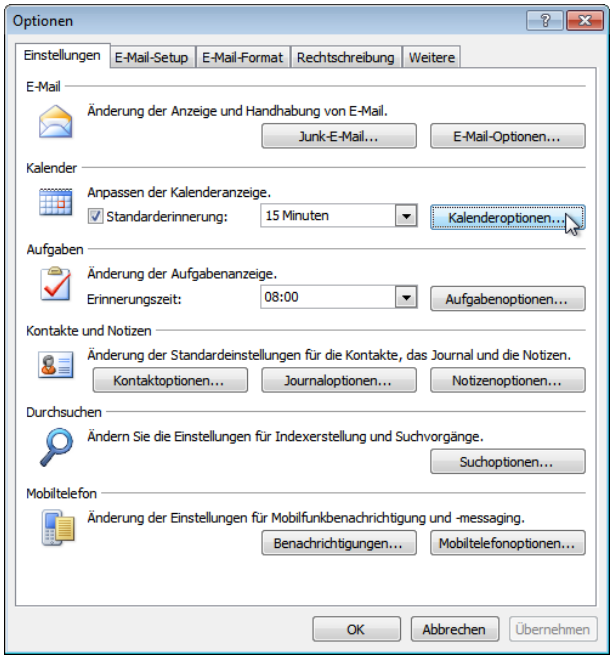
   Da das Intra2net System die Frei/Gebucht-Informationen automatisch erzeugt, darf das Kontrollkästchen "Veröffentlichen unter" nicht gesetzt sein.



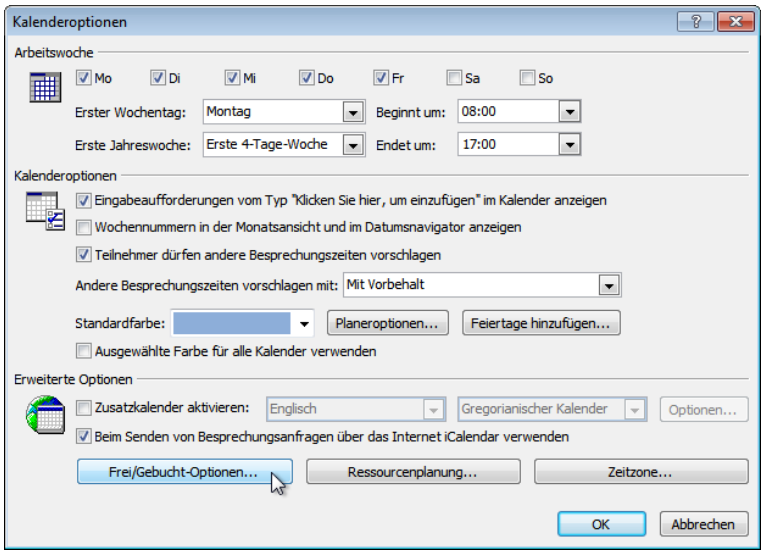
25.5.2. Outlook 2007

1. Wählen Sie in Outlook im Menü "Extras" den Punkt "Optionen" aus.

2. Klicken Sie auf die Schaltfläche "Kalenderoptionen".



3. Wählen Sie nun die Schaltfläche "Frei/Gebucht-Optionen" aus.

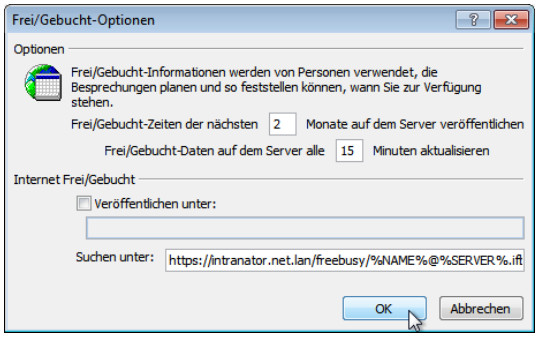


4. Tragen Sie den Suchpfad bei "Suchen unter" ein.

Die Adresse lautet **`https://intra.net.lan/freebusy/%NAME%@%SERVER%.ifb`**.

Verwenden Sie den Namen Ihres Intra2net Systems und geben die Adresse ansonsten genau so wie hier gezeigt ein.

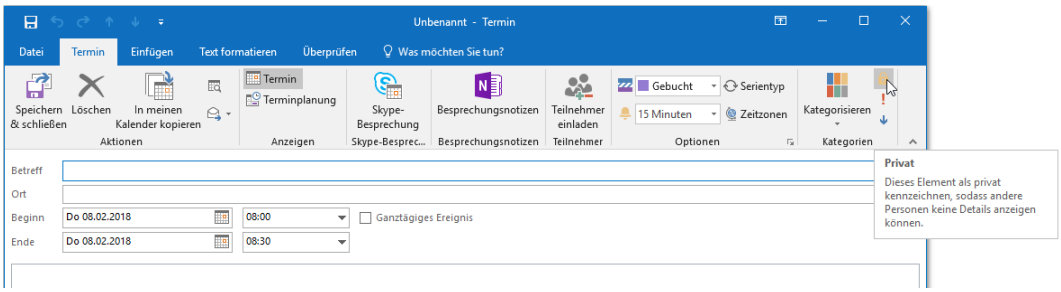
Da das Intra2net System die Frei/Gebucht-Informationen automatisch erzeugt, darf das Kontrollkästchen "Veröffentlichen unter" nicht gesetzt sein.



25.6. 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, der den Zustand ursprünglich auf "Privat" gesetzt hat.

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 31.2.1, „Einstellungen für den Store“.

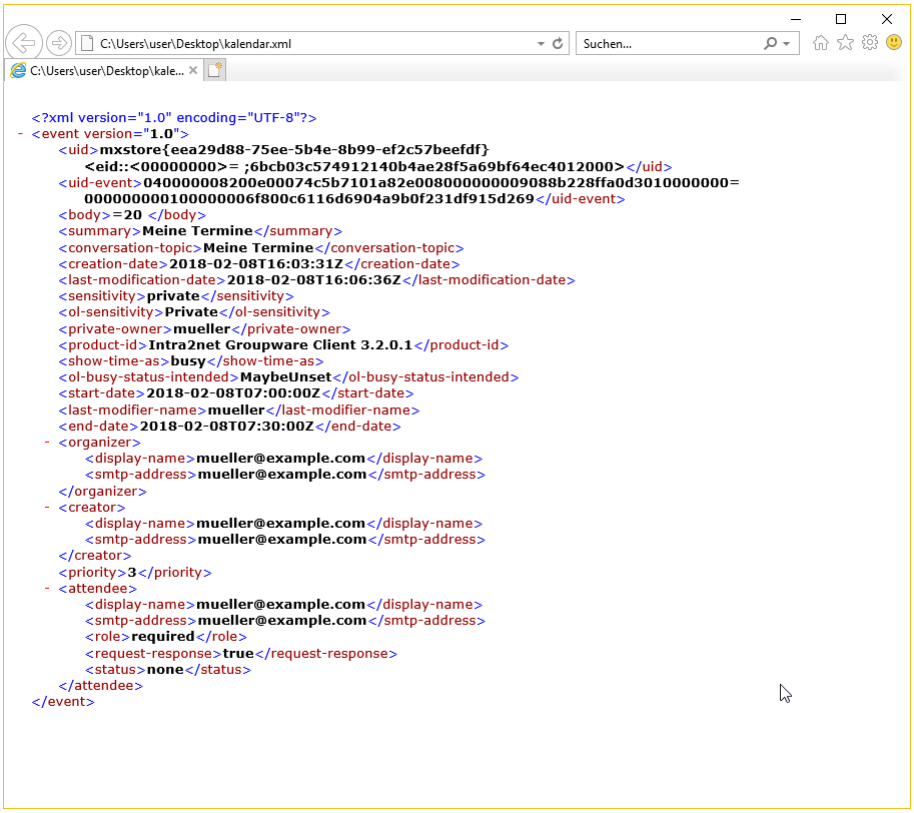




Achtung

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.



Wie man sieht, sind neben einigen nicht intuitiv deutbaren Informationen alle relevanten Daten des Termins im Klartext lesbar.

Als sichere Alternative bietet es sich daher an, statt dessen für private Daten einen separaten Ordner anzulegen und diesen nicht freizugeben.

25.7. 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 Groupwareobjekt beliebig Erinnerungen setzen und diese erscheinen zur Fälligkeit nur bei ihm selbst. Zur Identifikation des Benutzers wird dabei das Benutzerlogin verwendet, die Erinnerungen funktionieren also auch, wenn ein Benutzer unterschiedliche PCs 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.

Über die Werte **`InitialReminderSetting`** und **`ReminderChangesHandling`** in der Registry kann das Verhalten verändert werden. Details finden Sie in Abschnitt 31.2, „Erweiterte Einstellungen in der Registrierung“.

25.8. 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 31.2, „Erweiterte Einstellungen in der Registrierung“).

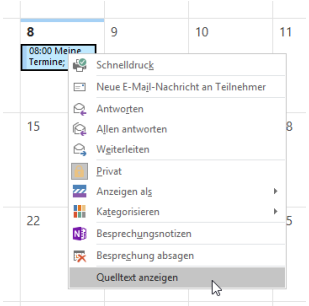
Mit dem Intra2net Groupware Client wird eine Beispieldatei als `userdefined_sync_fields_template.xml` mitgeliefert, die eine genaue Beschreibung und Beispiele enthält, wie benutzerdefinierte Felder definiert werden. Kopieren Sie diese Musterdatei auf `userdefined_sync_fields.xml` und öffnen sie mit einem 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.

25.9. Anzeige des Quelltexts 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".



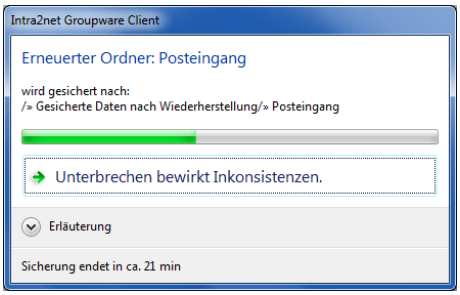
25.10. Sicherungsordner

Werden durch Wiederherstellen von Backups auf dem Server bzw. Verbindungsoperationen mit dem Server lokale Elemente gelöscht, sichert der Intra2net Groupware Client die ursprünglichen Versionen in spezielle Ordner. Im Folgenden werden die verschiedenen Arten von Sicherungsordnern für diese Funktion vorgestellt.

25.10.1. Gesicherte Daten nach Wiederherstellung

Wird auf dem Server ein Ordner gelöscht und durch einen neuen Ordner mit demselben Namen ersetzt, wird dies vom Groupware Client erkannt (anhand der internen *UIDVALIDITY*-Kennung von IMAP). Dies findet vor allem dann statt, wenn auf dem Server ein Backup wiederhergestellt wurde, welches die bisherigen Daten des Benutzers ersetzt.

Es werden dann alle lokalen Elemente in Sicherungsordner verschoben. Dieser Vorgang darf vom Nutzer nicht unterbrochen werden, da es sonst zu Inkonsistenzen in der Datendatei kommt. Darauf wird der Nutzer mit einem Dialog hingewiesen.



Es wird ein Ordner "Gesicherte Daten nach Wiederherstellung" in Outlook angelegt. Darunter befinden sich dann die Sicherungsordner mit dem Namen des ursprünglichen Ordners und einem Zeitstempel. Der Zeitstempel gibt den Zeitpunkt an, zu dem der Groupware Client die Ordnerwiederherstellung auf dem Server erkannt hat und nicht den Zeitpunkt, zu dem die Ordnerwiederherstellung auf dem Server stattgefunden hat.

Wurden die lokalen Sicherungsordner fertig angelegt, können die Daten frisch vom Server synchronisiert werden. Um den Server nicht zu überlasten, passiert dies zuerst nicht vollautomatisch für alle Ordner, sondern nur für die, die der Nutzer in Outlook öffnet. Alternativ kann der Nutzer Outlook neu starten. In der neuen Outlook-Sitzung greift wieder das normale Verhalten des Groupware Clients mit Synchronisierung aller Ordner im Hintergrund.

Die Sicherungsordner auf dem Client werden nicht automatisch gelöscht. Nach dem Wiederherstellen eines Backups auf dem Server empfehlen wir daher, einige Tage abzuwarten und die Benutzer dann zu befragen, ob ihre Daten vollständig sind. Danach sollten die Sicherungsordner manuell auf allen Clients gelöscht werden.

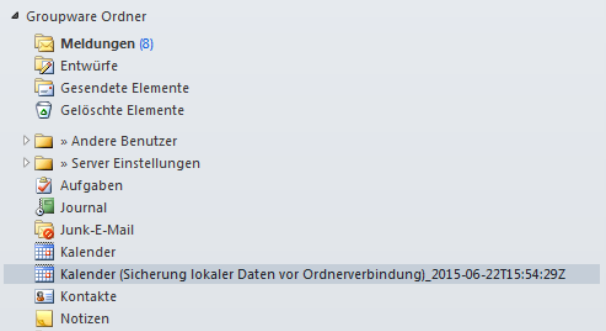


25.10.2. Sicherung lokaler Daten beim Zurückstellen auf Automatik

Werden Ordner neu verbunden, muss ein lokal existierender Ordner leer sein, bevor er mit einem auf dem Server vorhandenen Ordner verbunden werden kann. Ist der lokale Ordner nicht leer, bekommt der Benutzer normalerweise die Möglichkeit, entweder den Verbindungsvorgang abzubrechen oder die lokal vorhandenen Daten zu löschen.

Wird vom Modus manuelles Verbinden wieder auf automatisches Verbinden der Ordner zurückgeschaltet (zurück von dem in Abschnitt 24.2.1, „Umstellen auf Manuelles Verbinden“ beschriebenen), betrifft dies eine Vielzahl von Ordnern. Daher werden in diesem Fall von den lokal vorhandenen Daten Sicherungsordner erstellt. Diese erscheinen lokal auf der selben Hierarchieebene wie der verbundene Ordner. Er bekommt "(Sicherung lokaler Daten vor Ordnerverbindung)" und einen Zeitstempel als Kennung angehängt.

Dieser Sicherungsordner enthält alle Daten, die vor dem Erstellen der Verbindung im lokalen Ordner vorhanden waren. Wir empfehlen, dass der Benutzer diesen Sicherungsordner manuell durchgeht und auf dem Server fehlende Daten per Drag&Drop in den jetzt mit dem Server verbundenen Ordner verschiebt. Danach sollte der Sicherungsordner auf dem Client gelöscht werden. Der Sicherungsordner wird auf dem Client nicht automatisch gelöscht.



25.11. Hinweise an den Benutzer

Der Groupware Client informiert den Nutzer über besondere Ereignisse, Fehler etc. in dem er E-Mails an den Benutzer im Posteingang anlegt. Diese E-Mails sind durch den speziellen Absender "Intra2net Groupware Client" gekennzeichnet.

Beispielsweise werden solche Hinweise erzeugt, wenn neue Freigaben für den Benutzer bereitstehen:



Die Hinweise zu neuen Freigaben können über die Einträge ACL_ChangeNotification in der Registry konfiguriert werden. Siehe hierzu Abschnitt 31.2.1, „Einstellungen für den Store“.

Die E-Mails mit Hinweisen werden im Groupware Client nur lokal gespeichert und werden nicht auf den Server synchronisiert.

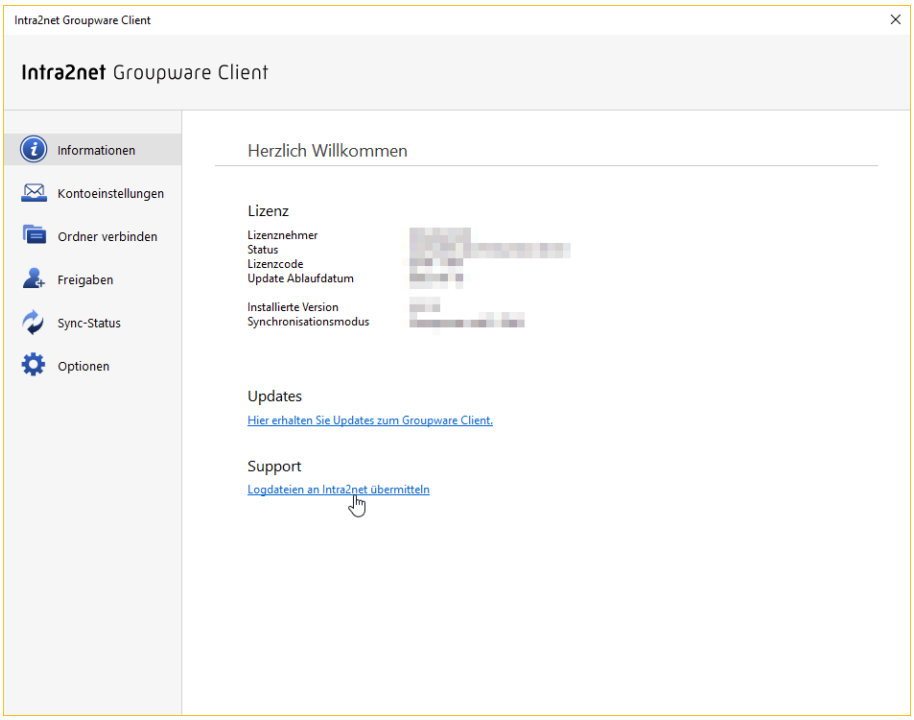
25.12. Logdateien

Der Groupware Client protokolliert standardmäßig interne Details zur den Konten, den Freigaben, der Datensynchronisation und Aktionen des Nutzers. Diese Daten sind im Fehlerfall die Grundlage zur Rekonstruktion des Geschehens, den möglichen Ursachen und evtl. der Wiederherstellung von Daten.

Die Logdateien werden standardmäßig in `%LOCALAPPDATA%\Intra2net`, welches üblicherweise auf das versteckte Verzeichnis `AppData\Local\Intra2net` unterhalb des Profilverzeichnisses des Benutzers verweist, abgelegt. Die Dateien werden täglich, oder wenn Sie 170 MB überschritten haben, rotiert und für standardmäßig 14 Tage aufbewahrt. Die Standardwerte und der Umfang der Logs können über die Registry angepasst werden, siehe Abschnitt 31.2, „Erweiterte Einstellungen in der Registrierung“.

25.12.1. Übermitteln von Logdateien an den Support

Werden Sie vom Intra2net Support dazu aufgefordert die Logdateien des Groupware Clients einzusenden, geht dies am einfachsten über eine spezielle Funktion im Menü "Groupware Client > Informationen". Sie benötigen dafür die Ticketnummer des Supportfalls.



26. Kapitel - Erweiterte E-Mail-Konfiguration

26.1. E-Mails komplett oder nur Kopfzeilen abrufen

Über die Schaltfläche "Nachrichten herunterladen" im Menü "Groupware Client > Optionen" können Sie festlegen, ob neue E-Mails in einem Ordner sofort komplett abgerufen werden sollen oder vorerst nur die Kopfzeilen. Sobald eine E-Mail, von der bisher nur die Kopfzeilen vorliegen, vom Nutzer in Outlook angeklickt und geöffnet wird, beginnt im Hintergrund automatisch das Herunterladen des vollständigen Inhalts.

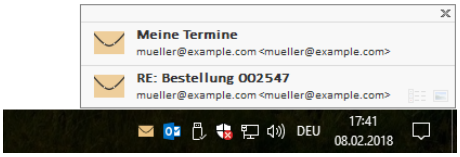
Sie können für jeden E-Mail-Ordner individuell festlegen, ob neue E-Mails immer vollständig heruntergeladen werden oder nur die Kopfzeilen. Die Standardeinstellung für neu verbundene Ordner ist "Element samt Anlagen". Sie können die Standardeinstellung verändern, indem Sie die Einstellung für den Wurzelordner anpassen.

Vorteil des Herunterladens nur als Kopfzeilen ist der deutlich geringere Platzbedarf in der Datendatei auf dem lokalen System. Eine kleinere Datendatei hat häufig auch eine schnellere Reaktionsgeschwindigkeit von Outlook zur Folge.

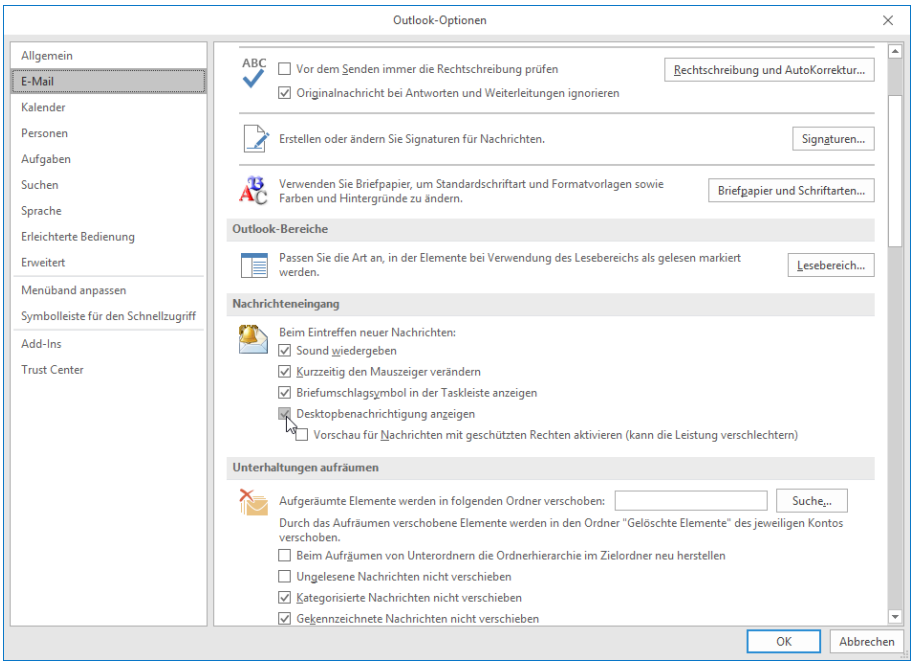
Nachteil des Herunterladens nur als Kopfzeilen ist, dass Outlook nicht im Inhalt der noch nicht vollständig heruntergeladenen E-Mails suchen kann. Auch wird zum Lesen der E-Mail immer eine Verbindung zum Intra2net System benötigt. Das Verschieben oder Kopieren von E-Mails in eine andere Datendatei oder einen Ordner eines anderen Server-Kontos ist erst möglich, sobald die E-Mail lokal vollständig vorliegt.

26.2. Benachrichtigung über neue E-Mails

Der Benutzer kann mit Desktopbenachrichtigungen über das Eintreffen neuer E-Mails in einem der Posteingangsordner benachrichtigt werden. Diese erscheinen unten rechts im Bildschirm und enthalten Absender und Betreff der neuen E-Mails.



Die Desktopbenachrichtigung können über das Menü "Datei", "Optionen", "E-Mail", Abschnitt "Nachrichteneingang" aktiviert oder deaktiviert werden.



Die Desktopbenachrichtigung zeigt maximal 3 neue E-Mails an. Treffen innerhalb von 60 Sekunden nach Anzeige der letzten Desktopbenachrichtigung weitere neue E-Mails ein, so wird für diese keine weitere Desktopbenachrichtigung angezeigt um den Benutzer nicht mit zu vielen Benachrichtigungen abzulenken. Für E-Mails, die bereits als gelesen markiert sind, wird keine Benachrichtigung angezeigt. Ebenso für E-Mails, die schon länger als 2 Stunden auf dem Server liegen.

Diese Werte können über die Registry angepasst werden, siehe Abschnitt 31.2.2, „Einstellungen für das Add-In“.

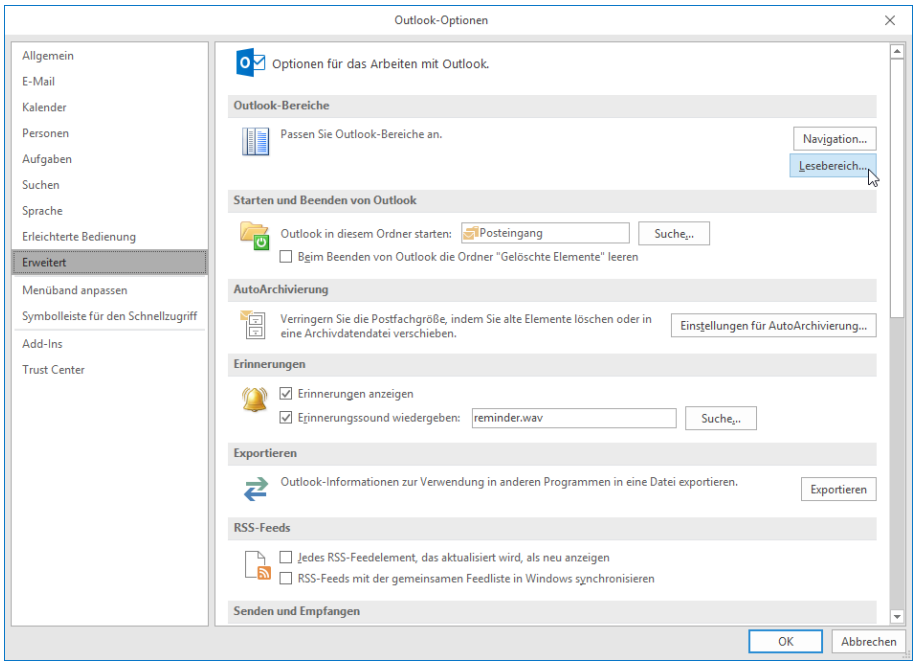
26.3. Gelesen-Markierung bei verschobenen E-Mails

Standardmäßig werden in Outlook E-Mails als gelesen markiert, sobald eine E-Mail in der Vorschau angezeigt wurde und danach eine andere E-Mail selektiert wird. Wird aber nicht direkt die nächste E-Mail selektiert, sondern die aktuell angezeigte E-Mail in einen anderen Ordner verschoben, so wird die noch als ungelesen markierte E-Mail verschoben. Die verschobene E-Mail bleibt dann weiterhin als ungelesen markiert, auch wenn eine andere E-Mail selektiert wird.

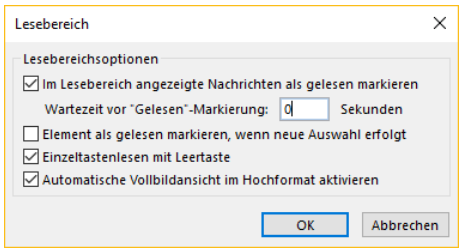
Um dieses Verhalten zu umgehen, stellen Sie die Optionen für die Gelesen-Markierung wie folgt um:

1. Öffnen Sie das Menü "Datei", "Optionen", Reiter "Erweitert".

2. Öffnen Sie in "Outlook-Bereiche" den Unterpunkt "Lesebereich".



3. Aktivieren Sie die Option "Im Lesebereich angezeigte Nachrichten als gelesen Markieren" und wählen eine Wartezeit von z.B. 0 Sekunden für ein sofortiges Markieren als gelesen.



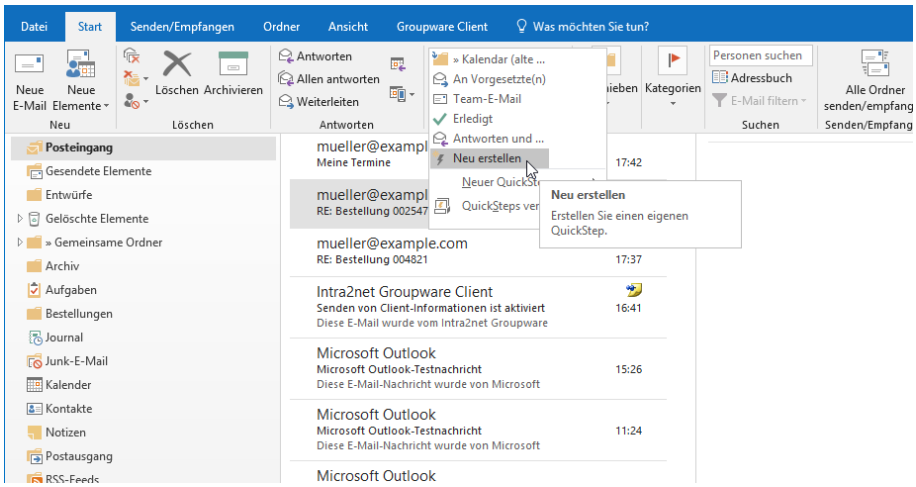
26.4. Erinnerungen und Nachverfolgen von E-Mails

Outlook bietet die Möglichkeit, Erinnerungen für E-Mails zu definieren und eine Liste von später zu bearbeitenden E-Mails zu erstellen (Nachverfolgen-Funktion). Dies ist mit dem Groupware Client nicht möglich. Außerdem können solche Erinnerungen und Nachverfolgen-Informationen generell nicht auf Mobilgeräte übertragen werden.

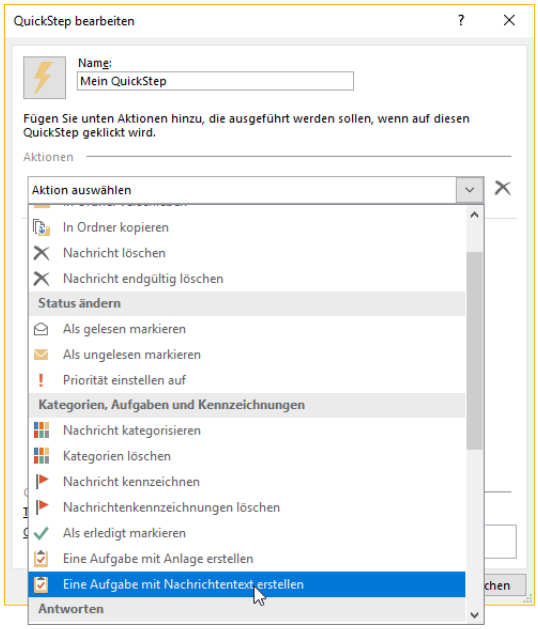
Daher empfehlen wir, statt der Nachverfolgen-Funktion für die E-Mail eine separate Aufgabe zu erstellen. Diese kann dann in Outlook, der Webgroupware und auf per ActiveSync angebundenen Geräten verwendet werden. Bei Bedarf kann sie auch für andere Nutzer freigegeben und von diesen bearbeitet werden, 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".

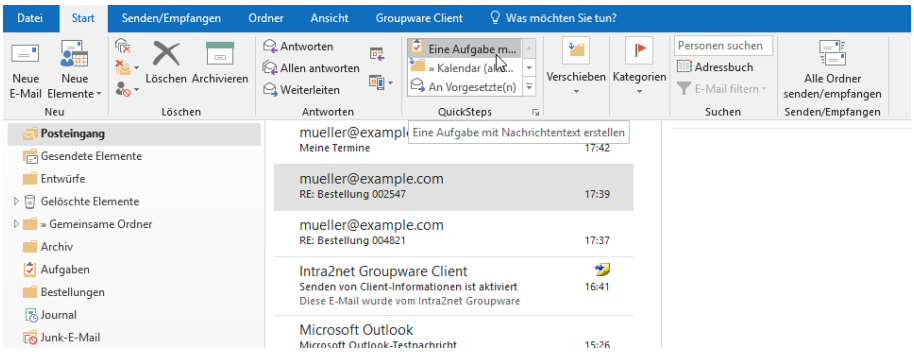


2. Wählen Sie die Aktion "Eine Aufgabe mit Nachrichtentext erstellen".



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.



26.5. Lesebestätigungen

Der SMTP-Standard sieht vor, dass ein Absender einer E-Mail vom Empfänger eine automatische Lesebestätigung (*Message Disposition Notification* (MDN)) erbitten kann. Outlook unterstützt dies und bietet in den E-Mail-Optionen die Möglichkeit den Umgang damit einzustellen. Standardmäßig ist vorgesehen, dass der Nutzer gefragt wird ob eine Lesebestätigung gesendet werden soll oder nicht.

Intra2net hat aber die Erfahrung gemacht, dass Outlook diese Option nicht vollständig beachtet und in manchen Fällen dennoch ungefragt Lesebestätigungen an Absender versendet. Vor allem wurde dies im Zusammenhang mit dem Verschieben oder Löschen von E-Mails beobachtet. Hier wurden dann von Outlook ungefragt auch alte E-Mails mit "Ihre Nachricht wurde ungelesen gelöscht" beantwortet.

Hinzu kommt, dass der Groupware Client für eine korrekte Funktion E-Mails löschen und durch neue Versionen ersetzen muss, z.B. wenn ein anderer Nutzer oder Gerät die E-Mail verändert hat. Diese Arbeitsweise funktioniert bei E-Mails mit Lesebestätigung nicht für den Nutzer praktikabel, da er bei einer jeden solchen Änderung an einer E-Mail mit Lesebestätigung von Outlook per Dialog zum Versand der Lesebestätigung gefragt werden würde.

Daher entfernt der Groupware Client die Anforderung von Lesebestätigungen von allen eingehenden E-Mails.

Sollte der Versand von Lesebestätigungen dennoch unbedingt gewünscht werden, so kann das Entfernen der Lesebestätigungen auf eigenes Risiko des Nutzers durch das Setzen des Registry-Wertes `MdnAllow` unterdrückt werden. Weitere Informationen zur Registry finden Sie in Abschnitt 31.2.1, „Einstellungen für den Store“.

27. Kapitel - Kompatibilität und Zusammenarbeit

27.1. Personal-Firewalls auf dem Client

Der Intra2net Groupware Client muss aus dem Outlook-Prozess heraus per IMAP/IMAPS, SMTP und HTTP/HTTPS auf das Intra2net System 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.

27.2. Virenscanner auf dem Client

Auf dem Client installierte Virenscanner 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 Virenscanner auf dem Client aktiviert, so versuchen Sie zuerst, das Scannen von IMAP zu deaktivieren. Neue E-Mails durchlaufen zuerst das Intra2net System und seinen Virenscanner, 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, Outlook-Addin deaktivieren
Eset	NOD32 Antivirus	Scannen des IMAP-Protokolls deaktivieren, Outlook-Addin deaktivieren
Eset	Endpoint Antivirus	Stört auch ohne Outlook-Addin und im deaktivierten Zustand die Netzwerk-Kommunikation, muss deinstalliert werden
F-Secure	Internet Security	Keine Änderung notwendig
G Data	Alle Antivirus-Produkte	Outlook-Addin deaktivieren
Kaspersky	Internet Security	Outlook-Addin deaktivieren
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

27.3. Kompatibilität mit PDAs und Mobiltelefonen

Verwenden Sie wenn möglich die ActiveSync-Funktion des Intra2net Systems um eine direkte Verbindung zwischen Intra2net System und Mobilgerät ohne einen Umweg über Outlook herzustellen. Dadurch können die Daten auf dem Mobilgerät auch von unterwegs aus aktualisiert werden. Außerdem ist kein Add-In für Outlook notwendig, welches unter Umständen Probleme hervorrufen kann.

Die Konfiguration von ActiveSync zwischen Intra2net System und Mobilgeräten finden Sie erklärt im 35. Kapitel, „Mobile Geräte per ActiveSync anbinden".

27.4. 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 Nutzung von Programmen, die die in Outlook gespeicherten Daten mit anderen Datenbanken in beide Richtungen synchronisieren, kann im Zusammenhang mit dem Groupware Client zu unerwünschten Effekten führen. Typische Effekte in diesem Zusammenhang sind ständige Änderungsvorgänge, Duplikate und der Verlust von in Outlook vorgenommenen Änderungen.

Die Zusammenarbeit mit anderen Add-Ins oder Plugins für Outlook wird nicht garantiert.

27.4.1. Inkompatible Add-Ins

Mit folgenden Outlook Add-Ins konnten wir Störungen beobachten:

- Avira Antivirus Premium
- CardScan Microsoft Outlook Add-In
- CodeTwo CatMan
- d.3 Smart Outlook (d.Velop AG)
- Emisoft Anti-Malware
- Evernote for Outlook Add-In
- G Data AntiVirus
- iTunes Outlook AddIn (Apple)
- Kaspersky Small Office Security
- Nuance PDF Converter Add-In
- Outlook Change Notifier AddIn (Apple)
- Panda Internet Security Antivirus Add-In
- Powerbird
- Skype Meeting Add-In

- TeamViewer Meeting Add-In
- TrendMicro Worry Free Business Security

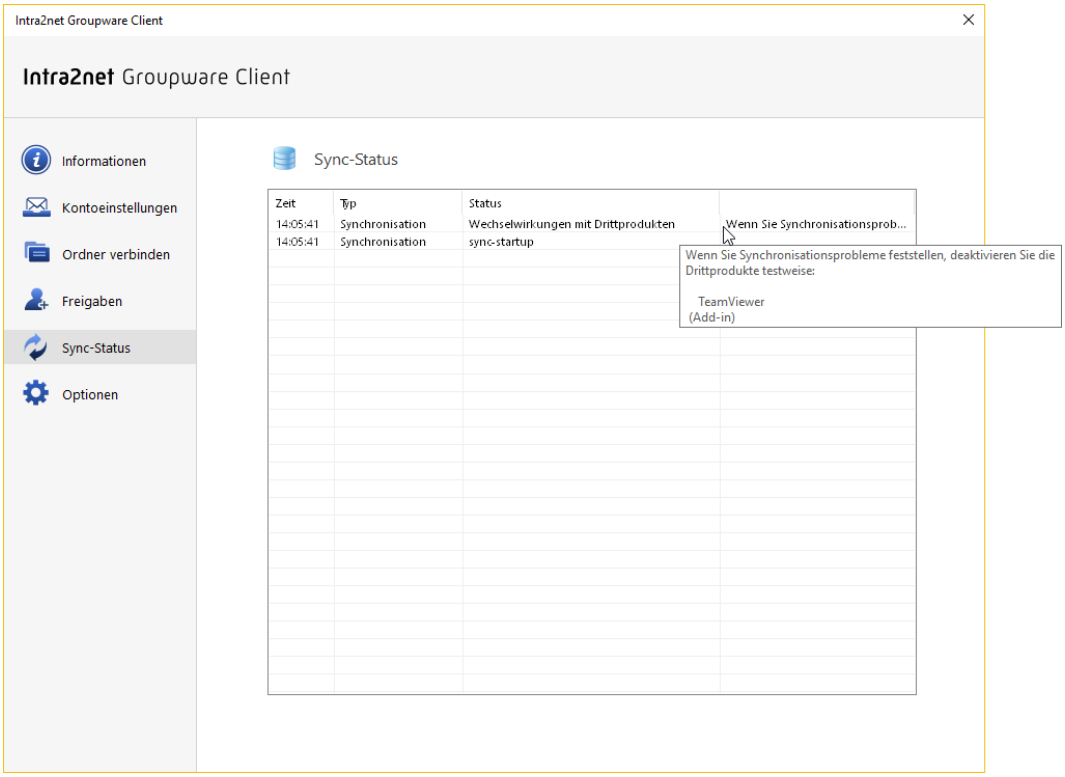
Von der Nutzung dieser Add-Ins zusammen mit dem Groupware Client raten wir ab.

Sollte eines oder mehrere dieser Add-Ins in Outlook installiert oder aktiv sein, so deaktivieren Sie sie über das Menü "Datei", "Optionen", "Add-Ins" bevor Sie den Groupware Client einrichten.

27.5. Automatische Erkennung von Kompatibilitätsproblemen

Der Groupware Client enthält ein Modul, welches versucht mögliche Kompatibilitätsprobleme mit Drittprodukt-Modulen automatisch zu erkennen. Wird solches Modul erkannt, so bekommt der Benutzer einmalig eine entsprechende Meldung mit den Namen der betroffenen Programme bzw. Add-Ins im Posteingang angezeigt.

Zusätzlich werden mögliche Kompatibilitätsprobleme und die betroffenen Programme jederzeit im Menü "Groupware Client > Sync-Status" angezeigt.



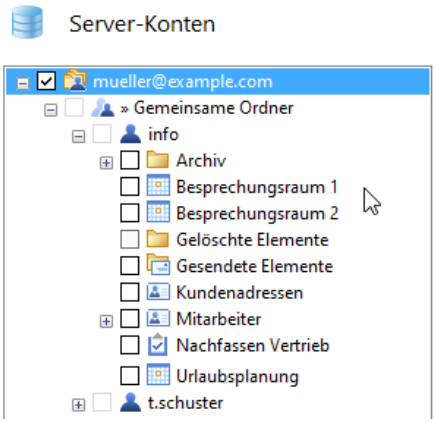
Die Erkennung solcher Module kann über die Registry deaktiviert werden, siehe Abschnitt 31.2.1, „Einstellungen für den Store“.

28. Kapitel - Konzept für öffentliche Ordner

Öffentliche Ordner sind E-Mail- und Groupware-Ordner, die nicht einer Person zugeordnet sind, sondern von mehreren oder allen Benutzern eines Unternehmens gemeinsam genutzt werden. Im Intra2net System wird dieses Konzept dadurch umgesetzt, dass ein zusätzliches, normales Benutzerkonto angelegt wird und von diesem Ordner an Benutzergruppen freigegeben werden.

Als Name für ein von allen Nutzern verwendetes Benutzerkonto bietet sich z.B. "info" an, ansonsten zur Gruppe passende Namen wie z.B. "vertrieb" oder "service".

Innerhalb dieses Benutzerkontos können dann Unterordner mit beliebigen Ordnertypen (E-Mail, Kalender, Kontakte, Aufgaben,...) angelegt werden. Damit können zusätzlich zu einem allgemeinen E-Mail-Postfach u.a. ein Urlaubskalender, die Verwaltung von Ressourcen wie Besprechungsräumen oder Servicefahrzeugen, Pflege der Kundenadressen, Pflege der Kontaktdaten der Mitarbeiter,... umgesetzt werden.



28.1. Einrichtung

Gehen Sie wie folgt vor, um öffentliche Ordner einzurichten:

1. Legen Sie auf dem Intra2net System im Menü " Benutzermanager > Benutzer" ein neues Benutzerkonto an. Für Details siehe Abschnitt 14.2, „Benutzer“.

2. Sollen nicht alle Nutzer gleiche Zugriffsrechte auf die öffentlichen Ordner bekommen, legen Sie im Menü " Benutzermanager > Gruppen" eine oder mehrere Benutzergruppen an und fügen diesen die passenden Benutzer als Mitglieder hinzu.

3. Legen Sie auf einem PC ein zusätzliches Outlook-Profil zur Verwaltung der öffentlichen Ordner an. Gehen Sie dabei vor wie im 20. Kapitel, „Profil einrichten“ beschrieben. Verwenden Sie die Zugangsdaten des eben angelegten Benutzerkontos.

4. Starten Sie Outlook mit dem eben neu angelegten Verwaltungsprofil.

5. Legen Sie die gewünschten Ordner in Outlook an und geben sie an die gewünschten Benutzergruppen frei wie im 23. Kapitel, „Ordner freigeben“ beschrieben.

6. Die einzelnen Nutzer können die eben freigegebenen Ordner nun in ihren Groupware Clients verbinden wie in Abschnitt 22.2, „Gemeinsame Ordner verbinden“ beschrieben.

28.2. E-Mails

Das Benutzerkonto für öffentliche Ordner kann E-Mails empfangen und versenden wie jedes andere Benutzerkonto auch.

Damit die Mitarbeiter Zugriff auf eingehende E-Mails bekommen, geben Sie den Posteingang des Kontos frei und verbinden ihn bei den Nutzern.

Damit die Mitarbeiter den öffentlichen Ordner als Absenderadresse nutzen können, richten Sie bei den Mitarbeitern eine passende Versandidentität ein wie in Abschnitt 21.3.2, „Mehrere Absenderadressen“ beschrieben. Hinterlegen Sie dabei auch den Unterordner "Gesendete Elemente" des öffentlichen Ordners als Ordner für gesendete Nachrichten, damit auch diese zentral verwaltet und von allen Mitarbeitern eingesehen werden können.

29. Kapitel - Migration von E-Mails mit IMAPCopy

Wenn Sie größere Mengen von E-Mails von einem bestehenden E-Mail-Server auf das Intra2net System übernehmen möchten, ist meist das Programm IMAPCopy der schnellste Weg. IMAPCopy kopiert die E-Mails automatisiert von einem IMAP-Server zu einem anderen und kann dabei mehrere Konten am Stück verarbeiten.

Voraussetzung ist also, dass der bestehende E-Mail-Server über das IMAP-Protokoll erreichbar ist. Bei einigen Groupware-Servern, wie z.B. Tobit David oder Microsoft Exchange, muss der IMAP-Dienst unter Umständen zuerst aktiviert werden.

IMAPCopy ist Open Source und kann von folgender URL geladen werden: http://ardiehl.de/imapcopy/index.html.



Entpacken Sie das Programm in ein separates Verzeichnis. Es wird über die Datei `ImapCopy.cfg` gesteuert. Eine passende Beispieldatei wird mitgeliefert. Öffnen Sie diese mit einem Texteditor und bearbeiten sie. Zeilen, die mit # beginnen, sind Kommentarzeilen und werden vom Programm ignoriert.

Passen Sie folgende Befehle in der Datei an:

SourceServer	Der DNS-Name oder die IP des Quellservers, von dem die E-Mails abgerufen werden sollen
SourcePort	Der TCP-Port über den der IMAP-Dienst auf dem Quellserver angesprochen wird. Normalerweise **143**.
DestServer	Der DNS-Name oder die IP des Zielservers. Also hier der Name des Intra2net Systems.
DestPort	Der TCP-Port für den IMAP-Dienst auf dem Zielserver. Für das Intra2net System immer **143**.
skipfolder	Ordner auf dem Quellserver, die nicht kopiert werden sollen. Bei Bedarf können ein oder mehrere Einträge aktiviert werden und damit z.B. gelöschte E-Mails vom Kopieren ausgeschlossen werden. Verwenden Sie pro auszuschließendem Ordner ein "skipfolder"-Befehl in einer separaten Zeile.
copyfolder	Wenn nur bestimmte Ordner kopiert werden sollen, dann aktivieren Sie diesen Befehl und geben die zu kopierenden Ordner in einzelnen "copyfolder"-Befehlen an. Ist kein "copyfolder"-Befehl angegeben, werden automatisch alle sichtbaren Ordner unterhalb von `INBOX` kopiert.
DenyFlags	Verwenden Sie hier den voreingestellten Wert "\Recent", da dieses Flag nicht kopiert werden kann.
Copy	Geben Sie jedes zu kopierende Konto in einem "Copy"-Befehl an und ersetzen die Beispielzeilen mit foo und bar. Der 1. Parameter ist der Login des Benutzers auf dem Quellserver Der 2. Parameter ist das Passwort des Benutzers auf dem Quellserver Der 3. Parameter ist der Login des Benutzers auf dem Intra2net System

	Der 4. Parameter ist das Passwort des Benutzers auf dem Intra2net System Mehrere Copy-Befehle werden nacheinander abgearbeitet.

Zum Ausführen öffnen Sie eine Konsole mit cmd und wechseln mit cd in das Verzeichnis, in welches Sie IMAPCopy vorher entpackt haben.

Testen Sie als Erstes die grundsätzliche Konfiguration durch Eingabe von **`imapcopy -t`**.

Der Programmfortschritt und eventuelle Fehler- oder Erfolgsmeldungen werden auf der Konsole ausgegeben. Nur wenn Sie IMAPCopy wie beschrieben in einer separaten Konsole geöffnet haben, können Sie diese Meldungen auch nach Beendigung des Programms noch sehen.

Das Programm prüft jetzt die Erreichbarkeit des Quell- und Zielservers sowie die Logins. Werden Ihnen Fehler angezeigt, so passen Sie die Konfigurationsdatei an und testen die Konfiguration erneut.

Testen Sie nun die Erkennung der Ordnerstruktur durch Eingabe von **`imapcopy -0`**.

Das Programm versucht jetzt alle Ordner vom Quellserver einzulesen und auf dem Intra2net System anzulegen. Es werden aber noch keine E-Mails kopiert. Kontrollieren Sie über die Webgroupware des Intra2net Systems, ob dort alle Ordner korrekt angelegt wurden. Passen Sie evtl. die Konfiguration von IMAPCopy an.

Starten Sie jetzt das tatsächliche Kopieren aller E-Mails durch Eingabe von **`imapcopy`**.

30. Kapitel - Migration von Microsoft Exchange

Um von Microsoft Exchange auf den Intra2net Business Server und Groupware Client zu migrieren, gibt es 2 Varianten:

Zum einen die Offline-Migration, bei der während der Migration keiner der beiden Server genutzt werden kann. Die Migration muss hintereinander weg am Stück durchgeführt werden und kann nicht unterbrochen werden. Diese Variante ist einfacher und schneller, kann aber meist nur außerhalb der regulären Geschäftszeiten umgesetzt werden.

Alternativ dazu gibt es die Migration im laufenden Betrieb. Diese Variante ist etwas aufwendiger, kann aber dafür im laufenden Betrieb und mit nur sehr geringfügigen Einschränkungen für die Nutzer umgesetzt werden. Es wird dabei Benutzer für Benutzer umgezogen. Daher kann die Migration mit dieser Variante auch über mehrere Tage gestreckt werden.

30.1. Offline-Migration

Bei dieser Variante der Migration können während der Migration weder der bisherige Exchange, noch das neue Intra2net System für E-Mail und Groupware genutzt werden. Der Empfang neuer E-Mails wird für diesen Zeitraum blockiert. Stimmen Sie daher den Termin rechtzeitig mit den betroffenen Benutzern ab und planen genug Zeit ein.

Voraussetzungen:

- Voll funktionsfähiger Microsoft Exchange Server
- Intra2net Business Server in Grundkonfiguration
- Administratorrechte für den Exchange Server, die Active Directory Domain und den Intra2net Business Server
- Liste mit allen Benutzern und ihren Passwörtern im lokalen Active Directory
- Zugriff auf die bestehenden Outlook-Installationen aller Benutzer
- Bei Abholung der E-Mails von einem externen Provider per POP3: Liste mit allen Logins und Passwörtern für die E-Mail-Abholung

30.1.1. Die Migration in einzelnen Schritten

1. Richten Sie den Intra2net Business Server so ein, dass er zumindest eine IP im LAN, DNS, passendes lokales SSL-Zertifikat und Internetzugang hat. Er benötigt eine andere IP als der bisherige Exchange Server, damit beide während der Migration miteinander kommunizieren können. Die Konfiguration der einzelnen Punkte finden Sie beschrieben im Teil 2, „Allgemeine Funktionen“.

2. Legen Sie für alle Benutzer ein Konto auf dem Intra2net System an. Legen Sie bei Bedarf Benutzergruppen an. Dies empfiehlt sich vor allem, um später die Freigabe von E-Mail- und Groupware-Ordnern leichter organisieren zu können.

3. Gehen Sie Benutzer für Benutzer im Active Directory durch und übernehmen die vorhandenen E-Mail-Alias-Adressen ins Menü "Benutzermanager > Benutzer : Adressen" auf dem Intra2net System.

4. Deaktivieren Sie den Empfang jeglicher neuer E-Mails und den Zugriff per OWA. Verbieten Sie allen Benutzern Outlook zu öffnen. Kein Benutzer darf ab diesem Moment mehr Änderungen an den Groupware- oder E-Maildaten vornehmen.

5. Erzeugen Sie ein Backup aller E-Mails und Groupwaredaten auf dem Exchange Server.

6. Warten Sie, bis das Backup vollständig erstellt wurde und kopieren es zur Sicherheit auch noch auf einen anderen Server.

7. Konfigurieren und aktivieren Sie auf dem Exchange Server den Zugriff auf die E-Mails mit dem IMAP-Protokoll falls dies bisher noch nicht möglich ist.

8. Verwenden sie IMAPCopy um die E-Mails aller Benutzer vom Exchange auf das Intra2net System zu kopieren. Die Nutzung von IMAPCopy wird beschrieben in 29. Kapitel, „Migration von E-Mails mit IMAPCopy".

9. Öffnen Sie die Outlook-Installation des ersten Benutzers.

10. Erzeugen Sie eine lokale Outlook-Datendatei, die alle Groupware-Ordner (nicht unbedingt dagegen die E-Mail-Ordner) des Benutzers enthält. Verwenden Sie dazu die Import/Export-Funktion von Outlook.

11. Installieren Sie den Intra2net Groupware Client auf dem PC des Benutzers.

12. Legen Sie für diesen Benutzer ein neues Outlook-Profil an und konfigurieren es für die Nutzung mit dem Intra2net Groupware Client wie in Abschnitt 19.1, „Installation des Programms" und den folgenden Abschnitten beschrieben.

13. Übernehmen Sie die Groupwaredaten aus der vorher erstellten lokalen Outlook-Datendatei wie beschrieben in Abschnitt 21.2.1.2, „Import in den Groupware Client".

14. Kontrollieren Sie, ob in den Kontakte-Ordnern Benutzer aus der lokalen Domain vorhanden sind. Wenn ja, dann müssen die E-Mail-Adressen dieser Benutzer von der internen Exchange-Adressierung auf normale E-Mail-Adressen umgestellt werden.

15. Kontrollieren Sie in den Kalendern und Aufgaben, ob es dort zukünftige Termine bzw. offene Aufgaben gibt, in denen andere Teilnehmer aus der lokalen Domain hinterlegt sind. Diese anderen Teilnehmer sind in Form der internen Exchange-Adressierung hinterlegt und müssen auf normale E-Mail-Adressen umgestellt werden.

16. Wiederholen Sie Schritt 9 bis 15 für alle Benutzer.

17. Migrieren Sie die öffentlichen Ordner wie beschrieben in Abschnitt 30.2.3, „Öffentliche Ordner".

18. Deaktivieren Sie den Exchange Server vollständig und dauerhaft.

19. Konfigurieren Sie den Versand und Empfang neuer E-Mails im Intra2net System wie beschrieben im 15. Kapitel, „E-Mail".

30.2. Migration im laufenden Betrieb

Bei dieser Variante der Migration können die Benutzer während der Migration fast normal weiterarbeiten. Die Benutzer werden einer nach dem anderen vom Exchange auf das Intra2net System migriert.

Die einzigen Einschränkungen sind, dass der einzelne Benutzer, der momentan migriert wird, während seiner Migration nicht in Outlook arbeiten kann. Der Empfang von E-Mails ist für ihn aber weiterhin möglich. Die während der Migration empfangenen E-Mails können danach ganz normal genutzt werden. Außerdem kann während der Migrationsphase nicht über Systemgrenzen hinweg auf gemeinsam genutzte Ressourcen, wie z.B. öffentliche Ordner oder freigegebene Ordner, zugegriffen werden.

Voraussetzungen:

- Voll funktionsfähiger Microsoft Exchange Server
- Intra2net Business Server in Grundkonfiguration
- Administratorrechte für den Exchange Server, die Active Directory Domain und den Intra2net Business Server
- Liste mit allen Benutzern und ihren Passwörtern im lokalen Active Directory
- Zugriff auf die bestehenden Outlook-Installationen aller Benutzer
- Bei Abholung der E-Mails von einem externen Provider per POP3: Liste mit allen Logins und Passwörtern für die E-Mail-Abholung

30.2.1. Vorbereitung der Migration

1. Richten Sie den Intra2net Business Server so ein, dass er zumindest eine IP im LAN, DNS, passendes lokales SSL-Zertifikat und Internetzugang hat. Er benötigt eine andere IP als der bisherige Exchange Server, damit beide während der Migration miteinander kommunizieren können. Die Konfiguration der einzelnen Punkte finden Sie beschrieben im Teil 2, „Allgemeine Funktionen“.

2. Stellen Sie sicher, dass auf dem Intra2net System im Menü "Benutzermanager > Benutzer" für die normalen Benutzer noch *keine* Konten angelegt sind.

3. Richten Sie den Versand von E-Mails über das Intra2net System ein, siehe Abschnitt 15.1, „E-Mail-Versand“.

4. Hinterlegen Sie im Exchange das Intra2net System als Relayserver für den Versand aller E-Mails ins Internet.

5. Richten Sie den Empfang von E-Mails über das Intra2net System ein und leiten die E-Mails an den Exchange weiter. Siehe hierzu Abschnitt 15.3, „E-Mail-Empfang auf dem Intra2net System“ und Abschnitt 15.4, „Weiterleitung von gesamten Domains“.

6. Testen Sie den Empfang und Versand von E-Mails mit der neuen Konfiguration.

7. Testen Sie den Versand von internen E-Mails vom Exchange an das Intra2net System. Verwenden Sie als Adresse das Login und als Domain den voll qualifizierten lokalen DNS-Namen des Intra2net Systems, also z.B. **`admin@intra.net.lan`**. Kontrollieren Sie über die Webgroupware des Intra2net Systems ob die Test-E-Mail ankam.

8. Konfigurieren und aktivieren Sie auf dem Exchange Server den Zugriff auf die E-Mails mit dem IMAP-Protokoll falls dies bisher noch nicht möglich ist.

9. Falls auf dem Exchange Server einer oder mehrere Nutzer Mobilgeräte per ActiveSync angebunden haben, bereiten Sie die Nutzung von ActiveSync mit dem Intra2net System vor wie in 35. Kapitel, „Mobile Geräte per ActiveSync anbinden“ beschrieben.

10. Konfigurieren Sie auf dem Intra2net System die Archivierung von E-Mails über das Menü "Dienste > E-Mail > Archivierung". Archivieren Sie entweder in ein dediziertes Archivierungssystem, oder zumindest in ein separates E-Mail-Konto. Dies dient als Sicherung für neu empfangene E-Mails falls bei der Migration etwas schief läuft.

11. Erzeugen Sie ein Backup aller E-Mails und Groupwaredaten auf dem Exchange Server.

12. Warten Sie, bis das Backup vollständig erstellt wurde und kopieren es zur Sicherheit auch noch auf einen anderen Server.

30.2.2. Die Migration der einzelnen Benutzer

Führen Sie folgende Schritte nacheinander für jeden einzelnen Benutzer durch.

1. Legen Sie den Benutzer mit seinen Zugangsdaten und Gruppenzugehörigkeit auf dem Intra2net System an.

2. Konfigurieren Sie die E-Mail-Adressen des Benutzers unter "Benutzermanager > Benutzer : Adressen". Wählen Sie dabei explizit die auf den Exchange weitergeleiteten Domains aus. Ab diesem Moment landen neue E-Mails aus dem Internet für diesen Benutzer im Konto auf dem Intra2net System und nicht mehr auf dem Exchange.

3. Richten Sie auf dem Exchange eine E-Mail-Weiterleitung für diesen Benutzer an sein Konto auf dem Intra2net System ein. Verwenden Sie als Adresse den Login und als Domain den voll qualifizierten lokalen DNS-Namen des Intra2net Systems, also z.B. **`mustermann@intra.net.lan`**. Ab diesem Moment landen auch lokale E-Mails an diesen Benutzer auf dem Intra2net System und nicht mehr auf dem Exchange.

4. Bitten Sie diesen Benutzer während seiner Migration nicht mehr in Outlook oder OWA zu arbeiten. Deaktivieren Sie auch alle Mobilgeräte die per ActiveSync auf dieses Konto zugreifen.

5. Verwenden sie IMAPCopy um die E-Mails dieses einen Benutzers vom Exchange auf das Intra2net System zu kopieren. Die Nutzung von IMAPCopy wird beschrieben in 29. Kapitel, „Migration von E-Mails mit IMAPCopy“.

6. Öffnen Sie die Outlook-Installation des Benutzers.

7. Erzeugen Sie eine lokale Outlook-Datendatei, die alle Groupware-Ordner (nicht unbedingt dagegen die E-Mail-Ordner) enthält. Verwenden Sie dazu die Import/Export-Funktion von Outlook.

8. Installieren Sie den Intra2net Groupware Client auf dem PC des Benutzers.

9. Legen Sie für diesen Benutzer ein neues Outlook-Profil an und konfigurieren es für die Nutzung mit dem Intra2net Groupware Client wie in Abschnitt 19.1, „Installation des Programms“ und den folgenden Abschnitten beschrieben.

10. Übernehmen Sie die Groupwaredaten aus der vorher erstellten lokalen Outlook-Datendatei wie beschrieben in Abschnitt 21.2.1.2, „Import in den Groupware Client“.

11. Kontrollieren Sie, ob in den Kontakte-Ordnern Benutzer aus der lokalen Domain vorhanden sind. Wenn ja, dann müssen die E-Mail-Adressen dieser Benutzer von der internen Exchange-Adressierung auf normale E-Mail-Adressen umgestellt werden.

12. Kontrollieren Sie in den Kalendern und Aufgaben, ob es dort zukünftige Termine bzw. offene Aufgaben gibt, in denen andere Teilnehmer aus der lokalen Domain hinterlegt sind. Diese anderen Teilnehmer sind in Form der internen Exchange-Adressierung hinterlegt und müssen auf normale E-Mail-Adressen umgestellt werden.

13. Konfigurieren Sie bei diesem Benutzer evtl. vorhandene Mobilgeräte so um, dass Sie ab sofort das Intra2net System für ActiveSync verwenden.

30.2.3. Öffentliche Ordner

1. Öffnen Sie eine Outlook-Installation mit einem Exchange-Profil, welches volle Zugriffsrechte auf die öffentlichen Ordner hat.

2. Erzeugen Sie eine lokale Outlook-Datendatei, die alle öffentlichen Ordner enthält. Verwenden Sie dazu die Import/Export-Funktion von Outlook.

3. Legen Sie auf dem Intra2net System ein allgemeines Benutzerkonto, wie z.B. **`info`** an.

4. Richten Sie auf einem PC ein temporäres Outlook-Profil für die Nutzung mit dem Intra2net Groupware Client ein. Verwenden Sie dafür das eben angelegte Benutzerkonto.

5. Importieren Sie die vorher erzeugte Datendatei in dieses Outlook-Profil.

6. Geben Sie die Ordner mit dem Groupware Client nach Bedarf an Gruppen oder einzelne Benutzer frei. Siehe dazu 23. Kapitel, „Ordner freigeben“.

7. Geben Sie mindestens einem Benutzer das "Ordner"-Recht für alle Ordner des Kontos. Dieser Benutzer kann dadurch den Zugriff auf das Konto verwalten.

8. Öffnen Sie das Menü "Groupware Client > Sync-Status" und warten, bis alle Daten zum Server geschrieben wurden.

9. Schließen Sie Outlook. Das eben verwendete Outlook-Profil wird jetzt nicht mehr benötigt und kann gelöscht werden.

10. Benutzer, die auf die öffentlichen Ordner zugreifen möchten, können diese jetzt verbinden. Die dafür nötigen Schritte sind in Abschnitt 22.2, „Gemeinsame Ordner verbinden“ beschrieben.

30.2.4. Abschließende Schritte

1. Deaktivieren Sie die Weiterleitung der Domain(s) an den Exchange unter "Dienste > E-Mail > Domains".

2. Deaktivieren Sie den Exchange Server vollständig und dauerhaft.

3. Konfigurieren Sie unter "Dienste > E-Mail > Archivierung" entweder das endgültig genutzte Archivierungssystem oder deaktivieren die Archivierung wieder.

31. Kapitel - Referenzinformationen



Hinweis

Die in diesem Kapitel aufgeführten Informationen gelten ausschließlich für den Intra2net Groupware Client. Informationen zur Webgroupware und Activesync finden Sie im 38. Kapitel, „Referenzinformationen“.

31.1. 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.

31.1.1. Aufgaben

31.1.1.1. Unterstützte Elemente

- Betreff
- Kategorien und ihre Farbzuordnung
- 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

31.1.1.2. Nicht unterstützte Elemente

Ohne Gewähr auf Vollständigkeit. Im Zweifel werden nur die explizit als unterstützt aufgeführten Elemente unterstützt.

- Text/Inhalt (Formatierter Rich-Text)

31.1.2. Termine

31.1.2.1. Unterstützte Elemente

- Betreff
- Kategorien und ihre Farbzuordnung
- 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, die mit "Besprechung an diesen Teilnehmer senden" markiert sind
- Terminserien

Folgende Ausnahmen können für einzelne Termine von Serien verwendet werden:

- Löschen eines Einzeltermins
- Geänderter Betreff
- Geänderter Text/Inhalt (Nur Text)

- Geänderter Ort
- Änderungen von Datum und Uhrzeit

31.1.2.2. 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
- Teilnehmer, die nicht mit "Besprechung an diesen Teilnehmer senden" markiert sind

Folgende Ausnahmen können für einzelne Termine von Serien nicht verwendet werden:

- Geänderte Teilnehmer

31.1.3. Notizen

31.1.3.1. Unterstützte Elemente

- Betreff
- Kategorien und ihre Farbzuordnung
- Text/Inhalt

31.1.4. Kontakte

31.1.4.1. Unterstützte Elemente

- Vollständiger Name
- Anrede
- Vorname
- Weitere Vornamen
- Nachname
- Namenszusatz
- Initialen
- 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 und ihre Farbzuordnung
- Notiz (Nur Text)
- 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 25.8, „Benutzerdefinierte Felder in Kontakten“

31.1.4.2. 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.

31.1.4.3. 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)
- Nachverfolgung

31.1.5. Kontaktgruppen

31.1.5.1. Unterstützte Elemente

- Name der Kontaktgruppe
- Anzeigename jedes Mitglieds
- E-Mail-Adresse jedes Mitglieds
- Notiz zur Kontaktgruppe (Nur Text)

31.1.5.2. 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)
- Nachverfolgung

31.1.6. E-Mails

31.1.6.1. Unterstützte Elemente

- Absender
- Empfänger
- CC

- BCC
- Betreff
- Sendezeitpunkt
- Empfangszeitpunkt
- Wichtigkeit
- Internetkopfzeilen
- Inhalt (Nur Text, HTML und formatierter Rich-Text)
- Dateianhänge
- Kategorien (ausgenommen: Farben)

31.1.6.2. Nicht unterstützte Elemente

Ohne Gewähr auf Vollständigkeit. Im Zweifel werden nur die explizit als unterstützt aufgeführten Elemente unterstützt.

- Erinnerungen
- Nachverfolgung

31.1.7. Alle Objekte

Generell können folgende Elemente mit dem Intra2net Groupware Client nicht synchronisiert werden:

- Auto-Archivierung deaktivieren
- Anfügen anderer Outlook-Elemente oder (außer bei E-Mails) Dateien
- Verknüpfung mit Kontakten

31.2. Erweiterte Einstellungen in der Registrierung

Der Intra2net Groupware Client kann über folgende Einstellungen in der Windows-Registry weiter angepasst werden.

Alle Registry-Keys sind unterhalb von `HKLM\SOFTWARE\Intra2net AG\Intranator Groupware Client` zu finden. Wurde ein 32-Bit Outlook auf einem 64-Bit Betriebssystem installiert, liegen sie dagegen unter `HKLM\SOFTWARE\Wow6432Node\Intra2net AG\Intranator Groupware Client`.

Wurde der Intra2net Groupware Client nur für einen Benutzer installiert, wird statt HKLM der entsprechende Schlüssel unterhalb von HKCU verwendet.

Die meisten Einträge werden bei der Installation nicht automatisch angelegt. Solange die Einträge nicht angelegt sind, werden die in der Tabelle aufgeführten Standardwerte verwendet. Legen Sie einen Eintrag mit dem in der Tabelle aufgeführten Namen mit regedit an um die Werte zu verändern.

31.2.1. Einstellungen für den Store

Die Einstellungen für den Store sind im Schlüssel `mxstore_Store` zu finden.

Eintrag (und Datentyp)	Standardwert	Erklärung
SkipPrc (REG_SZ)	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 (REG_DWORD)	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 (REG_DWORD)	0x0000001b	Auswahl der Spalten, die bei einem zu protokollierenden Ereignis im Trace ausgegeben werden. Weitere Informationen erhalten Sie bei Bedarf über unseren Support.
TracerDisabled (REG_DWORD)	0	Hiermit wird ausgewählt, ob nur Starts und Fehler protokolliert werden (Wert 1) oder auch normale Vorgänge im Betrieb (Wert 0).
PathLog (REG_SZ)		Vollständiger Pfad, in dem die Tracedateien abgelegt werden. Ist dieser Eintrag nicht vorhanden, werden sie im `%LOCALAPPDATA%\Intra2net`-Verzeichnis abgelegt.
TraceSzMax (REG_DWORD)	170	Maximalgröße für eine Tracedatei in Megabytes. Bei Überschreiten dieser Größe wird die Datei rotiert.
TraceDaysToRemember (REG_DWORD)	14	Anzahl an Tagen, die Tracedateien maximal aufbewahrt werden.
TrgMin_FldChanged (REG_DWORD)	300	Kürzestes Intervall (in Sekunden), welches vom Benutzer bei den Updateintervallen für "Ordner verändert" eingestellt werden kann.
TrgMin_FldTreeChanged (REG_DWORD)	300	Kürzestes Intervall (in Sekunden), welches vom Benutzer bei den Updateintervallen für "Ordnerbaum verändert" eingestellt werden kann.
TrgMin_MailChanged (REG_DWORD)	60	Kürzestes Intervall (in Sekunden), welches vom Benutzer bei Unterordnern für "Abholen im Hintergrund" eingestellt werden kann.
TrgMin_MailChangedRoot (REG_DWORD)	1800	Kürzestes Intervall (in Sekunden), welches vom Benutzer beim Wurzelordner für "Abholen im Hintergrund" eingestellt werden kann.
TrgDefault_FldChanged (REG_DWORD)	3600	Standardintervall (in Sekunden) für "Ordner verändert", wenn der Benutzer nichts anderes eingestellt hat.

Eintrag (und Datentyp)	Standardwert	Erklärung
TrgDefault_FldTreeChanged (REG_DWORD)	3600	Standardintervall (in Sekunden) für "Ordnerbaum verändert", wenn der Benutzer nichts anderes eingestellt hat.
TrgDefault_MailChanged (REG_DWORD)	3600	Standardintervall (in Sekunden) für "Inhalt verändert", wenn der Benutzer nichts anderes eingestellt hat.
TrgDefault_Always (REG_DWORD)	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.
TrgDefault_Ctx_InFocus (REG_DWORD)	180	Standardintervall (in Sekunden) mit dem der Inhalt des aktuell in Outlook geöffneten Ordners synchronisiert wird.
Trigger_Reset (REG_DWORD)	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 (REG_DWORD)	1	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. 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.
CalPrivatePlaceholder_ResetOnOpen (REG_DWORD)	0	Wenn 1, wird die Einstellung von CalPrivatePlaceholder_Default nicht nur beim ersten Öffnen einer Datendatei übernommen, sondern bei jedem Start.
MemLoad_SyncOff (REG_DWORD)	90	Schwellwert in Prozent des gesamten Arbeitsspeichers. Ist mehr Arbeitsspeicher belegt, wird die Synchronisation temporär deaktiviert. Dies vermeidet Fehler durch zu knapp werdenden Arbeitsspeicher. Ein Wert von über 100 deaktiviert diese Funktion. Dies ist eine Schutzfunktion, die eine korrekte Funktion sicherstellt. Wird sie zu hoch eingestellt oder gar deaktiviert, kann dies zu Inkonsistenzen, Datenverlust und Programmabstürzen führen. Daher wird dringend

Eintrag (und Datentyp)	Standardwert	Erklärung
		empfohlen nicht vom Standardwert abzuweichen.
IMAP ID: ALLOW Send Id Info To Server (REG_DWORD)	1	Wenn 1, sendet der Groupware Client grundsätzlich Informationen über die lokal installierte Version und den Rechner über das IMAP-ID-Kommando an den IMAP-Server sowie per HTTPS an rss.intra2net.com. Der Umfang der übertragenen Informationen hängt von den anderen **`IMAP ID:`**-Schlüsseln ab.
IMAP ID: Send ONLY Product Version (REG_DWORD)	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 (REG_DWORD)	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 (REG_DWORD)	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 (REG_DWORD)	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 (REG_DWORD)	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 (REG_DWORD)	0	Wenn 0, wird ein nicht verbundener Posteingagsordner in `Meldungen` umbenannt. Wenn 1, behält der Ordner auch in unver-

Eintrag (und Datentyp)	Standardwert	Erklärung
		bundenem Zustand den Namen `Posteingang`. Wird der Ordner mit dem Server verbunden, ist er unabhängig von dieser Option immer `Posteingang` benannt.
SyncTemplatesFilePath (REG_SZ)	Installationsordner des Groupware Clients	Vollständigen Pfad des Ordners, aus dem die Datei `userdefined_sync_fields.xml` zur Definition benutzerdefinierter Felder geladen wird.
DoLastAuthorTagging (REG_DWORD)	1	Wenn 1 wird der Benutzername des letzten Bearbeiters bei jedem Objekt als Kategorie hinterlegt.
AutoSkipNewRemoteEmailFolder (REG_DWORD)	1	Wenn 0, werden bei aktivierter 1:1-Verbindung eines Kontos neu auf dem Server gefundene E-Mail-Ordner auch automatisch verbunden. Wenn 1, werden nur neu gefundene Groupware-Ordner automatisch verbunden.
StateSICompletion_Default (REG_DWORD)	0x01	Standardmodus für das Herunterladen von neuen E-Mails. 0x01 Nur Kopfzeilen 0x07 Vollständiger Inhalt Dieser Eintrag betrifft nur die Standardeinstellung. Über den in Abschnitt 26.1, „E-Mails komplett oder nur Kopfzeilen abrufen“ beschriebenen Weg können die Einstellungen weiterhin pro Ordner konfiguriert werden.
StateSICompletion_Fixed (REG_DWORD)	0	Wenn 1, wird ausschließlich der in StateSICompletion_Default festgelegte Modus für das Herunterladen von E-Mails verwendet. Der Benutzer hat keine Möglichkeit mehr den Modus über das Menü "Optionen" anzupassen.
UseRemoteIcon (REG_DWORD)	0	Wenn 1, werden bisher nur als Kopfzeilen vorliegende E-Mails mit einem speziellen Symbol (zeigt ein Telefon) in der Ordneransicht gekennzeichnet. Dieser Wert wird nur in dem Moment ausgewertet, in dem eine neue E-Mail nur mit Kopfzeilen vom Server geholt wird. Eine Änderung dieser Einstellung wirkt sich nicht auf bereits vorliegende E-Mails aus.
IconPreferAnsweredOverForwarded (REG_DWORD)	1	Wenn 1, wird bei E-Mails, die sowohl weitergeleitet, als auch beantwortet wurden, das "beantwortet"-Symbol angezeigt. Wenn 0, wird das "weitergeleitet"-Symbol angezeigt.

Eintrag (und Datentyp)	Standardwert	Erklärung
InitialReminderSetting (REG_SZ)	Crea-tor,Owner	Legt fest, für welche Benutzer eine Erinnerung beim Erstellen eines Termins oder einer Aufgabe hinterlegt wird. Creator Benutzer der den Termin anlegt Owner Eigentümer des Ordners, in dem der Termin gespeichert wird Die Werte werden mit Komma getrennt und ohne Leerzeichen eingegeben. Diese Einstellung gilt nur für das Anlegen eines neuen Termins oder Aufgabe, nicht für das Ändern bereits bestehender. Wird nur der Wert "Owner" eingestellt und ein neuer Termin mit Erinnerung in einem fremden Ordner angelegt, so wird aus technischen Gründen dennoch immer zusätzlich zur serverseitig gespeicherten Erinnerung für den Eigentümer des Ordners lokal eine Erinnerung im Outlook des Benutzers hinterlegt. Ist sie nicht gewünscht, kann der Benutzer sie nach dem Anlegen des Termins wieder entfernen ohne dabei die Erinnerung für den Eigentümer zu beeinflussen. Dieser Wert beeinflusst nur neu erstellte Termine oder Aufgaben. Eine Änderung dieser Einstellung wirkt sich nicht auf bereits vorliegende Termine oder Aufgaben aus.
ReminderChangesHandling (REG_SZ)	(leer)	Legt fest, wie Erinnerungen in Ordnern anderer Nutzer gehandhabt werden sollen. **`SharesInitFromOwner`** bedeutet, dass beim ersten Abruf eines Termins oder einer Aufgabe vom Server die Erinnerungseinstellungen des Eigentümers des Ordners einmalig übernommen werden. Danach wird die Erinnerung für den lokalen Nutzer vollkommen unabhängig von der des Eigentümers des Ordners behandelt. **`SharesAsOwner`** bedeutet, dass die Erinnungen für den lokalen Nutzer immer genauso wie für den Eigentümer des Ordners behandelt werden. Dieser Wert beeinflusst nur neu vom Server geholte Termine oder Aufgaben. Eine Änderung dieser Einstellung wirkt sich nicht

Eintrag (und Datentyp)	Standardwert	Erklärung
		auf bereits vorliegende Termine oder Aufgaben aus.
CntMaxFldToAllowAllBackground (REG_DWORD)	600	Sind beim Start von Outlook mehr Ordner verbunden als dieser Schwellwert, so werden nur noch die Ordner der obersten Ebene regelmäßig automatisch und im hinterlegten Intervall synchronisiert und alle anderen nur bei Öffnen des Ordners durch den Benutzer in Outlook. Werden zu viele Ordner automatisch synchronisiert, reicht das eingestellte Intervall nicht mehr aus um alle Ordner zu bearbeiten und es kommt zu Verzögerungen bei der Synchronisation.
PeriodicRecoverDelayMax (REG_DWORD)	0x001b7740 (= 30min)	Intervall in Millisekunden, in dem der Standardkalender auf noch nicht zum Server geschriebene lokale Änderungen durchsucht wird. Kleinstmöglicher Wert ist 0xEA60. Der Wert 0xffffffff bedeutet, das diese Funktion deaktiviert ist.
SendSyncOutDelayMax (REG_DWORD)	0x001b7740 (= 30min)	Intervall in Millisekunden, in dem der Standardordner für gesendete E-Mails jeder Datendatei auf noch nicht zum Server geschriebene E-Mails durchsucht wird. Kleinstmöglicher Wert ist 0xEA60. Der Wert 0xffffffff bedeutet, das diese Funktion deaktiviert ist.
RegMailAttrForBackGround (REG_SZ)	Mail,Groupware,MailBckGrnd,GroupwareBckGrnd	Steuert, für welche Ordnertypen Markierungen vom Server synchronisiert werden. Über Markierungen (Flags) werden Eigenschaften wie gelesen/ungelesen, markiert, gelöscht etc. einzelner Objekte übermittelt. Durch das Abschalten dieser Synchronisation kann die Performance erhöht werden. Mail — Aktuell selektierte Ordner mit E-Mails Groupware — Aktuell selektierte Ordner mit Groupwaredaten MailBckGrnd — Nicht selektierte Ordner mit E-Mails GroupwareBckGrnd — Nicht selektierte Ordner mit Groupwaredaten Einzelne Werte werden durch Kommas getrennt angegeben.

Eintrag (und Datentyp)	Standardwert	Erklärung
NoAutoIMAPAbo (REG_DWORD)	0	Wenn 1, wird beim Verbinden und Auflösen einer Verbindung eines E-Mail-Ordners kein IMAP-Abonnement angelegt bzw. aufgelöst.
FolderCollisionHandling (REG_SZ)	LikeOL	Steuert, wie Namenskollisionen beim Umbenennen oder Verschieben von Ordnern behandelt werden. Query: Der Benutzer wird gefragt Add: Der Ordner bekommt eine Zahl an den Namen angehängt LikeOL: Der Ordner bekommt eine Zahl an den Namen angehängt Merge: Der Inhalt der beiden gleichnamigen Ordner wird zusammengeführt
ApplyClassicFolderMove (REG_DWORD)	0	Wenn 1, werden Verschiebeoperationen von Ordnern lokal durchgeführt und als Lösch- und Hinzufügeoperationen für die einzelnen Objekte an den Server übermittelt. Dies ist wesentlich langsamer.
MailSourceCacheOff (REG_SZ)	On	Steuert, wie weit der vom Server gelesene Originalquelltext eines Objekts aufbewahrt wird. Durch das Weglassen dieser Informationen kann Speicherplatz in der Datendatei gespart werden. On: Originalquelltext und Metainformationen werden bis zum Größenlimit aus MailSourceCacheSzMax aufbewahrt MetaOnly: der Originalquelltext und Header werden nicht aufbewahrt, Metainformationen wie UID und Synchronisationszeitpunkt werden aber aufbewahrt HeaderOnly: Metainformationen wie UID und Synchronisationszeitpunkt sowie der Header-Teil des Originalquelltexts werden ohne Größenlimit aufbewahrt Off: Quelltext und Metainformationen werden gelöscht
MailSourceCacheSzMax (REG_DWORD)	16	Maximale Größe in Kilobytes bis zu der der Originalquelltext aufbewahrt wird, siehe MailSourceCacheOff.

Eintrag (und Datentyp)	Standardwert	Erklärung
FixDisabledAddIn (REG_DWORD)	1	Wenn 1, wird das Add-In (GUI) des Groupware Clients beim Start automatisch aktiviert.
NoWarnOnUnmappedStores (REG_DWORD)	0	Wenn 1, wird der Benutzer beim Start nicht gewarnt, falls es eine Datendatei des Groupware Clients gibt, bei der keine Ordner mit einem Server verbunden sind.
OnSrvSideFldDel_DelLocalAlways (REG_DWORD)	1	Steuert die Behandlung auf der Outlook-Seite, wenn ein Wurzelordner serverseitig gelöscht wird. Wenn 0, bleibt der Wurzelordner auf der Outlook-Seite erhalten und es wird nur die Verbindung entfernt. Wenn 1, wird der Wurzelordner auch auf der Outlook-Seite gelöscht. Dies betrifft aber nicht die Standard-Ordner von Outlook wie `Kontakte`, `Kalender` etc., da diese nicht gelöscht werden können.
MdnAllow (REG_DWORD)	0	Wenn 1, werden Anforderungen von Lesebestätigungen (MDNs) nicht aus eingehenden E-Mails entfernt. Dieser Wert beeinflusst nur neu vom Server geholte E-Mails. Eine Änderung dieser Einstellung wirkt sich nicht auf bereits vorliegende E-Mails aus.
AutoAddToAddressBook (REG_DWORD)	1	Wenn 1, werden neu verbundene Kontakteordner automatisch als Outlook-Adressbuch registriert.
NotifyThirdParties (REG_DWORD)	1	Wenn 1, werden mögliche Kompatibilitätsprobleme mit Programmen oder Add-Ins von Drittanbietern dem Nutzer gemeldet.
DisableSyncDialogs (REG_SZ)	(leer)	Deaktiviert Dialogfenster mit bestimmten Hinweisen und Fragen an den Benutzer dauerhaft. All — Alle Dialoge deaktiviert SlowFolderRenameIndication — Hinweis zu länger dauerndem Umbenennen eines Ordners RenameFolderAlsoOnServer — Frage ob ein Ordner nur lokal oder auch auf dem Server umbenannt werden soll

Eintrag (und Datentyp)	Standardwert	Erklärung
		MoveHandledAsCopyIndication: Hinweis, dass statt Verschieben ein Kopiervorgang ausgeführt wird MergeFolders: Frage ob ein Ordner kopiert oder mit einem bestehenden zusammengeführt werden soll FolderRenewIndication: Hinweis zur Erstellung einer Sicherungskopie bei auf dem Server erneuerten Ordnern Die Werte der zu deaktivierenden Dialoge werden mit Komma getrennt und ohne Leerzeichen und Bindestriche eingegeben.
OnRepair_Profiles (REG_DWORD)	0	Wenn 1, werden bei einer Reparaturinstallation des Groupware Clients alle Outlook-Profile mit Datendateien des Groupware Clients aller erreichbaren Nutzerkonten repariert. Bei 0 wird diese Reparatur nur bei dem Nutzerkonto durchgeführt, welches die Reparaturinstallation ausführt.
CategoryColorSyncRead (REG_DWORD)	1	Wenn 1, wird beim Hereinsynchronisieren von Groupware-Objekten vom Server die Kategorie-Farbzuordnung mit ausgewertet und evtl. in die Hauptkategorienliste übernommen. Bei 0 wird die auf dem Server abgelegte Kategorie-Farbzuordnung ignoriert.
CategoryColorSyncWrite (REG_DWORD)	1	Wenn 1, wird beim Raussynchronisieren von Groupware-Objekten mit Kategorien die lokale Kategorie-Farbzuordnung mit an den Server übermittelt. Bei 0 wird nur der Name der Kategorien geschrieben, nicht aber die lokal verwendete Kategorie-Farbzuordnung.

31.2.2. Einstellungen für das Add-In

Die Einstellungen für das Outlook Add-In (GUI) sind im Schlüssel `mxstore_GUI` zu finden.

Eintrag (und Datentyp)	Standardwert	Erklärung
Trace (REG_DWORD)	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 (REG_DWORD)	0x0000001b	Auswahl der Spalten, die bei einem zu protokollierenden Ereignis im Trace ausgegeben

Eintrag (und Datentyp)	Standardwert	Erklärung
		werden. Weitere Informationen erhalten Sie bei Bedarf über unseren Support.
TracerDisabled (REG_DWORD)	0	Hiermit wird ausgewählt, ob nur Starts und Fehler protokolliert werden (Wert 1) oder auch normale Vorgänge im Betrieb (Wert 0).
PathLog (REG_SZ)		Vollständiger Pfad, in dem die Tracedateien abgelegt werden. Ist dieser Eintrag nicht vorhanden, werden sie im `%LOCALAPPDATA%\Intra2net`-Verzeichnis abgelegt.
TraceSzMax (REG_DWORD)	170	Maximalgröße für eine Tracedatei in Megabytes. Bei Überschreiten dieser Größe wird die Datei rotiert.
TraceDaysToRemember (REG_DWORD)	14	Anzahl an Tagen, die Tracedateien maximal aufbewahrt werden.
AllowOwnRightsEdit (REG_DWORD)	1	Ist diese Einstellung aktiv, so darf der Benutzer seine eigenen Rechte auf einen Ordner bearbeiten.
AllowShareOwnerRightsEdit (REG_DWORD)	0	Beim Wert 1 darf der Benutzer die Rechte des Eigentümers eines Ordners bearbeiten. Dafür muss dem Benutzer das Recht "Ordner" für diesen Ordner vergeben sein.
ShowAdvancedOptions (REG_DWORD)	1	Ist diese Einstellung aktiv, so wird der Optionen-Dialog (u.a. zur Einstellung der Synchronisationshäufigkeit) angezeigt.
NotifyNewMail (REG_DWORD)	1	Bei 1 sind Benachrichtigungen über neue E-Mails aktiviert.
NotifyNewMailMaxInterval (REG_DWORD)	60	Zeit in Sekunden, in der nach einer Benachrichtigung über neue E-Mails keine weitere Benachrichtigung angezeigt wird.
NotifyNewMailMaxItems (REG_DWORD)	3	Maximale Anzahl von E-Mails, die in einer Benachrichtigung über neue E-Mails angezeigt werden.
NotifyNewMailTimeOnMouseOverMs (REG_DWORD)	1000	Zeit in Millisekunden nach der sich eine Benachrichtigung über neue E-Mails schließt wenn der Mauszeiger im Bereich der Benachrichtigung ist.
NotifyNewMailInitialDelay (REG_DWORD)	5	Wartezeit in Sekunden bis nach dem Eingang einer neuen E-Mail eine Benachrichtigung angezeigt wird.
NotifyNewMailMaxAge (REG_DWORD)	120	Maximales Alter von ungelesenen E-Mails in Minuten für die Benachrichtigungen über neue E-Mails angezeigt werden. Zur Berechnung des Alters wird der Eingangszeitpunkt auf dem Server verwendet.

Eintrag (und Datentyp)	Standardwert	Erklärung
SyncStateFetchInterval (REG_DWORD)	5	Intervall in Sekunden in dem die Anzeige im Sync-Status-Menü aktualisiert wird.
UpdateCheckEnabled (REG_DWORD)	1	Bei 1 wird beim Start des Groupware Clients geprüft, ob eine neue Version verfügbar ist. Prüfung über einen HTTPS-Zugriff zu rss.intra2net.com, maximal ein Zugriff pro Kalendertag.
EnableIncellEditClose (REG_DWORD)	1	Bei 1 werden direkt in einer Übersichtsmaske editierte Elemente beim Verlassen forciert geschlossen und können damit dann zum Server synchronisiert werden.
OlReceiveRulesEnabled (REG_DWORD)	0	Mit dem Wert 1 werden die clientseitigen Sortierregeln aktiviert. Dies ist nur in Ausnahmefällen sinnvoll und birgt Risiken u.a. von Duplikaten, verwenden Sie statt dessen besser serverseitige Sortierregeln.
DfltLinkMode (REG_SZ)	OlHide,SrvOwnAuto,SrvShareTree,SrvOwnTree,SrvOwnRooted	Steuert die Ordneransicht im "Ordner verbinden"-Dialog. Der Wert "OlHide,SrvOwnAuto,SrvShareTree,SrvOwnTree,SrvOwnRooted" entspricht Expertenmodus aus, "SrvOwnAuto,SrvShareTree,SrvOwnTree,SrvOwnRooted" entspricht Expertenmodus an.

31.3. 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 https://www.intra2net.com/de/download/manuals/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

32. Kapitel - Einführung in die Web-Groupware

Die Web-Groupware ermöglicht es, mit einem gewöhnlichen Webbrowser auf E-Mails und Groupwaredaten wie Kalender, Aufgaben, Kontakte und Notizen zuzugreifen.

Sie ist auf der Oberfläche des Intra2net Systems über das Menü "Groupware" erreichbar. Beim Zugriff aus dem Internet ohne das Recht "Fernadministration über HTTPS" (Menü " Benutzermanger > Gruppen : Administrationsrechte") öffnet sie sich direkt nach dem Login.

32.1. 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 Intra2net System kann man auswählen, welchen Anzeigemodus man verwenden möchte. Standardmäßig versucht das System anhand der Browserkennung automatisch den am besten passenden Anzeigemodus zu ermitteln (Einstellung "Automatisch").

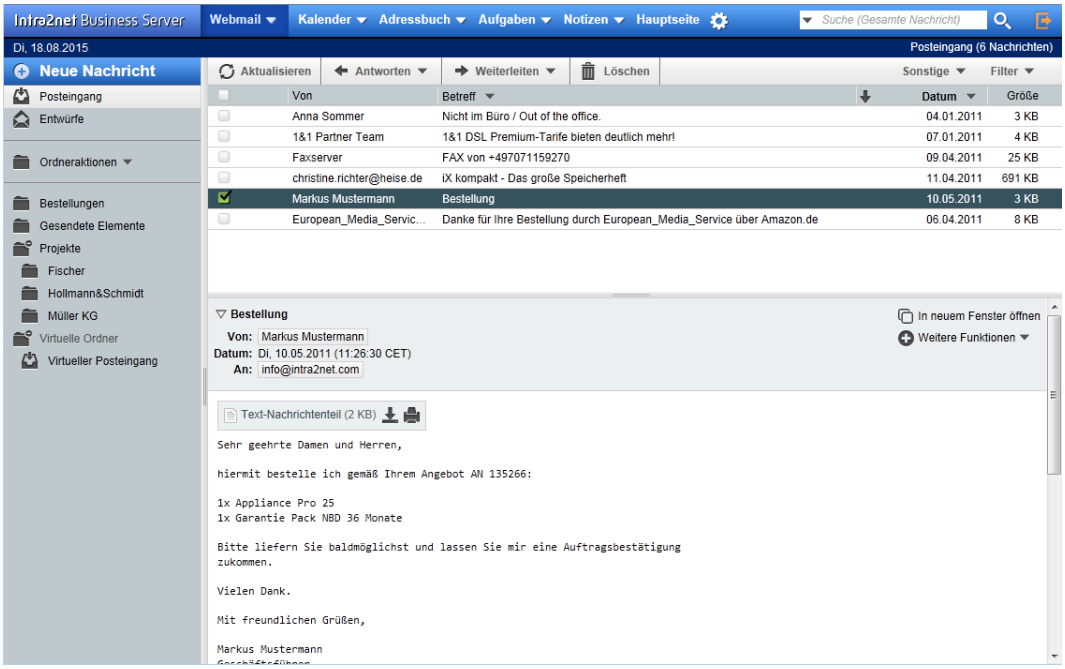
Die folgende Dokumentation bezieht sich auf den dynamischen Modus.

33. Kapitel - E-Mail

33.1. E-Mails lesen und bearbeiten

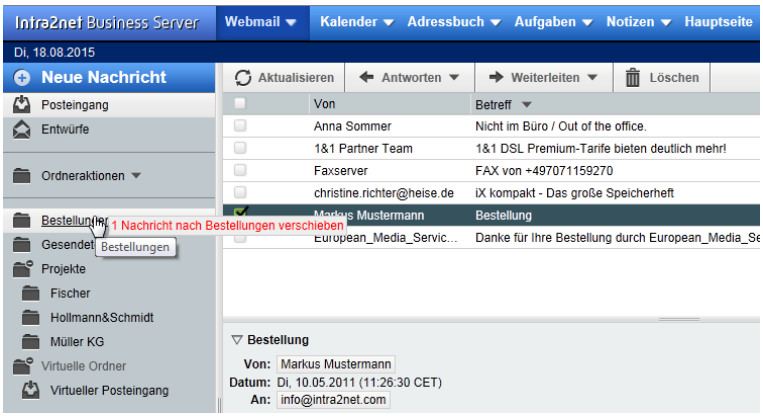
33.1.1. E-Mails anzeigen

Unter dem Menüpunkt "Webmail" findet sich in der Web-Groupware die Möglichkeit, E-Mails zu lesen, zu schreiben und zu bearbeiten.



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.



33.1.2. Gelöschte E-Mails

E-Mails werden durch den Löschbefehl in den Papierkorb verschoben.

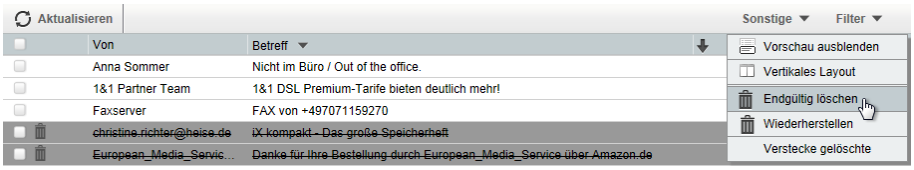
Soll eine gelöschte E-Mail wiederhergestellt werden, so kann Sie ganz normal per Drag&Drop aus dem Papierkorb wieder in den richtigen Ordner zurück verschoben werden.

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*).



Sie können die so markierten E-Mails mit der Webgroupware endgültig löschen oder ausblenden. Diese Funktionen finden Sie im Menü "Sonstige".



33.1.3. E-Mails exportieren

Um einzelne E-Mails in anderen Programmen weiterzuverarbeiten oder sie für die Fehlersuche genauer analysieren zu können, gibt es die Möglichkeit E-Mails im RFC822-Format (zum Teil auch nach der Dateiendung .EML genannt) zu exportieren.

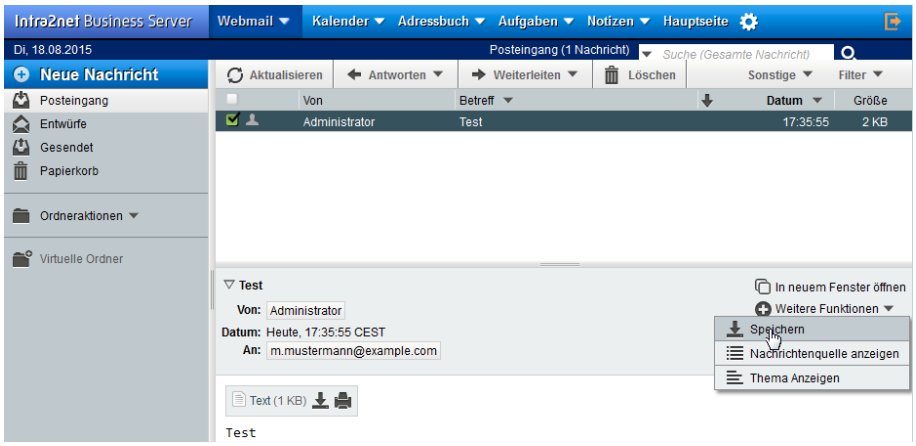
Gehen Sie dafür wie folgt vor:

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.



4. 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.

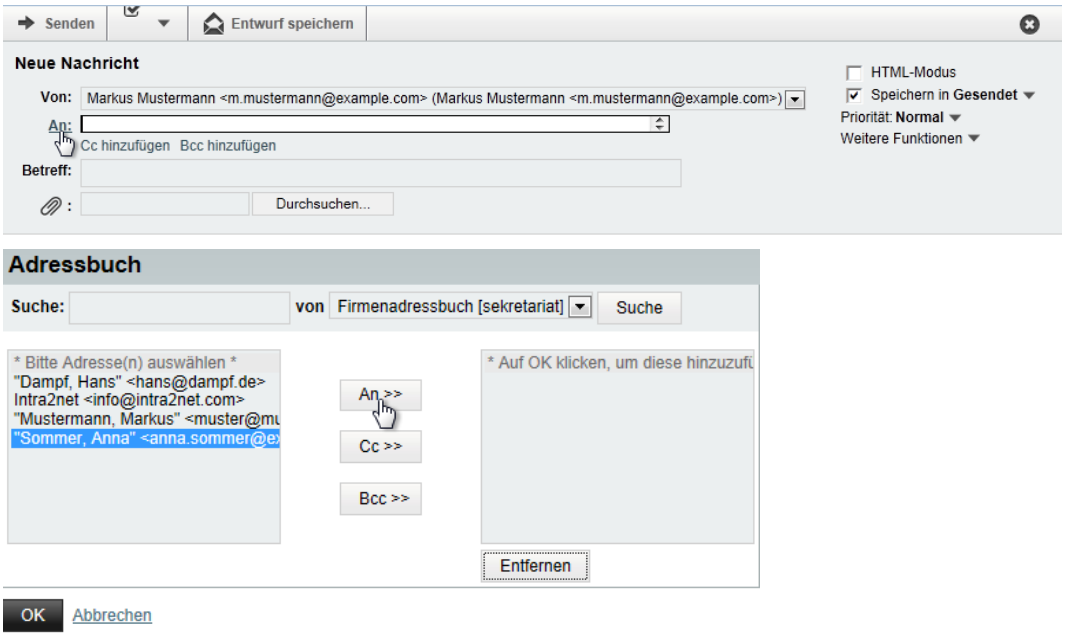
33.2. E-Mails senden

33.2.1. 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.

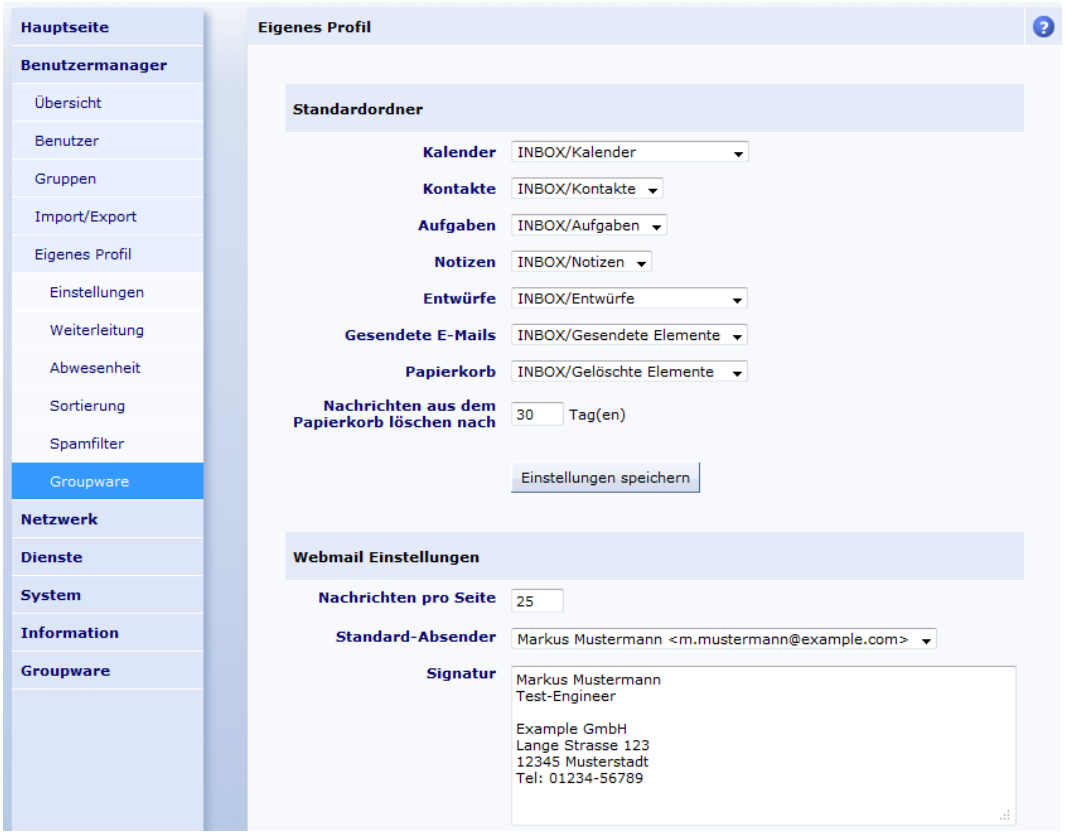
Alternativ kann man auf "An" klicken, um passende Empfänger aus den Adressbüchern hinzuzufügen.



33.2.2. 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.

33.3. Ordner verwalten

33.3.1. Ordnerhierarchie

In der linken Bildschrimhälfte 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.

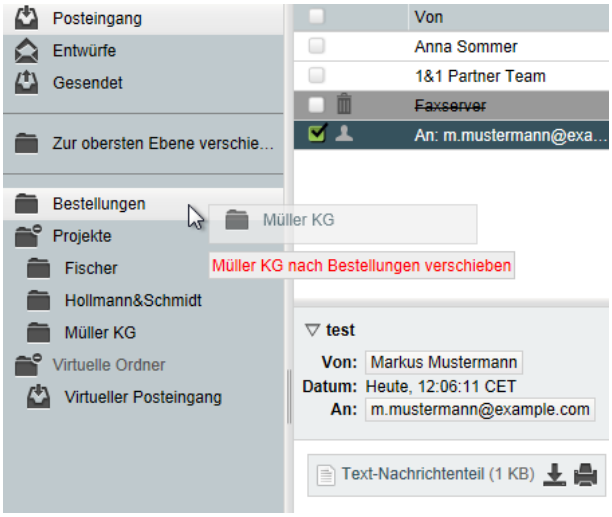
Der tatsächliche Name dieser Ordner kann im Menü "Benutzermanager > Eigenes Profil > Groupware" bzw. vom Administrator im Menü "Benutzermanager > Benutzer : Groupware" konfiguriert werden.

Alle weiteren Unterordner des Benutzers werden unterhalb von "Ordneraktionen" in alphabetischer Reihenfolge dargestellt.

33.3.2. 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.



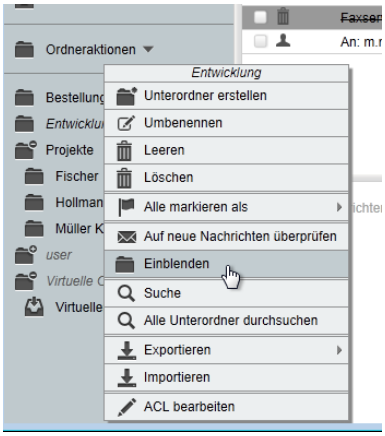
33.3.3. Ordner abonnieren

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 abonnieren Ordner angezeigt, diese werden mit kursivem Ordernamen dargestellt.



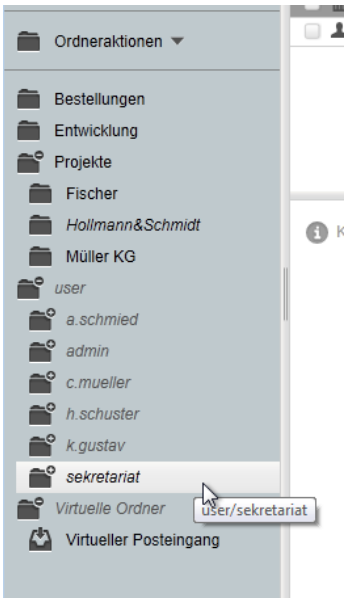
Um einen Ordner zu abonnieren, öffnen Sie mit der rechten Maustaste das Kontextmenü des entsprechenden Ordners und wählen "Einblenden".



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.

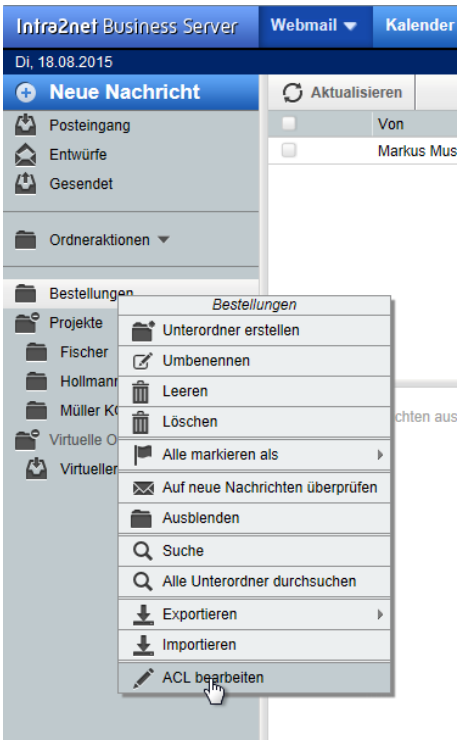
Hat ein anderer Benutzer Ihnen einen seiner E-Mail-Ordner freigegeben, so ist dieser in der Hierarchie `user` und darunter dem Benutzerlogin zu finden. Hat ein anderer Benutzer Ihnen seinen Posteingang freigegeben, so entspricht das dem Benutzernamen selbst; es wird kein Unterordner `Posteingang` angezeigt.



Freigegebene Ordner anderer Benutzer sind nach der Freigabe erst mal versteckt und müssen wie oben beschrieben abonniert werden bevor sie dauerhaft angezeigt werden.

33.3.4. 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 Intra2net System, also z.B. **`group:Alle`**.



34. Kapitel - Adressbuch



Hinweis

Dieses Kapitel, sowie weitere über Kalender und Aufgaben, sind momentan noch in Arbeit und werden in Kürze veröffentlicht.

35. Kapitel - Mobile Geräte per ActiveSync anbinden

35.1. 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 Intra2net Lizenzen nutzbar, die die Funktion Mail Server enthalten.

35.2. Einstellungen auf dem Server

Um Geräte per ActiveSync mit dem Intra2net System zu verbinden, müssen auf dem Server zuerst folgende Grundeinstellungen vorgenommen bzw. überprüft werden:

1. Prüfen Sie, wie das Intra2net System 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 Intra2net System 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 Intra2net Systems 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. Das Intra2net System muss für das Mobilgerät über einen DNS-Namen im Internet adressierbar sein.

   Hat das Intra2net System eine feste IP, richten Sie für diese einen DNS-Eintrag in der eigenen offiziellen Domain ein. Das System ist dann unter einem Namen wie z.B. **`intra.kundenname.de`** oder **`mail.example.com`** erreichbar. Dies kann normalerweise beim Webspace-Provider, der die eigene Domain verwaltet, kostenlos und zeitnah eingerichtet werden.

   Bekommt das Intra2net System bei jeder Interneteinwahl eine andere IP zugewiesen, muss zur Adressierung ein DynDNS-Dienst eingerichtet werden. Siehe hierfür Abschnitt 11.13, „DynDNS“.

   Eine feste IP kann nicht direkt und ohne DNS-Namen verwendet werden, da Zertifizierungsstellen keine Zertifikate auf IPs ausstellen dürfen.

4. Der Zugriff auf ActiveSync findet ausschließlich über HTTPS statt. Für die Verschlüsselung wird daher ein passendes Zertifikat benötigt, welches von einer externen Zertifizierungsstelle auf den externen DNS-Namen (siehe oben) ausgestellt wurde. Gehen Sie wie in Abschnitt 10.5, „Verwenden einer externen Zertifizierungsstelle“ beschrieben vor, um dieses Zertifikat einzurichten.

   Wir raten dringend davon ab zu versuchen die ActiveSync-Verbindung mit einem selbstsignierten Zertifikat aufzubauen. Bei vielen Geräten erfordert dies eine komplexere Konfiguration und/oder gefährdet die Sicherheit der Verbindung. Das Einrichten eines Zertifikats einer externen Zertifizierungsstelle ist dagegen einfach, schnell, kostenlos und sicher.

5. Testen Sie, ob der Zugriff auf HTTPS aus dem Internet funktioniert sowie die Zertifikate korrekt konfiguriert sind. Verwenden Sie hierfür das Menü "System > Diagnose > Externes HTTPS".

6. 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.

7. 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.

8. 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.

9. Konfigurieren Sie die einzelnen Geräte wie in den folgenden Kapiteln beschrieben.

35.3. Besonderheiten und Tipps

35.3.1. 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.

35.3.2. Synchronisationsschritte

Meldet sich das Mobilgerät am Intra2net System zur Synchronisation, bekommt es alle Änderungen seit der letzten Synchronisation mitgeteilt und aktualisiert daraufhin seine

Daten. Genauso werden auf dem Mobilgerät vorgenommene Änderungen an das Intra2net System 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.

35.3.3. Geräte verwalten und neu synchronisieren

Auf dem Intra2net System 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 Datenkonsistenzprobleme gelöst werden. Dies wird auch automatisch beim Rückspielen eines Backups des Intra2net Systems ausgelöst.

35.3.4. 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.

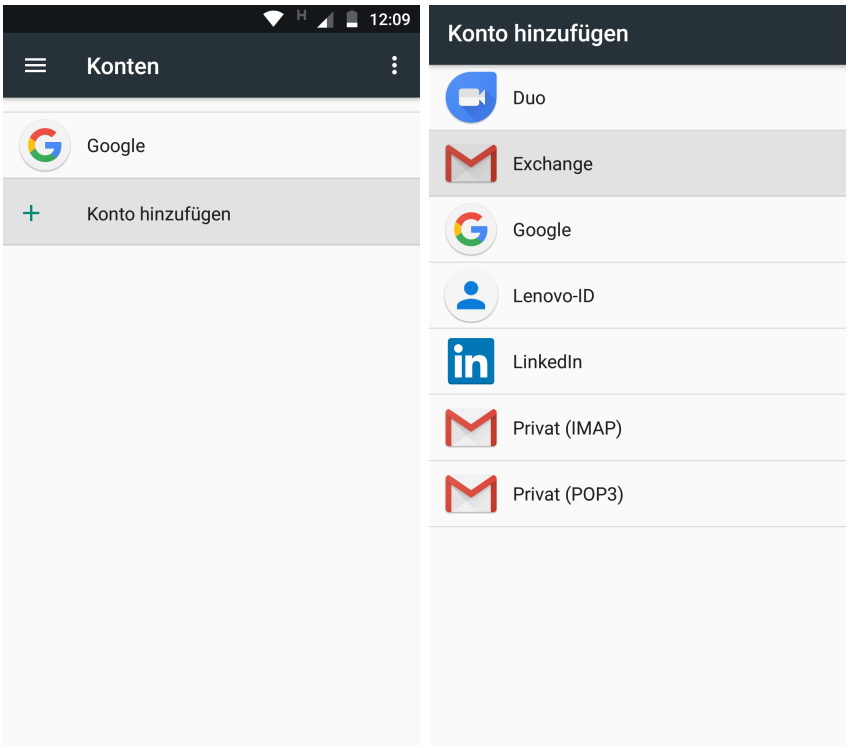
36. Kapitel - ActiveSync mit Android-Geräten

Bevor Sie das Gerät konfigurieren können, müssen Sie das Intra2net System für die Anbindung vorbereiten. Führen Sie dazu die in Abschnitt 35.2, „Einstellungen auf dem Server“ beschriebenen Schritte durch.

Gehen Sie danach zur Konfiguration des Geräts wie folgt vor:

1. Stellen Sie als erstes sicher, dass die Zugangsdaten vertraulich bleiben. Die dafür nötigen Schritte werden in Abschnitt 52.1, „Gerät vorbereiten“ beschrieben.

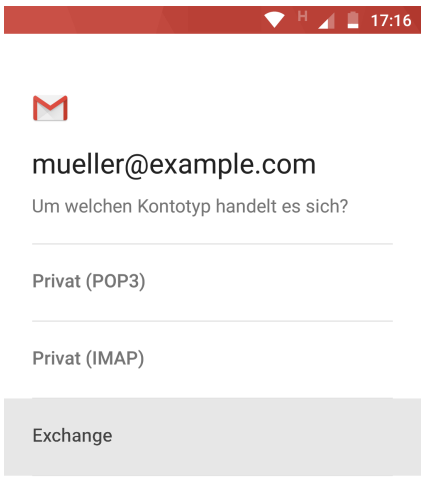
2. Öffnen Sie auf dem Android-Gerät die "Einstellungen", Menüpunkt "Konten" und wählen "Konto hinzufügen". Der Typ des hinzuzufügenden Kontos ist "Exchange".



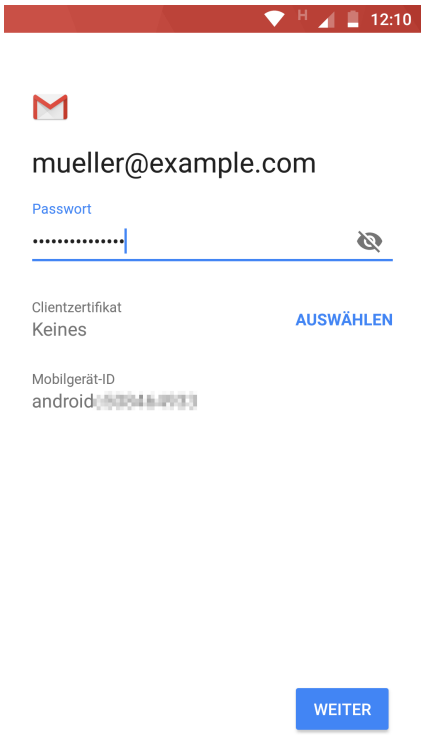
3. Geben Sie Ihre E-Mail-Adresse ein. Wählen Sie dann "Manuell Einrichten".



4. Wählen Sie "Exchange" als Kontotyp.

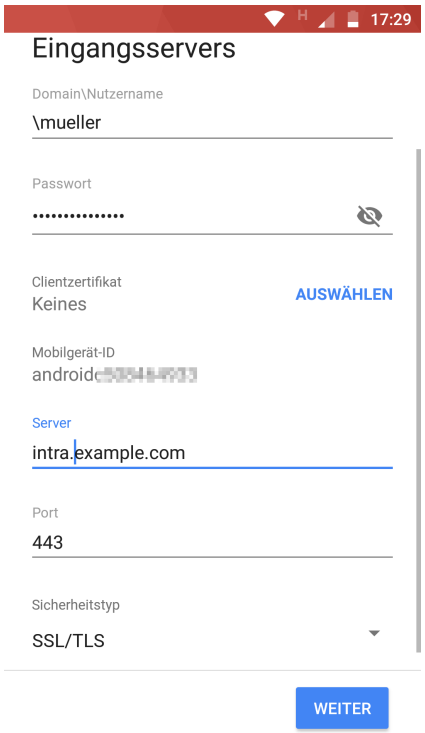


5. Geben Sie das Passwort des Benutzers auf dem Intra2net System ein.



6. Tragen Sie unter "Domain/Nutzername" einen \ (*Backslash*) direkt gefolgt vom Benutzernamen auf dem Intra2net System ein. Benutzernamen auf dem Intra2net System bestehen ausschließlich aus Kleinbuchstaben, geben Sie daher hier auch ausschließlich Kleinbuchstaben ein.

   Tragen Sie im Feld "Server" den externen DNS-Namen des Intra2net Systems ein. Der Sicherheitstyp muss auf "SSL/TLS" stehen.



7. Es darf keine Meldung über einen Zertifikatsfehler erscheinen. Sollte eine solche erscheinen, so brechen Sie hier ab und prüfen Sie die in Abschnitt 35.2, „Einstellungen auf dem Server“ beschriebenen Schritte.

8. Als nächstes wird konfiguriert, wie häufig Daten zwischen Server und Mobilgerät synchronisiert werden sollen.

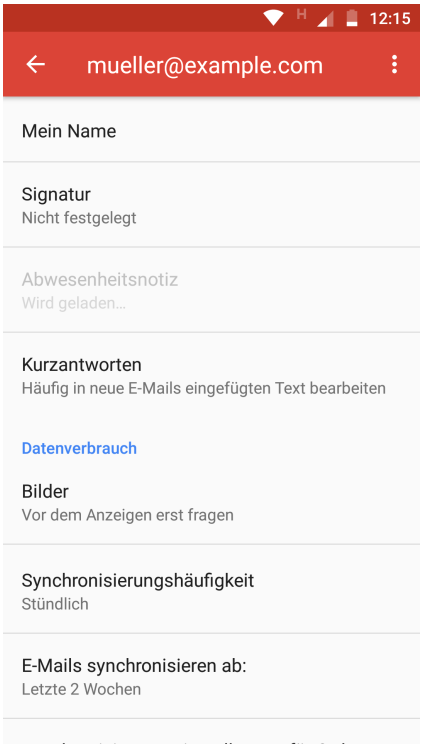


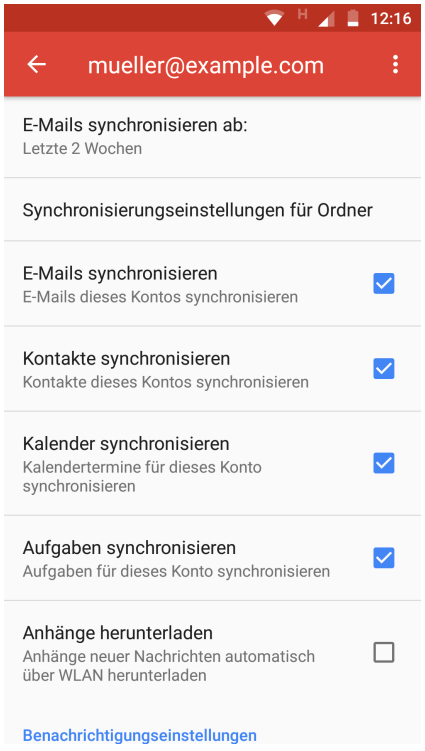
Tipp

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. Außerdem haben wir bei einigen Geräten im Push-Modus Übertragungsfehler beobachtet, die zu einer Verdoppelung 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.





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.

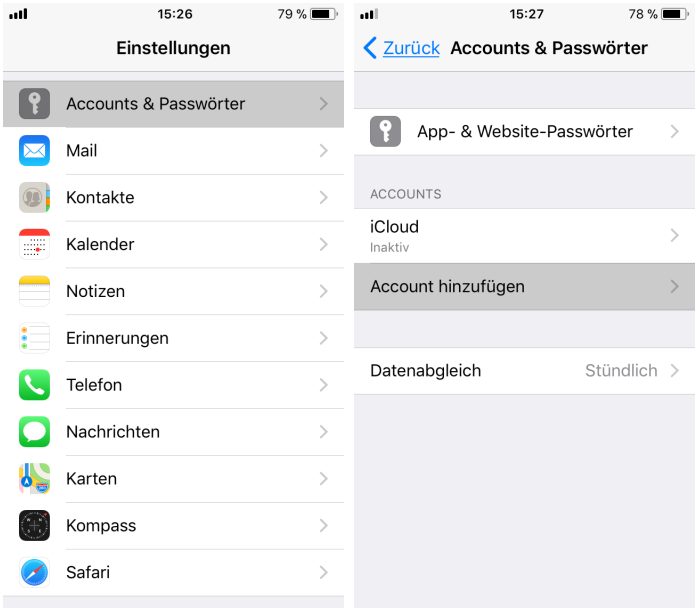
Alle betroffenen Applikationen bieten auch die Möglichkeit, manuell eine Synchronisation der Daten auszulösen. Diese Möglichkeit ist einem sehr kurzen Synchronisationsintervall typischerweise vorzuziehen.

37. Kapitel - ActiveSync mit Apple iOS-Geräten

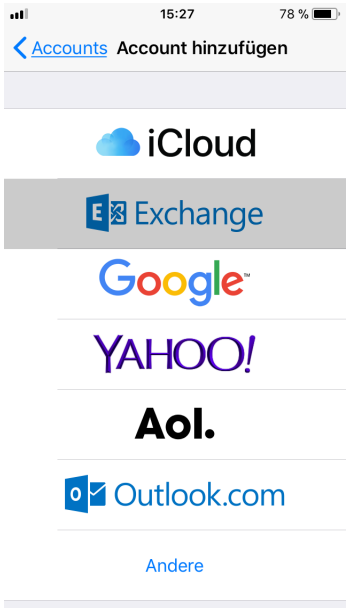
Bevor Sie das Gerät konfigurieren können, müssen Sie das Intra2net System für die Anbindung vorbereiten. Führen Sie dazu die in Abschnitt 35.2, „Einstellungen auf dem Server“ beschriebenen Schritte durch.

Gehen Sie danach zur Konfiguration des Geräts wie folgt vor:

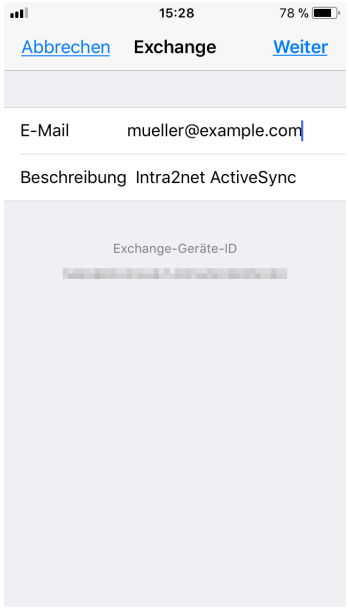
1. Öffnen Sie die "Einstellungen", Unterpunkt "Accounts & Passwörter" und wählen "Account hinzufügen".



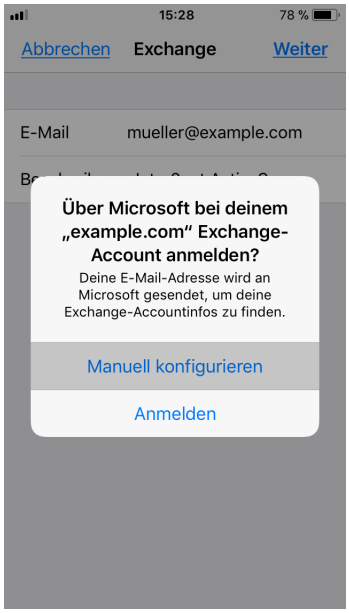
2. Der Typ des hinzuzufügenden Kontos ist "Exchange".



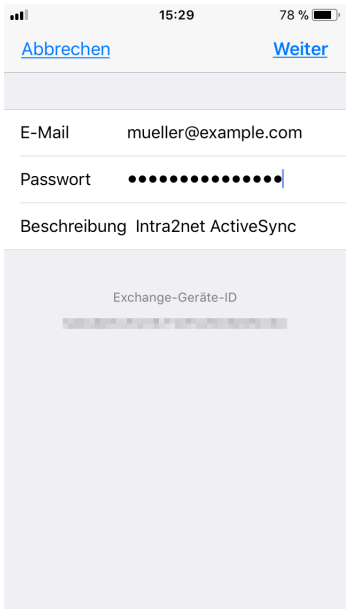
3. Tragen Sie die E-Mail-Adresse und einen Namen für das Konto auf dem iOS-Gerät ein.



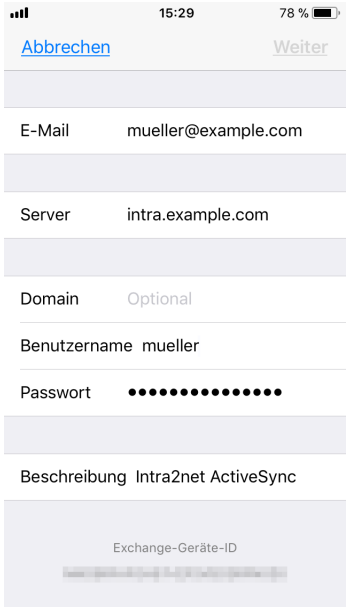
4. Wählen Sie "Manuell konfigurieren".



5. Tragen Sie das Passwort des Benutzerkontos auf dem Intra2net System ein.

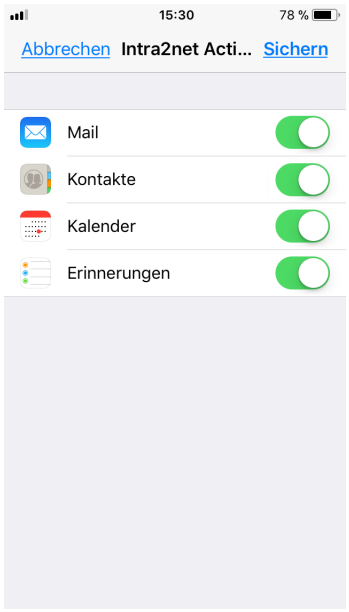


6. Tragen Sie den externen DNS-Namen des Intra2net Systems im Feld "Server" ein. Tragen Sie den Benutzernamen (Login) des Kontos auf dem Intra2net System ein. Lassen Sie das Feld "Domain" leer.



7. Es darf keine Sicherheitswarnung oder Meldung zu einem Zertifikatsfehler erscheinen. Sollte eine solche erscheinen, so brechen Sie hier ab und prüfen Sie die in Abschnitt 35.2, „Einstellungen auf dem Server“ beschriebenen Schritte.

8. Wählen Sie, welche Objekttypen Sie synchronisieren möchten.

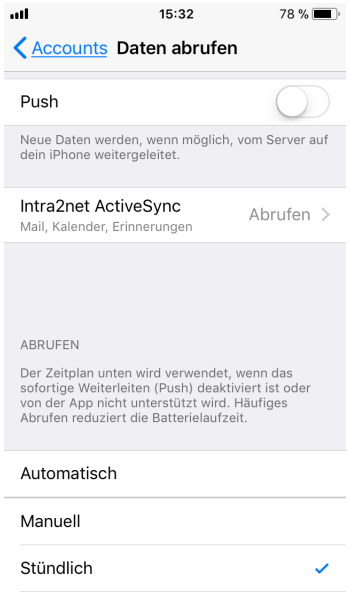


9. Öffnen Sie als letztes das Menü "Datenabgleich" und stellen ein, wie häufig die Daten synchronisiert werden sollen.



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 Synchronisationsintervall typischerweise vorzuziehen.

38. Kapitel - Referenzinformationen



Hinweis

Die in diesem Kapitel aufgeführten Informationen gelten ausschließlich für die Webgroupware und Activesync. Informationen zum Intra2net Groupware Client finden Sie im 31. Kapitel, „Referenzinformationen“.

Die Webgroupware und die ActiveSync-Schnittstelle unterstützen nicht alle Felder, die per ActiveSync oder vom Intra2net Groupware Client gesendet werden können. Die in diesen Feldern gespeicherten Daten können daher in der Webgroupware oder über ActiveSync nicht angezeigt, genutzt oder bearbeitet werden. Außerdem können die darin gespeicherten Daten beim Ändern anderer Felder des selben Objekts verloren gehen.

Mindestens folgendes wird in der Webgroupware und Activesync nicht unterstützt:

- Bilder in Kontakten
- Termin- und Aufgabenserien mit dem Wiederholungstyp "Arbeitswoche" sowie Wiederholungstyp monatlich bei Vorgabe des letzten Wochentags (z.B. "letzer Montag jedes Monats")
- Ausnahmen in Termin- und Aufgabenserien, bei denen im Vergleich zur Serie mehr geändert wird, als dass ein Element der Serie komplett entfällt
- Farbdarstellung von Kategorien: Kategorien werden nur textuell angezeigt
- Verarbeitung von per E-Mail eingehenden Aufgabenzuweisungen
- Kontaktgruppen
- Erinnerungen und Nachverfolgen-Markierung von E-Mails
- Anfügen anderer Elemente oder Dateien an Groupware-Objekte (nicht E-Mails, hier sind Anhänge selbstverständlich möglich)
- Verknüpfen von Groupware-Objekten untereinander, z.B. mit Kontakten
- Als privat markierte Groupware-Objekte werden in einigen Sonderfällen dem Besitzer nicht mehr angezeigt
- Telefonnummern im Feld "Telefonzentrale Firma". Nutzen Sie stattdessen "Telefon geschäftlich"

Für Activesync gilt weiterhin die Einschränkung, dass pro Groupware-Objekttyp (Termin, Adresse, Aufgabe,...) immer nur ein Ordner übertragen wird. Diese Einschränkung kann durch das Einrichten zusätzlicher Konten abgemildert werden, siehe hierzu Abschnitt 35.3.4, „Synchronisieren von mehreren Kalendern oder Kontakteordnern“.

Weitere Informationen folgen in Kürze. Sollten Sie bis dahin detailliertere Informationen zur Unterstützung einzelner Datentypen oder Funktionen benötigen, so wenden Sie sich bitte an den Intra2net Vertrieb.

Teil 5. Firewall

39. Kapitel - Auswahl der Firewall-Regellisten

Die Firewall des Intra2net Systems 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.

39.1. 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 Rechteblock 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-Profils überhaupt zum Tragen.

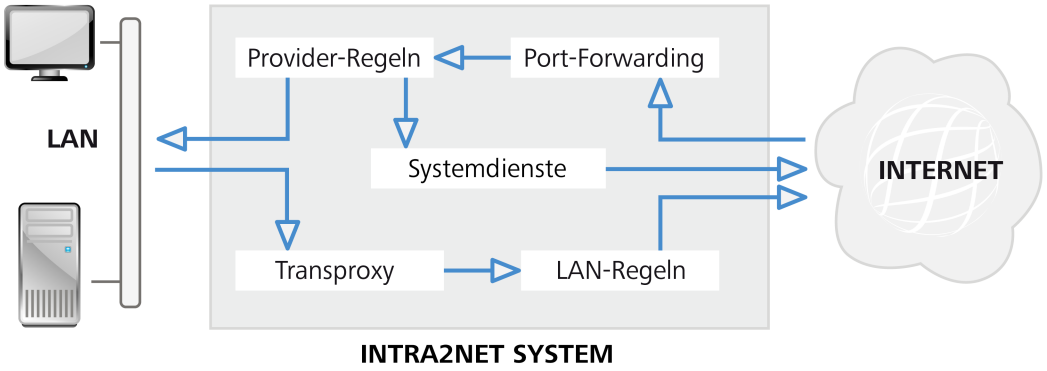
39.2. Regellisten fürs Internet

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.

39.3. Weg der Pakete durch die Firewall

39.3.1. Paketwege im LAN und Internet



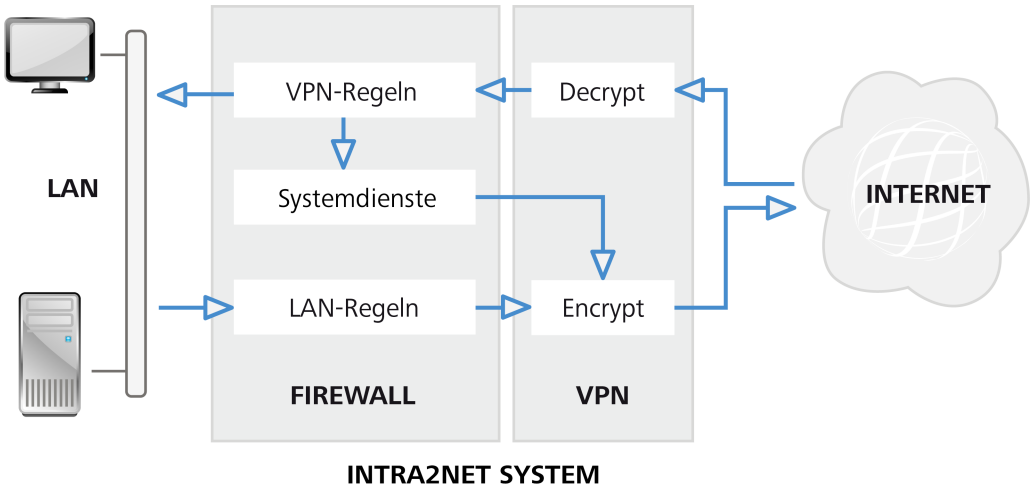
Der Weg der Pakete lässt sich relativ einfach zusammenfassen:

- 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 Intra2net Systems selbst können nicht beschränkt werden.

39.3.2. 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.


VPN-Regeln
Decrypt
Systemdienste
LAN
INTERNET
LAN-Regeln
Encrypt
FIREWALL
VPN
INTRA2NET SYSTEM

40. 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 Intra2net System 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.

40.1. 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 das Intra2net System selbst, erlauben aber keinerlei Zugriff ins Internet oder auf E-Mails.

„Basis LAN“ erlaubt den Zugriff auf folgende Dienste des Intra2net Systems:

- DNS
- Weboberfläche per HTTPS
- Windows-Freigabe (SMB) für Backups
- ICMP-Basisdienste wie z.B. Ping
- SSH für Zugriff auf die Systemkonsole des Intra2net Systems

„Basis LAN und lokale Netze“ erlaubt zusätzlich noch vollen Zugriff auf alle anderen an das Intra2net System 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.

40.2. 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 das Intra2net System 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 Intra2net Systems 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. „Proxyzwang“ 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 das Intra2net System alle Zugriffe auf HTTP-Server für den Benutzer unsichtbar auf den Proxy des Intra2net Systems 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 Intra2net System" sorgt dafür, dass die E-Mail-Protokolle auf das Intra2net System beschränkt werden. Damit wird der Zugriff von E-Mail-Programmen direkt auf Mailserver im Internet unterbunden und so sichergestellt, dass alle E-Mails über das Intra2net System laufen müssen. Dies macht Sinn um z.B. dafür zu sorgen, dass der E-Mail-Virenscanner oder eine Archivierungsfunktion nicht umgangen werden können.

40.3. Providerprofile

Providerprofile sind sehr einfach strukturiert. Jeder der Dienste, auf die typischerweise von außen auf das Intra2net System zugegriffen wird, kann separat freigeschaltet werden.

Die Providerprofile decken nur den Zugriff auf das Intra2net System selbst sowie Port-Forwarding ab. Soll eine De-Militarized-Zone (DMZ) verwendet werden, muss eine Vollständige Regelliste konfiguriert werden.

41. Kapitel - Vollständige Regellisten

Vollständige Firewall-Regellisten erlauben die volle Funktionalität der Firewall einzusetzen und sind daher etwas komplexer zu konfigurieren als die Firewall-Profile.

41.1. 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.

41.1.1. 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 komplette Portbereiche (wie z.B. Zielports 5000 bis 5050 für die Fernwartung des Intra2net Supports) 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 Intra2net System eingetragen.

41.1.2. 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 Intra2net System 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.

41.1.3. Netzgruppen mit DNS-Rechnernamen

In Netzgruppen können nicht nur, wie im vorherigen Abschnitt beschrieben, IP-basierte Objekte eingetragen werden, sondern auch DNS-Rechnernamen.

Das Intra2net System aktualisiert die eingetragenen DNS-Rechnernamen ständig automatisch im Hintergrund und passt die Firewall-Regellisten ggf. an. Löst ein DNS-Rechnername auf mehrere IP-Adressen auf, werden diese alle in die Netzgruppe eingefügt.

Im Menü "Information > System > DNS Netzgruppen" ist eine Übersicht über alle momentan zu den DNS-Rechnernamen aufgelösten IP-Adressen zu sehen. Bei Bedarf kann über den Link "Erneuern" ein DNS-Rechnername manuell neu aufgelöst werden.

Einige Dienstanbieter setzen Gruppen von ständig rotierenden IP-Adressen ein, z.B. für Load-Balancing. Um damit umzugehen belässt das Intra2net System eine IP-Adresse noch 24 Stunden länger in der Liste, auch wenn sie momentan nicht mehr in der DNS-Auflösung enthalten ist. Diese Funktion wird *Extended Hold* genannt und die betroffenen IP-Adressen mit "(EH)" in der Übersicht gekennzeichnet.

41.1.4. Automatische Objekte

Das Intra2net System 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 Intra2net System definierten Rechner und Bereiche. Bei DHCP-Bereichen betrifft dies nur die belegten IPs.
DHCP-Bereiche	Alle DHCP-Bereiche (auch die nicht belegten IPs).
Entfernte VPN Netze	Die Netze hinter den aktuell aktiven VPN-Gegenstellen. Bei „LAN zu Host"-Verbindungen ist dies die VPN-Gegenstelle selbst.
IPs des Systems im LAN	IP-Adressen des Intra2net Systems 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 Intra2net Systems im Internet. Ist das System offline, so trifft diese Bedingung nicht mehr zu.
Internet	Alles außerhalb der lokalen Netze und VPNs.

41.2. Regellisten

41.2.1. 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 das Intra2net System 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.

41.2.2. 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).

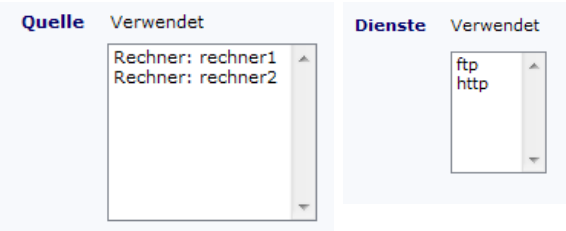
Trifft keine Regel einer Regelliste zu, wird das Paket verworfen (implizites Deny). Dies wird durch die unveränderliche Regel am Schluss der Regelliste visualisiert. Wird ein Paket an eine andere Regelliste weitergeleitet und trifft dort keine Regel zu, wird das Paket an die ursprüngliche Regelliste zurückverwiesen. Die in der weitergeleiteten Regelliste angezeigte „Deny“ Regel gilt nicht für den Rücksprung.

41.2.3. 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:



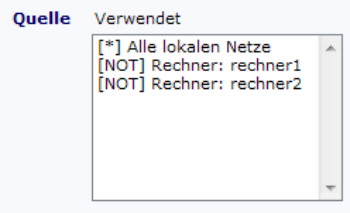
Quelle	Dienst	Trifft zu
Rechner1	Ping	Nein
Rechner1	HTTP	Ja
Rechner1	FTP	Ja
Rechner2	HTTP	Ja

Quelle	Dienst	Trifft zu
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

41.2.4. 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 Intra2net Systems (nur bei Typ „LAN 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.

41.2.5. Extra-Optionen

Auf der Karteikarte „Extra“ sind noch weitere Bedingungen untergebracht.

41.2.5.1. 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.

41.2.5.2. 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.

41.2.5.3. 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.

41.2.5.4. Paketgröße

Eine Bedingung, die zutrifft, sobald das Paket eine Größe in dem angegebenen Bereich hat.

41.2.5.5. Verbindungsstatus

Das Intra2net System 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

41.2.5.6. TCP-Flags

Diese Bedingung wird normalerweise nicht benötigt, der Verbindungsstatus bietet mehr Möglichkeiten.

41.2.6. Besonderheiten bei Provider-Regellisten

Einige Server (vor allem öffentliche FTP-Server) versuchen bei einem Verbindungsaufbau 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 Intra2net System 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.

42. Kapitel - Weitere Funktionen

42.1. 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.

42.2. Spoofing im LAN verhindern

Das Intra2net System stellt in allen Fällen sicher, dass lokale IP-Adressen nur über die entsprechenden LAN-Schnittstellen auf das Intra2net System 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 das Intra2net System eintreffen dürfen, sondern nur über die, die mittels der Gateway-IP des Routings ausgewählt wurde.

42.3. Blockieren von IPs nach zu vielen Loginfehlern

Ist diese Option aktiviert, zählt das Intra2net System 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.

42.4. Firewall-Notmodus

Für den Fall, dass Sie sich einmal selbst mit der Firewall aussperren: Im Kommandozeilenmenü (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.

43. Kapitel - Fallbeispiele und Aufgaben

43.1. Aufgabe 1: Erweitern eines einfachen Rechnerprofils

Gegeben ist folgendes einfaches Rechnerprofil:

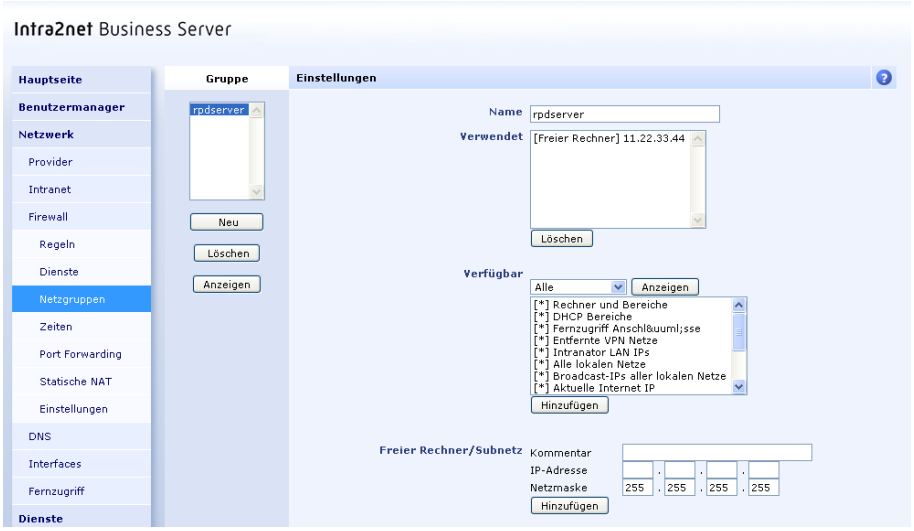
- Zugriffsberechtigung: WWW/FTP/E-Mail/News
- Zugriff auf lokale Netze nicht erlaubt
- keine zusätzlichen Dienste freigegeben
- Webzugriff über Proxy: Proxyzwang
- E-Mail-Transfer nur über Intra2net System: aktiv

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.

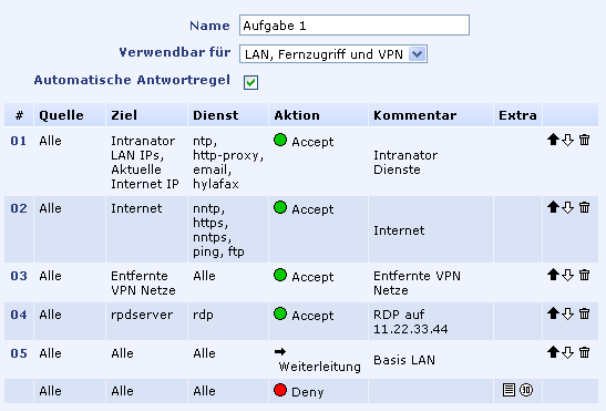
Legen Sie einen Rechner mit dem Namen "R10" und der IP 192.168.1.10 an und weisen ihm diese Firewallregelliste zu.

43.1.1. Musterlösung

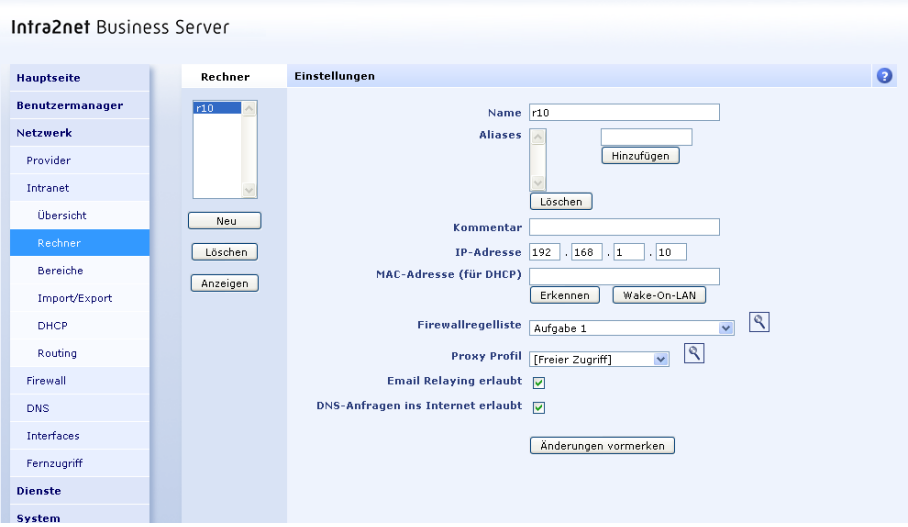
Anlegen einer Netzgruppe für den Rechner 11.22.33.44 unter Netzwerk > Firewall > Netzgruppen



Firewall Regelliste



Dem Rechner R10 die neue Firewall Regelliste zuweisen



43.2. Aufgabe 2: Portforwarding nur von einer externen IP erreichbar

- Richten Sie ein Portforwarding für den Port 3389 auf den Rechner R10 ein.
- Konfigurieren Sie die Firewall so, dass dieses Portforwarding nur von einer einzigen IP (33.44.55.66) aus genutzt werden kann.
- Der Zugriff auf HTTPS, SMTP und SMTP-Submission, nicht aber für weitere Dienste, soll von überall her möglich sein.
- Legen Sie eine entsprechende Firewallregelliste an und weisen sie dem Standardprovider zu.

43.3. Aufgabe 3: Separiertes Gästenetz

Das Intra2net System 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.

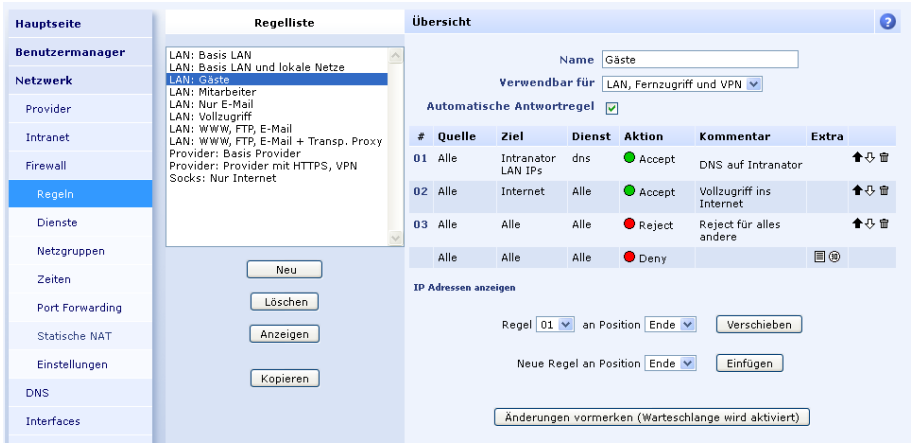
Im Detail:

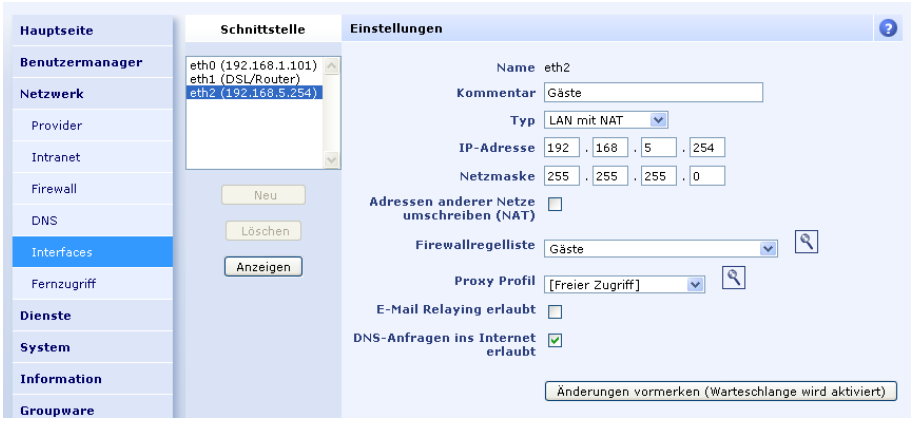
- Das Mitarbeiter-Netz verwendet 192.168.1.0/24, das Gäste-Netz verwendet 192.168.5.0/24. Jedes der beiden Netze verwendet eine separate Schnittstelle des Intra2net Systems.

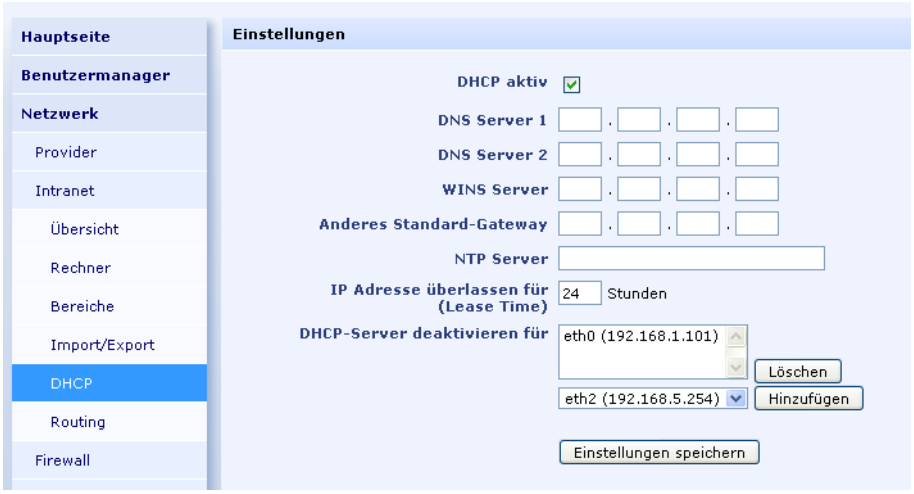
- Aus dem Gäste-Netz ist Vollzugriff ins Internet erlaubt. Zugriff auf das Intra2net System ist nur für DNS zulässig. Ein Zugriff ins Mitarbeiter-Netz darf auf keinen Fall möglich sein.

- Das Intra2net System 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.

43.3.1. Musterlösung









43.4. Aufgabe 4: Beschränkter Zugang aus dem VPN

Ein Benutzer soll sich zur Fernwartung eines Servers von einem VPN-Client mit dem Intra2net System verbinden. Über diese Verbindung soll er nur einen bestimmten Dienst auf einem Server ansprechen können.

- Der Zielrechner für die Fernwartung hat den Namen "testserver" und die IP 192.168.1nn.100.
- Legen Sie eine neue Firewall-Regelliste an, die nur den Zugriff auf diesen Server mit dem Dienst HTTP erlaubt.
- Für die Adressierung ist außerdem noch Zugriff auf das DNS des Intra2net Systems erforderlich. Alle nicht erlaubten Zugriffe sollen mit Reject zurückgewiesen werden.
- Aktivieren Sie diese Firewall-Konfiguration für eine bestehende VPN-Einwahlverbindung.
- Bauen Sie die VPN-Verbindung auf und testen mit einem Webbrowser, ob Sie den Server per HTTP ansprechen können. Es sollte eine Testseite angezeigt werden.
- Öffnen Sie das Programm "zenmap GUI", welches Teil der Portscanner-Suite Nmap ist. Führen Sie zum Test der Firewall-Regelliste einen "Intense Scan" auf den Zielserver durch. Es darf nur der Dienst HTTP erreichbar sein.
- Führen Sie einen "Intense Scan" auf die IP des Intra2net Systems im VPN-Netz durch, also 192.168.1nn.254. Es darf nur der Dienst DNS erreichbar sein.

43.5. Aufgabe 5: Webserver in der DMZ

Szenario:

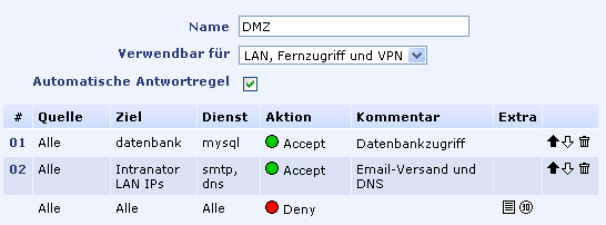
- Ein Webserver steht in einer DMZ (De-Militarized Zone) und hat eine offizielle IP (LAN ohne NAT). Es wird klassisches Routing verwendet (siehe Abschnitt 11.7.1, „Klassisches Routing“).

- Der Router des Providers hat die IP 88.89.90.1, die externe IP des Intra2net Systems 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), das Intra2net System 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 das Intra2net System 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 Intra2net Systems nutzen.

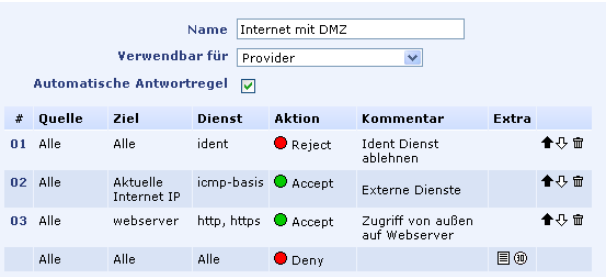
43.5.1. Musterlösung

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



Providerregel



Teil 6. IPSec VPN

44. Kapitel - IPSec Grundlagen

44.1. 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.

44.2. 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.

44.3. 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 das Intra2net System bringt eine solche Zertifizierungsstelle normalerweise nur wenig Vorteile, dennoch setzt das Intra2net System 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 das Intra2net System normalerweise selbstsignierte Zertifikate, bei denen der Inhaber (Subject genannt) auch gleichzeitig der Zertifikatsaussteller (Issuer) ist. Dadurch sind bei der Bedienung keine zusätzlichen Schritte für die Verwendung von Zertifikaten nötig. Selbstverständlich können aber auch externe Zertifizierungsstellen verwendet werden.

44.4. 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. Das Intra2net System 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.

44.5. 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 Intra2net System 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 Intra2net System über die Verschlüsselungsprofile konfiguriert. Ist auf dem Intra2net System eine

PFS-Gruppe vorgegeben, wird diese beim Verbindungsaufbau verwendet. Baut die Gegenseite die Verbindung auf, akzeptiert das Intra2net System 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 Intra2net System 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.

44.6. 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.

44.7. Kompatibilität mit anderen IPSec-Gegenstellen

IPSec ist standardisiert und das Intra2net System 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 einfachere 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.

45. 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 Intra2net System eine Schlüsselverwaltung vorgesehen.

45.1. 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. Das Intra2net System unterstützt Schlüssellängen von 1024 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 Intra2net System 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.

45.1.1. Zertifizierungsstellen (CAs)

Um die Bedienung zu vereinfachen, erzeugt das Intra2net System 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 das Intra2net System 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 an. Dieses Zertifikat wird nur indirekt zum Signieren verwendet, nennen Sie es deshalb beispielsweise **`server-ca`**.

2. Exportieren Sie dieses Zertifikat und importieren es auf der Gegenseite als vertrauenswürdige Root-CA.

3. Legen Sie nun auf dem Intra2net System einen weiteren eigenen Schlüssel an. Dieser wird nachher vom System 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.

45.2. Fremde Schlüssel

Damit das Intra2net System eine Verbindung aufbauen kann, muss es zuerst den Public-Key der Gegenstelle kennen. Exportieren Sie Ihn daher auf der Gegenstelle, übertragen und importieren ihn.

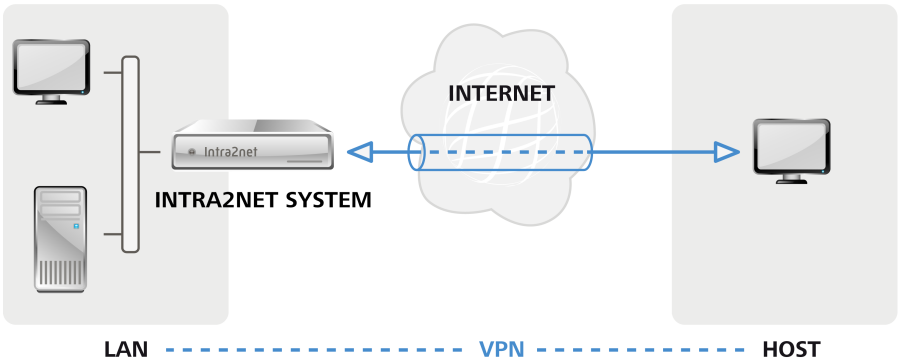
Gehen Sie zum Importieren auf die Seite System > Schlüssel > Fremde Schlüssel, wählen einen Namen und stellen den Schlüsseltyp ein. Öffnen Sie nun den Schlüssel in einem Texteditor, markieren und kopieren ihn in die Zwischenablage. Nun können Sie ihn in das Copy & Paste Feld einfügen.

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 das Intra2net System die beiden gängigsten Fingerprint-Verfahren MD5 und SHA1. Es reicht aus, wenn Sie einen der beiden Fingerprints vergleichen.

46. Kapitel - Anbinden von einzelnen PCs

46.1. 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 Intra2net System 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.

Für die meisten unterstützten Clients kann das Intra2net System automatisch passende Konfigurationsdateien vorbereiten, die im Client nur noch importiert werden müssen. Eine manuelle Konfiguration ist aber auch immer möglich.

46.2. Vorbereiten der Konfiguration auf dem Intra2net System

46.2.1. Zertifikat erstellen

Das Intra2net System benötigt einen eigenen, privaten Schlüssel mit X.509-Zertifikat um VPN-Verbindungen von Clients entgegen nehmen zu können. Dieser eine Schlüssel kann problemlos für alle VPN-Verbindungen gemeinsam verwendet werden. Technisch wäre es möglich diesen Schlüssel auch für SSL/TLS-Verbindungen zu verwenden. Allerdings haben dafür genutzte Zertifikate typischerweise nur eine kurze Laufzeit, weswegen ein Schlüssel nur für die VPN-Verbindungen normalerweise die bessere Wahl ist.

Einige VPN-Clients fordern ein CA-signiertes Zertifikat, weswegen wir empfehlen von Anfang an gleich ein solches, wie im Folgenden beschrieben, einzurichten.

1. Das Intra2net System sollte für die VPN-Clients über einen DNS-Namen im Internet adressierbar sein.

Hat das Intra2net System eine feste IP, richten Sie für diese einen DNS-Eintrag in der eigenen offiziellen Domain ein. Das System ist dann unter einem Namen wie z.B. **`intra.kundenname.de`** oder **`mail.example.com`** erreichbar. Dies kann normalerweise beim Webspace-Provider, der die Domain verwaltet, kostenlos und zeitnah eingerichtet werden.

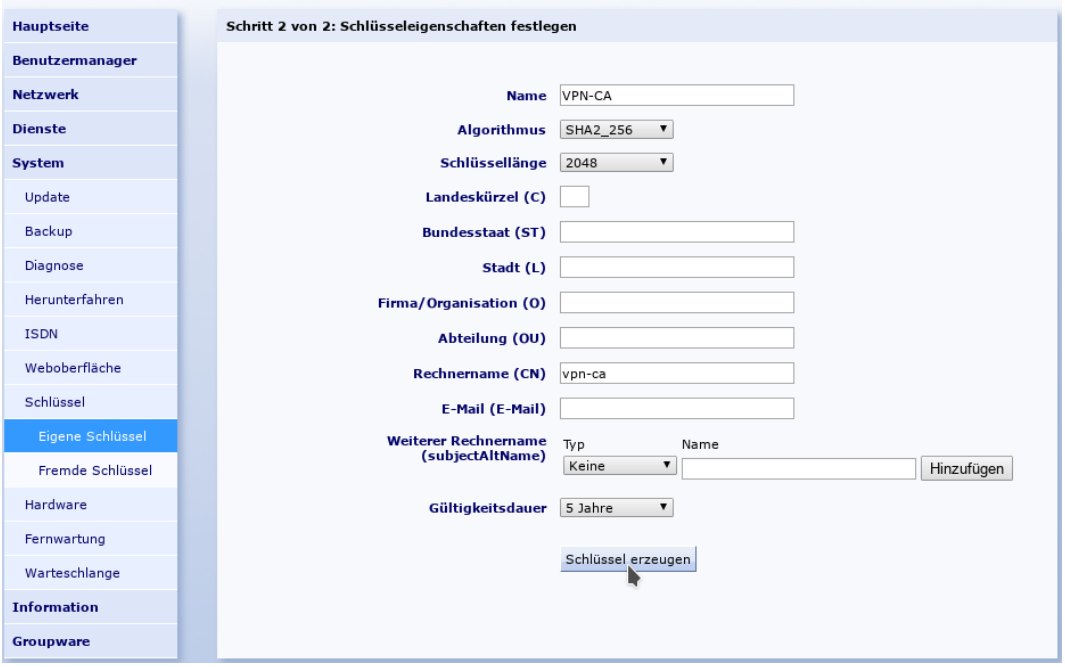
Bekommt das Intra2net System bei jeder Interneteinwahl eine andere IP zugewiesen, muss zur Adressierung ein DynDNS-Dienst eingerichtet werden. Siehe hierfür Abschnitt 11.13, „DynDNS“.

Eine feste IP kann bei einigen VPN-Clients nicht direkt und ohne DNS-Namen verwendet werden. Außerdem ist eine Änderung der IP bei Providerwechsel aufwendig. Wir raten daher dazu, ausschließlich DNS-Namen und keine IPs zur Adressierung zu verwenden.

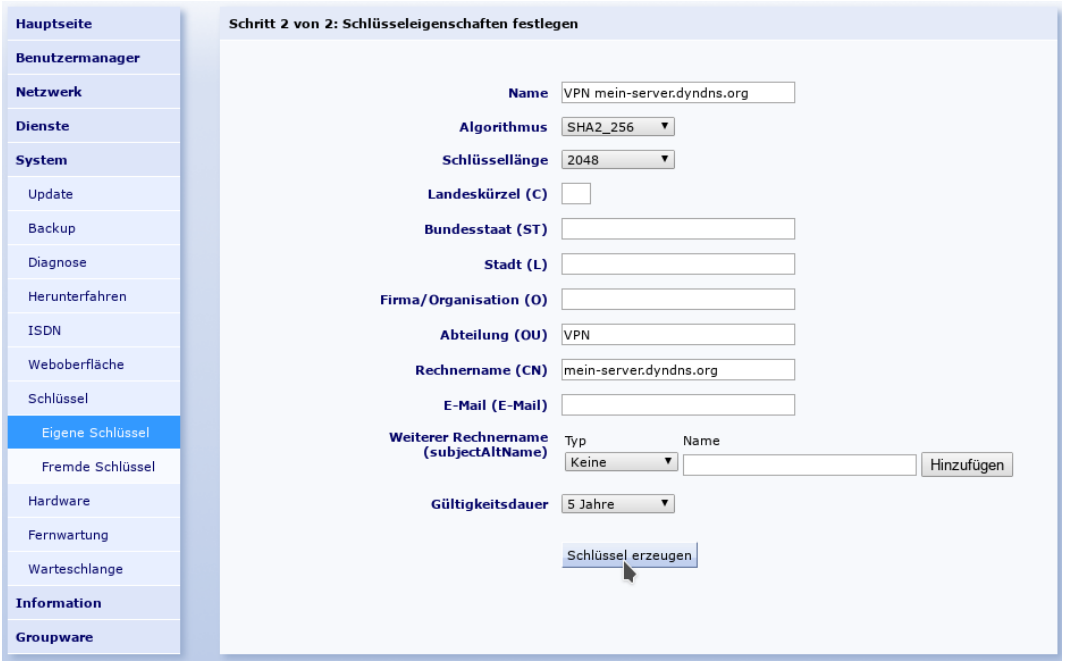
2. Gehen Sie in das Menü "Netzwerk > DNS > Einstellungen" und hinterlegen diesen extern erreichbaren DNS-Namen im Feld "Vollständiger Rechnername für Verbindungen aus dem Internet".

3. Gehen Sie in das Menü "System > Schlüssel > Eigene Schlüssel" und legen einen neues, selbstsigniertes Zertifikat an.

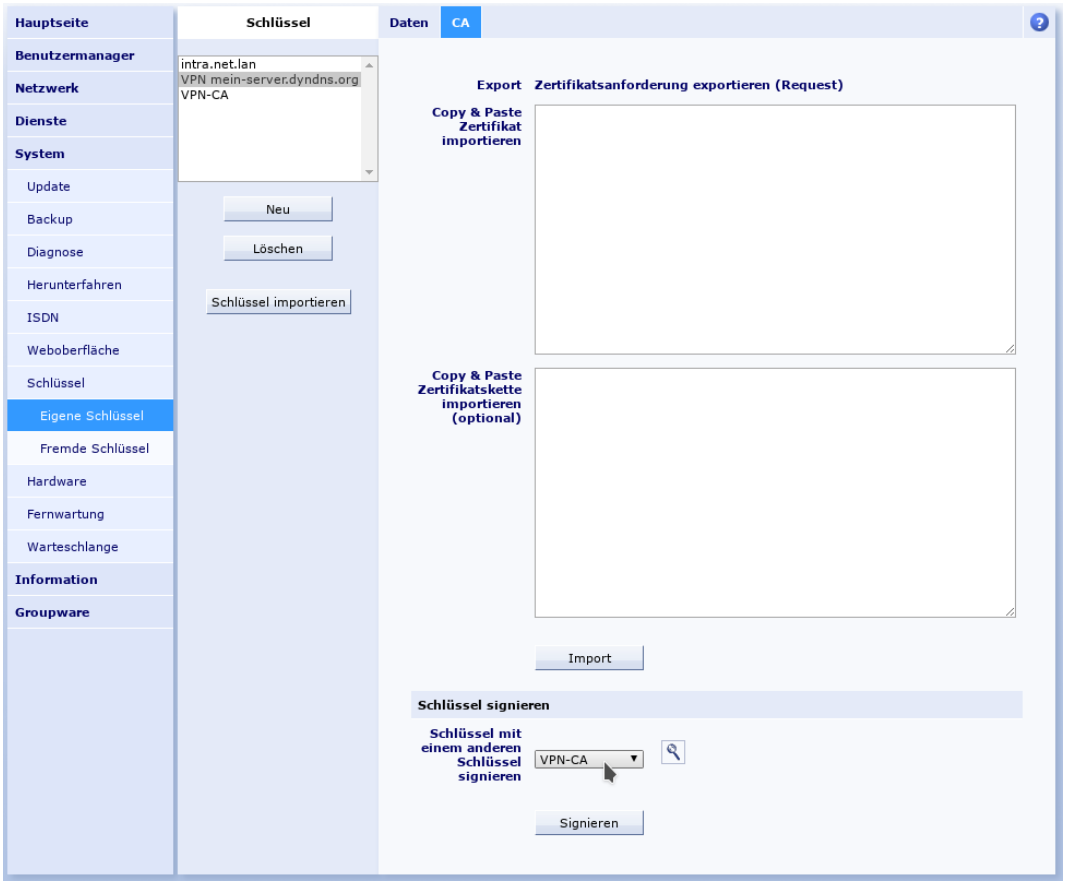
4. Nennen Sie den Schlüssel **`VPN-CA`** oder ähnlich und tragen das auch als Rechnername ein. Geben Sie *NICHT* den DNS-Hostnamen des Intra2net Systems als Rechnername ein. Wir empfehlen eine Gültigkeitsdauer von 5 Jahren. Lassen Sie den Schlüssel erzeugen.



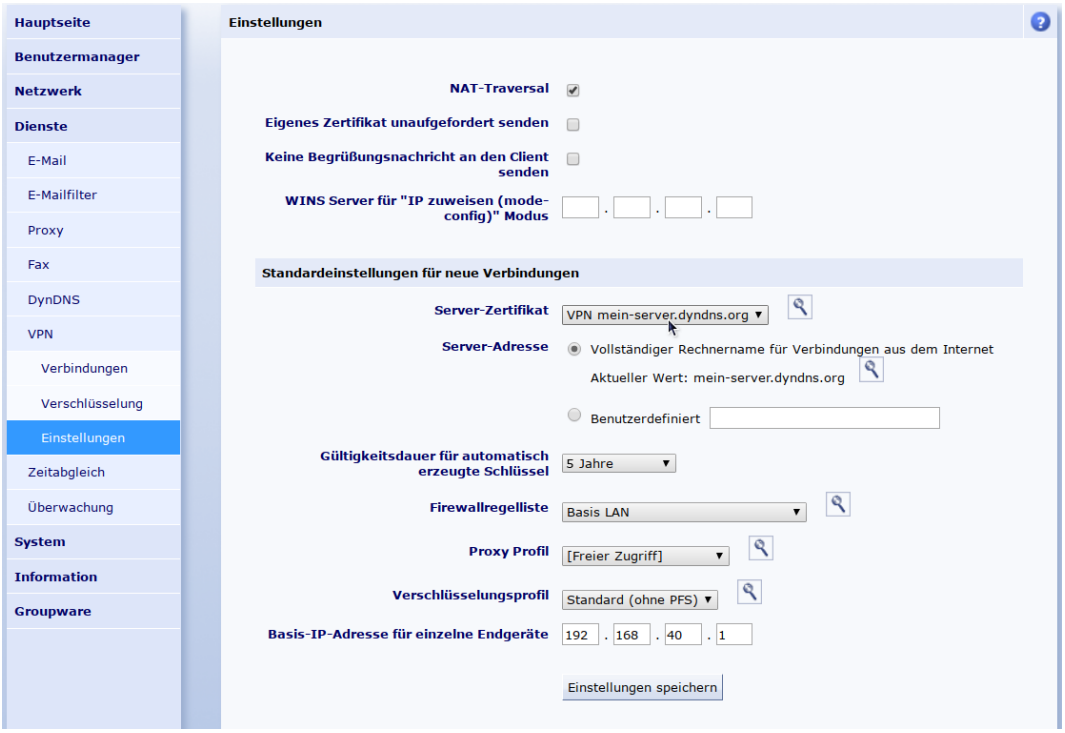
5. Legen Sie ein weiteres neues, selbstsigniertes Zertifikat an. Geben Sie dem Schlüssel den Namen "VPN" und hängen dann den externen DNS-Hostnamen Ihres Intra2net Systems an, also z.B. **`VPN mein-server.dyndns.org`**. Tragen Sie den externen DNS-Hostnamen unter "Rechnername (CN)" ein. Um ID-Konflikte mit für TLS verwendeten Schlüsseln zu umgehen, tragen Sie z.B. bei "Abteilung (OU)" den Wert **`VPN`** ein. Lassen Sie den Schlüssel erzeugen.



6. Wechseln Sie bei dem eben erzeugten Schlüssel auf den Reiter "CA". Lassen Sie dann diesen Schlüssel mit dem vorher erzeugten VPN-CA-Schlüssel signieren.



7. Gehen Sie in das Menü "Dienste > VPN > Einstellungen" und legen das eben erzeugte und signierte Server-Zertifikat als Standard fest.



46.2.2. Standardeinstellungen für neue Verbindungen

Im Menü "Dienste > VPN > Einstellungen" können Sie die Standardeinstellungen für neu erstellte VPN-Verbindungen festlegen. Die dort hinterlegten Einstellungen gelten sowohl für IPSec- als auch WireGuard-Verbindungen.

Server-Zertifikat und Server-Adresse sind wie in Abschnitt 46.2.1, „Zertifikat erstellen“ beschrieben zu konfigurieren.

Wählen Sie eine Firewallregelliste, die den für VPN-Clients üblicherweise gewünschten Zugriff ins lokale Netz erlaubt.

Jeder VPN-Client bekommt für die VPN-Verbindung eine individuelle, virtuelle IP zugewiesen. Diese muss außerhalb aller lokalen Netze, Routings und anderen VPN-Verbindungen liegen. Tragen Sie unter "Basis-IP-Adresse für einzelne Endgeräte" die IP für den ersten VPN-Client ein. Alle weiteren VPN-Clients erhalten fortlaufende IPs.

46.3. Automatische Konfiguration für Clients auf dem Intra2net System

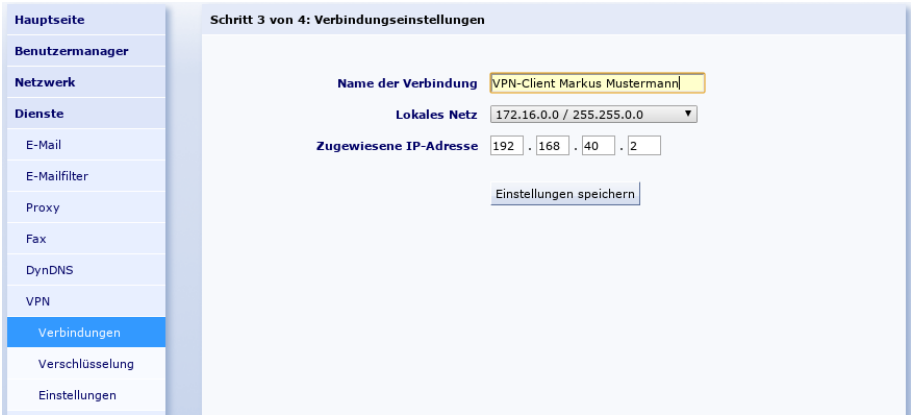
Für die meisten VPN-Clientprogramme kann das Intra2net System aus der VPN-Konfiguration auf dem Intra2net System direkt fertige Konfigurationsdateien erzeugen. Diese müssen auf dem Client nur noch importiert werden. Gehen Sie dafür wie folgt vor:

1. Gehen Sie in das Menü "Dienste > VPN > Verbindungen" und legen eine neue Verbindung an. Wählen Sie den Typ "IPSec: Einzelnes Endgerät".

2. Wählen Sie die VPN-Clientsoftware aus. Soll der Typ später geändert werden, so muss die Verbindungskonfiguration neu angelegt werden.

3. Geben Sie der Verbindung einen aussagekräftigen Namen, z.B. den Namen des Mitarbeiters oder Geräts, welches sich verbinden soll. Hat ein Mitarbeiter mehrere

Geräte, die VPN-Verbindungen aufbauen können sollen, benötigen Sie für jedes Gerät eine eigene Verbindungkonfiguration.



4. Wählen Sie das lokale Netz, in das der VPN-Client die Verbindung aufbauen soll.

   Bei den meisten Client-Typen haben Sie hier die Wahl, ob nur die Pakete in ein spezielles Netz durch den VPN-Tunnel laufen, oder ob jegliche Verbindungen vom Client, in die lokalen Netze und das Internet, durch den VPN-Tunnel und das Intra2net System laufen sollen. Wählen Sie für Letzteres bei "Lokales Netz" die Option "Alles (0.0.0.0/0.0.0.0)", für alle anderen Fälle das gewünschte Netz.

5. Bei Verbindungen von iOS- und Android-Clients müssen Sie ein Benutzerkonto auswählen, welches für den Login per XAUTH-Verfahren verwendet wird. Der Benutzer muss sich dafür in einer Gruppe befinden, die über das Recht "Anmeldung am VPN mit XAUTH" verfügt.

6. Geben Sie als Nächstes das Passwort, mit dem der private Schlüssel geschützt werden soll, ein.

7. Anschließend wird automatisch die Verbindung erstellt und die passende Konfigurationsdatei für den Client bereitgestellt. Speichern Sie diese ab und transferieren sie zum Client.

8. Importieren Sie die Konfigurationsdatei auf dem Client. Die dafür nötigen Schritte finden Sie in den folgenden Kapiteln erklärt.

Bei Bedarf können Sie die Konfiguration für den Client auch später über den "Download"-Link erneut exportieren.



Das Passwort für den privaten Schlüssel des Clients, welches bei den meisten Clients bei jedem Verbindungsaufbau eingegeben werden muss, wird vom Intra2net System nicht gespeichert. Es muss daher für jeden Export neu eingegeben werden. Wollen Sie das Passwort ändern, müssen Sie also einfach nur eine neue Konfiguration für den Client exportieren.

46.4. Manuelle Konfiguration auf dem Intra2net System

46.4.1. 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 Intra2net System 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.

Erstellen Sie daher am besten ein Zertifikat für VPNs wie in Abschnitt 46.2.1, „Zertifikat erstellen“ beschrieben.

Weitere Details zur Schlüsselverwaltung finden Sie im 45. Kapitel, „Schlüsselmanagement“.

Eine auf dem Intra2net System konfigurierte Verbindung gilt für die Verbindung zwischen einem Client und einem Netz hinter dem Intra2net System. Möchten Sie vom Client auf mehrere Netze hinter dem Intra2net System zugreifen, können Sie einfach mehrere Verbindungen konfigurieren. Achten Sie darauf, für jede dieser Verbindungen immer dieselbe Kombination an Schlüsseln/Zertifikaten zu verwenden.

46.4.2. Grundeinstellungen

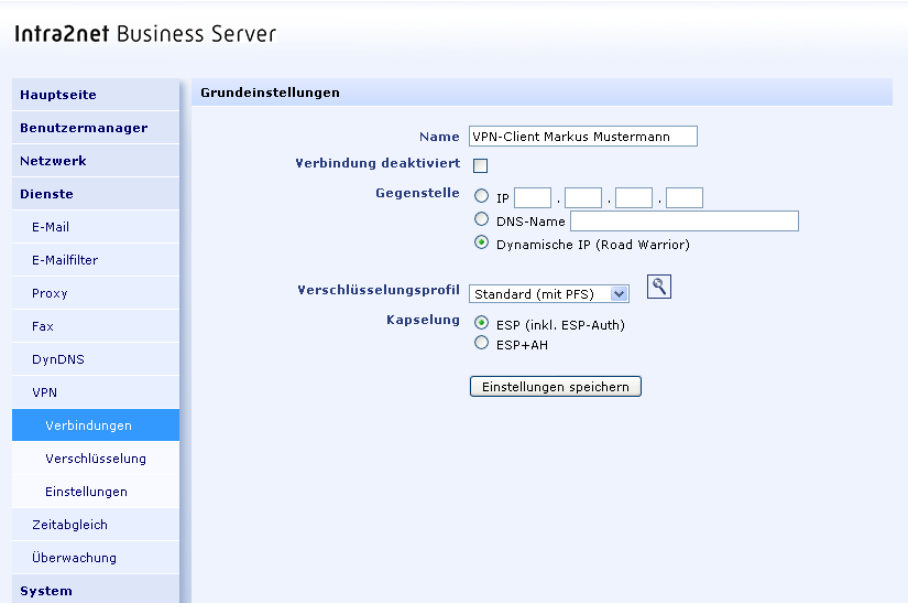
Im Menü "Dienste > VPN > Verbindungen" können Sie VPN-Verbindungen im Intra2net System konfigurieren.

Wenn Sie eine neue Verbindung manuell konfigurieren möchten, wählen Sie "IPSec: Site-to-Site oder eigene Konfiguration".

Stellen Sie die Optionen für die Gegenstelle ein. Die Gegenstelle ist bei einzelnen Rechnern üblicherweise nicht bekannt. Stellen Sie sie daher auf "Dynamische IP (Road Warrior)".

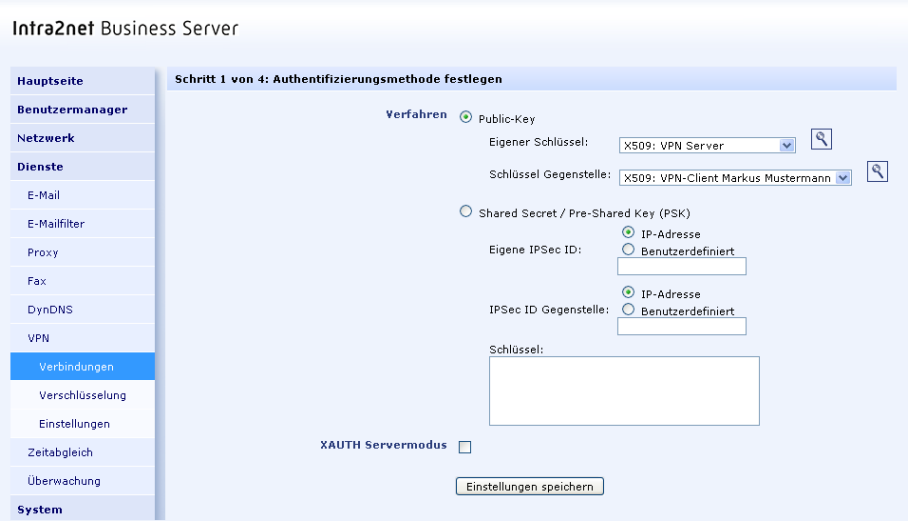
Über das Verschlüsselungsprofil können die verwendeten Verschlüsselungsalgorithmen ausgewählt werden; zu Details siehe Abschnitt 44.5, „Algorithmen“. Wichtig ist vor allem, dass die Einstellung für PFS (Perfect Forward Secrecy) auf beiden Seiten identisch ist.

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.



46.4.3. 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 Benutzers, der auf dem Intra2net System 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 44.6, „Einschränkungen“ genannten Gründen davon ab, Verbindungen per Pre-Shared Key (PSK) zu authentifizieren. Vor allem bei mehreren mobilen Rechnern ist diese Lösung besonders gefährlich.

46.4.4. Tunnel konfigurieren

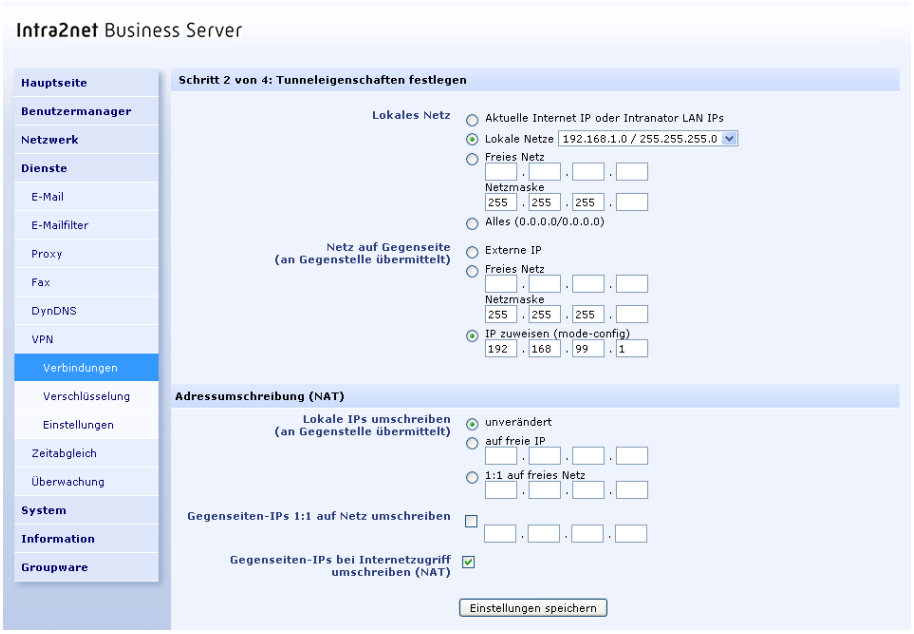
Auf der Seite "Tunnel" wird konfiguriert, welches Netz durch diese VPN-Verbindung mit welcher virtuellen Client-IP verbunden wird.

Über den Punkt "Lokales Netz" wird das zu verbindende Netz auf Seite des Intra2net Systems gewählt. Wählen Sie bei der Option "Lokale Netze" eines der direkt an das Intra2net System angeschlossenen oder gerouteten Netze aus.

Möchten Sie, dass jeglicher Datenverkehr des Clients über das Intra2net System 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 unbenutzte IP, die auch nicht in einem der Netze des Intra2net Systems 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 das Intra2net System automatisch seine eigene IP.

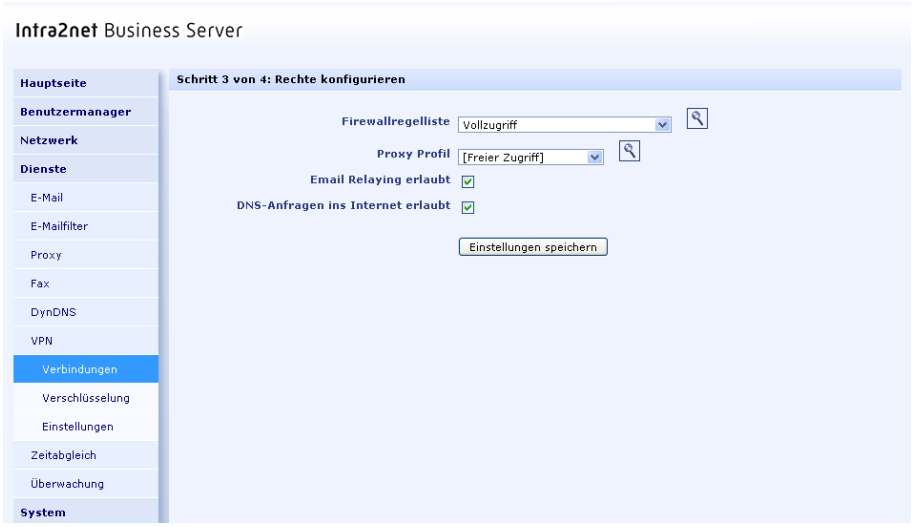


Wurde unter "Lokales Netz" ein Netz eingestellt, welches Adressen enthält, die nicht in lokalen oder anderen VPN-Netzen liegen, kann der Client über das VPN aufs Internet zugreifen. Dies gilt insbesondere für die Einstellung "Alles". Da die virtuelle IP normalerweise aus einem privaten Adressbereich stammt, kann sie über die Option "Gegenseiten-IPs bei Internetzugriff umschreiben" auf die externe Adresse des Intra2net Systems 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 58. Kapitel, „Lösen von IP-Adresskonflikten in VPNs durch NAT“ erklärt.

46.4.5. 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 9.3, „Zugriffsrechte eines Netzwerkobjekts“.



46.4.6. Aktivierung

In diesem Menü wird konfiguriert, wann die Verbindung aufgebaut und bestehende Sitzungen verlängert werden. Bei VPN-Clients kann das Intra2net System selbst die Verbindung nicht initiieren. Stellen Sie daher den Start auf "Passiv / manuell" und verwenden für die restlichen Optionen die vorgegebenen Werte.



47. Kapitel - VPN mit dem NCP Secure Entry Windows Client

Der NCP Secure Entry Windows Client wird über mehrere Distributoren vertrieben. Eine 30-tägige Testversion kann von der Homepage von NCP [https://www.ncp-e.com] heruntergeladen werden.

47.1. Import

Bereiten Sie zuerst das Intra2net System auf eine Verbindung mit VPN-Clients vor wie in Abschnitt 46.2, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben. Danach kann die komplette Konfiguration für den Client durch das Intra2net System, wie in Abschnitt 46.3, „Automatische Konfiguration für Clients auf dem Intra2net System“ beschrieben, erzeugt werden.

Transferieren Sie die so erzeugte Konfigurationsdatei auf den Client-PC, z.B. per USB-Stick oder über ein Fernwartungsprogramm. Zur Vereinfachung der Installation sind in der ZIP-Datei eine Batchdatei und ein Powershell-Skript enthalten. Da diese von vielen E-Mail-Filtern blockiert werden, empfehlen wir die Datei nicht per E-Mail zu versenden.

Gehen Sie dann auf dem Client-PC wie folgt vor, um die Konfiguration zu importieren:

1. Die Konfiguration besteht aus mehreren einzelnen Dateien und wird als ZIP-Datei gepackt übertragen. Öffnen Sie die ZIP-Datei im Windows Explorer und extrahieren alle enthaltenen Dateien in ein neues Verzeichnis.

2. In den entpackten Dateien ist die Batchdatei `install-ncp-certs.bat` enthalten. Starten Sie diese durch einen Doppelklick, um die Zertifikate zu installieren.

   Die Zertifikatsdateien werden dadurch in Unterverzeichnisse von `C:\ProgramData\NCP\SecureClient` kopiert, der private Schlüssel für den Client nach `certs`, der öffentliche Schlüssel des Intra2net Systems nach `cacerts`.

3. Starten Sie den NCP Secure Entry Client und öffnen das Menü "Konfiguration > Profile".

4. Klicken Sie auf "Hinzufügen / Import" und "Profile importieren".



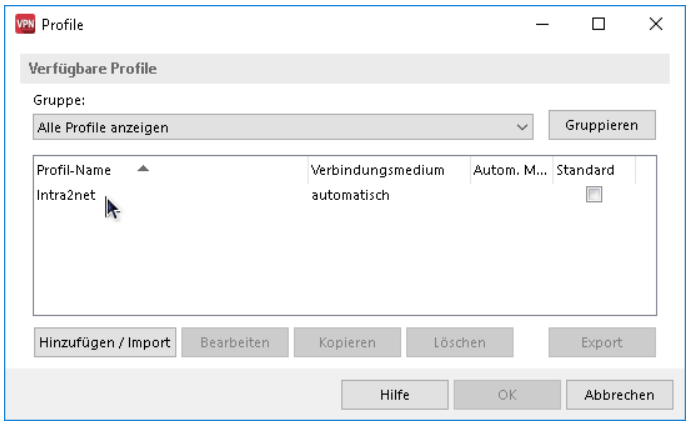
5. Gehen Sie auf "Weiter" und wählen jetzt die vorher entpackte INI-Datei aus.



6. Bestätigen Sie den Import. Das Profil sollte jetzt ohne Fehler importiert werden können.



7. Das neue Profil wird jetzt in der Profilübersicht angezeigt und kann verwendet werden.

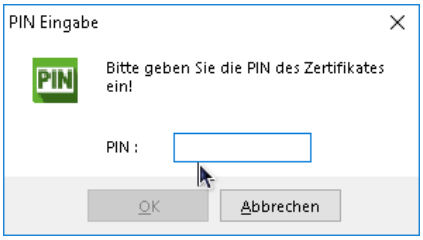


47.2. Verbindung aufbauen

Sie können die Verbindung durch das Umlegen des Schaltersymbols im NCP-Client aufbauen.

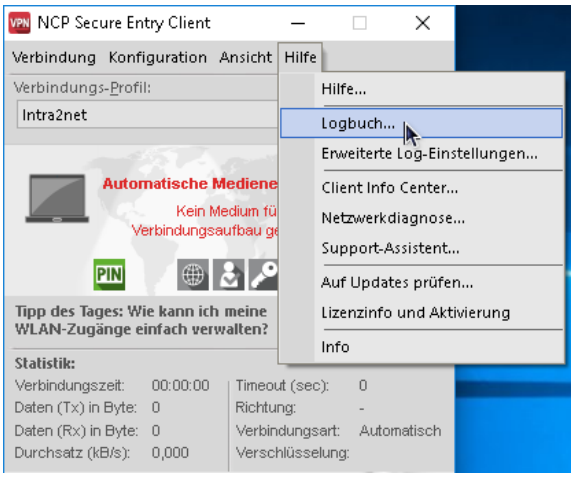


Für den Aufbau der Verbindung muss das Passwort, mit dem der private Schlüssel geschützt ist, eingegeben werden. Dieses Passwort wurde beim Erzeugen der Verbindung auf dem Intra2net System festgelegt.

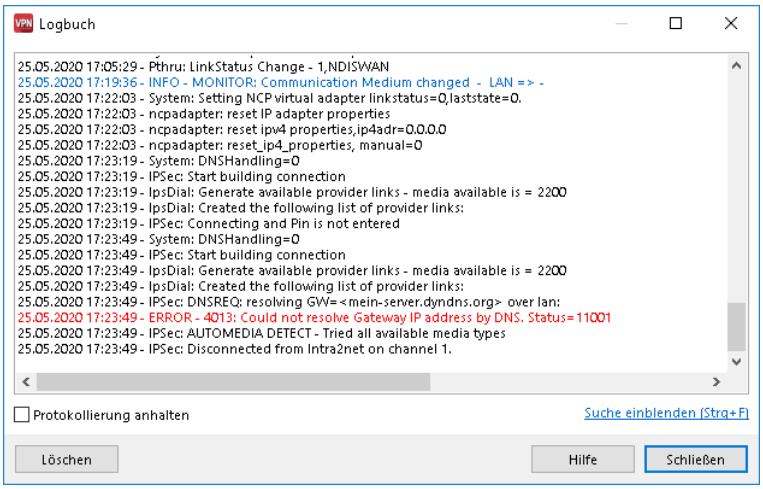


47.3. Verbindungsprotokolle

Um Fehler im Verbindungsaufbau zu analysieren, bietet sich das Logbuch des Clients an. Öffnen Sie es über das Menü "Hilfe > Logbuch".



Sie können den Inhalt über die Zwischenablage in einen Editor übertragen, dort speichern und dann als Datei an den Support übermitteln.

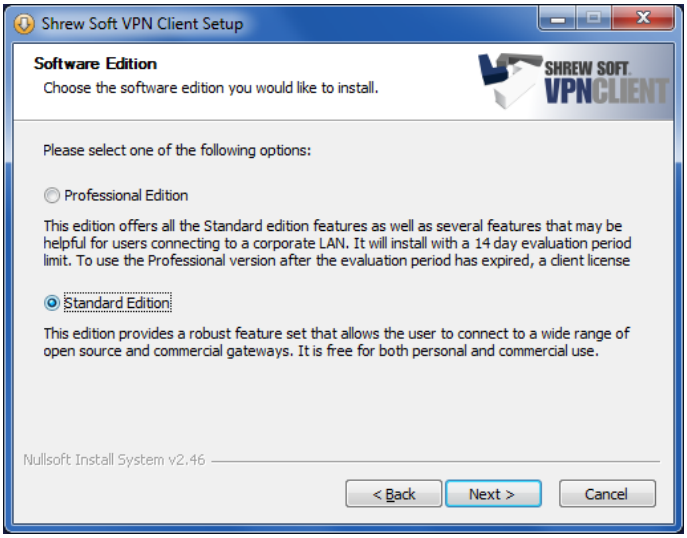

Logbuch
25.05.2020 17:05:29 - Pthru: LinkStatus Change - 1,NDISWAN
25.05.2020 17:19:36 - INFO - MONITOR: Communication Medium changed - LAN => -
25.05.2020 17:22:03 - System: Setting NCP virtual adapter linkstatus=0,laststate=0.
25.05.2020 17:22:03 - ncpadapter: reset IP adapter properties
25.05.2020 17:22:03 - ncpadapter: reset ipv4 properties,ip4adr=0.0.0.0
25.05.2020 17:22:03 - ncpadapter: reset_ip4_properties, manual=0
25.05.2020 17:23:19 - System: DNSHandling=0
25.05.2020 17:23:19 - IPSec: Start building connection
25.05.2020 17:23:19 - IpsDial: Generate available provider links - media available is = 2200
25.05.2020 17:23:19 - IpsDial: Created the following list of provider links:
25.05.2020 17:23:19 - IPSec: Connecting and Pin is not entered
25.05.2020 17:23:49 - System: DNSHandling=0
25.05.2020 17:23:49 - IPSec: Start building connection
25.05.2020 17:23:49 - IpsDial: Generate available provider links - media available is = 2200
25.05.2020 17:23:49 - IpsDial: Created the following list of provider links:
25.05.2020 17:23:49 - IPSec: DNSREQ: resolving GW=<mein-server.dyndns.org> over lan:
25.05.2020 17:23:49 - ERROR - 4013: Could not resolve Gateway IP address by DNS. Status=11001
25.05.2020 17:23:49 - IPSec: AUTOMEDIA DETECT - Tried all available media types
25.05.2020 17:23:49 - IPSec: Disconnected from Intra2net on channel 1.
Protokollierung anhalten
Suche einblenden (Strg+F)
Löschen
Hilfe
Schließen

48. Kapitel - VPN mit dem Shrew Soft VPN Client

Der Shrew Soft VPN Client für Windows ist ein kostenlos verfügbarer VPN Client für Windows 10, 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: https://www.shrew.net/download/vpn

Wählen Sie bei der Installation die "Standard Edition". Diese enthält alle für die Verbindung mit dem Intra2net System notwendigen Funktionen.



48.1. Import

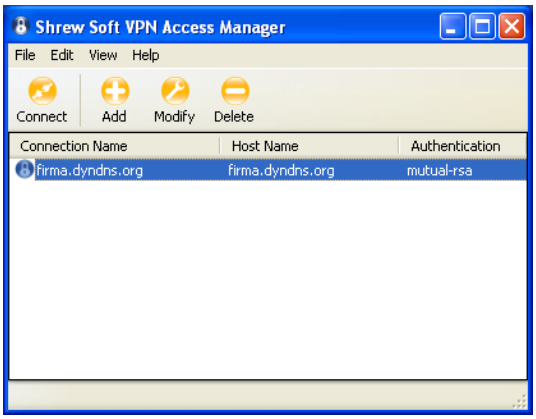
Bereiten Sie zuerst das Intra2net System auf eine Verbindung mit VPN-Clients vor wie in Abschnitt 46.2, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben. Danach kann die komplette Konfiguration für den Client durch das Intra2net System, wie in Abschnitt 46.3, „Automatische Konfiguration für Clients auf dem Intra2net System“ beschrieben, erzeugt werden.

Transferieren Sie die so erzeugte Konfigurationsdatei auf den Client-PC, z.B. als E-Mail-Anhang. Übergeben Sie dem Benutzer das Passwort, mit dem der private Schlüssel geschützt ist, auf einem anderen Weg, z.B. persönlich vor Ort. Versenden Sie dieses Passwort aus Sicherheitsgründen nicht per E-Mail.

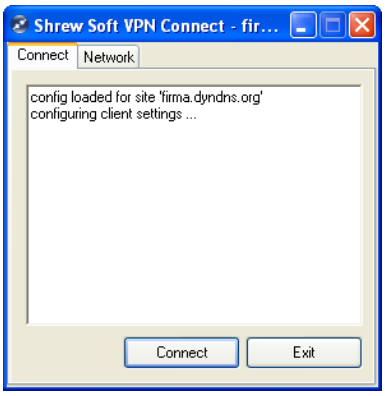
Starten Sie den VPN Access Manager und gehen ins Menü "File > Import". Wählen Sie die vom Intra2net System erzeugte Datei mit der Endung `.vpn` aus und importieren sie.

48.2. Verbindung aufbauen

1. Öffnen Sie im Hauptmenü des Access Managers die eben importierte Verbindung durch einen Doppelklick oder die Schaltfläche "Connect".



2. Bauen Sie die Verbindung durch einen Klick auf "Connect" auf.



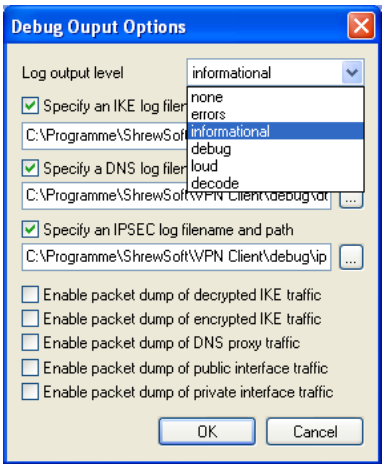
3. Sie werden nun nach dem auf dem Intra2net System festgelegten Passwort für den eigenen Schlüssel gefragt. Geben Sie es ein und die Verbindung wird aufgebaut.

48.3. Verbindungsprotokolle

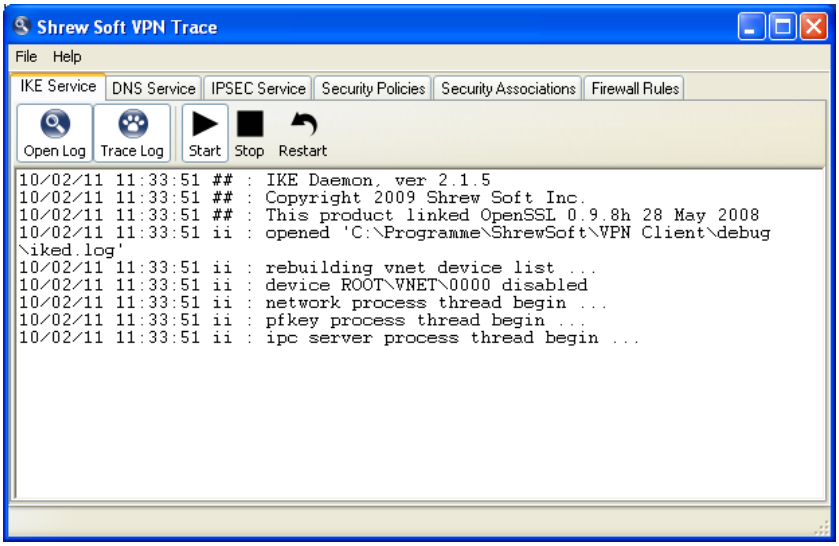
Um Fehler im Verbindungsaufbau zu analysieren, bieten sich die Verbindungsprotokolle des Clients an.

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".



49. Kapitel - VPN mit Mac OS X

49.1. 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.

49.2. 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. Verwenden Sie keine Umlaute oder Sonderzeichen.

   ```
   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.

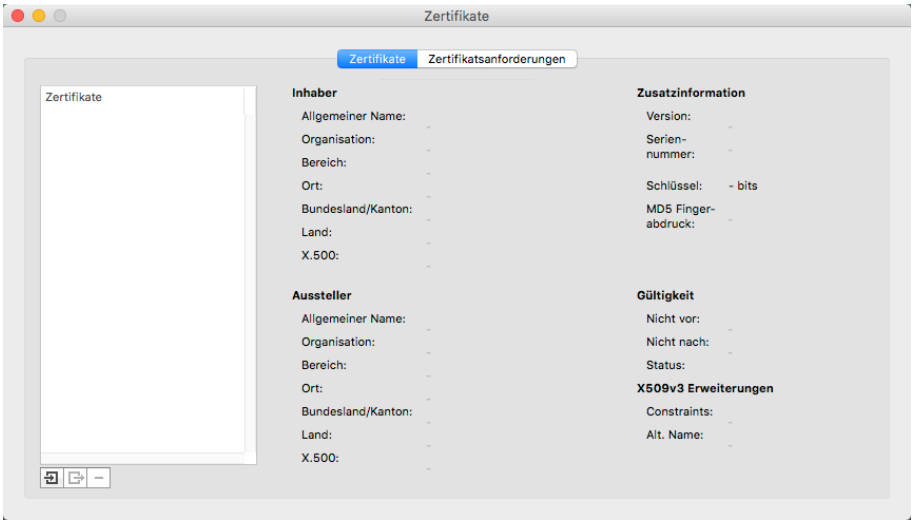
5. Aktuelle Versionen von IPSecuritas lesen den privaten Schlüssel nur noch im PKCS 12-Format ein. Mit folgendem Befehl auf der Kommandozeile wird das in Schritt 2 erstellte Schlüsselpaar passend umgewandelt:

```
openssl pkcs12 -export -in newcert.pem -inkey private_key.pem -out new-
cert.p12
```

An dieser Stelle müssen Sie ein Passwort eingeben, mit dem der private Schlüssel gesichert wird. Dieses Passwort wird später beim Import in IPSecuritas wieder benötigt. Das Resultat wird unter dem Dateinamen `newcert.p12` gespeichert.

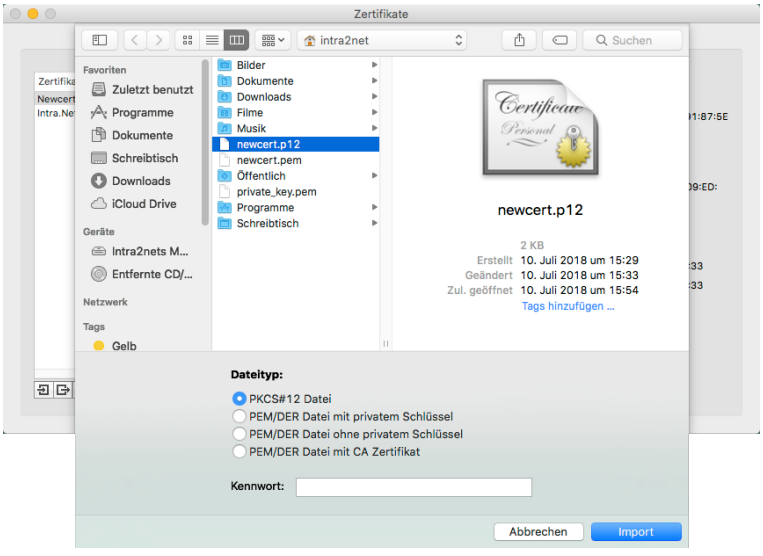
49.3. Zertifikate importieren

1. Starten Sie IPSecuritas und öffnen das Menü "Zertifikate", "Zertifikate bearbeiten".

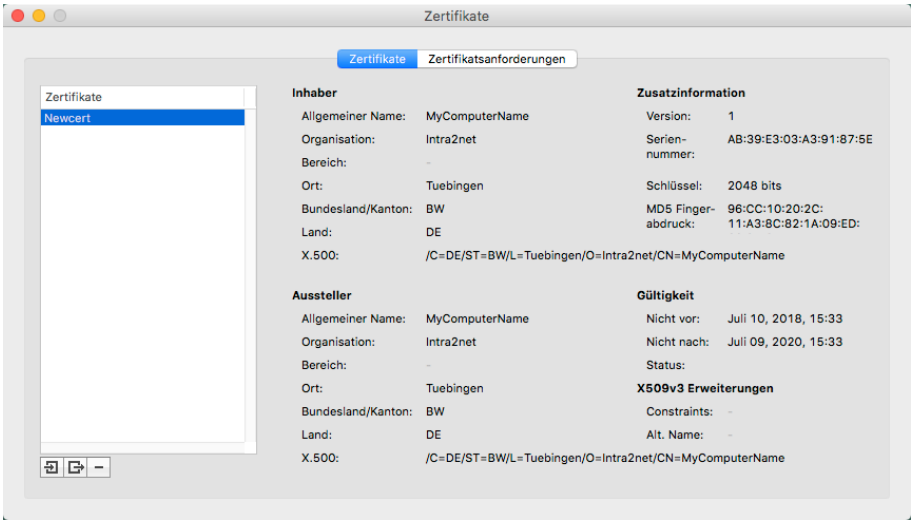


2. Klicken Sie links unten auf das "Importieren"-Symbol.

3. Wählen Sie die PKCS 12 Datei aus (im Beispiel `newcert.p12`) und stellen den Typ auf "PKCS#12 Datei". Außerdem tragen Sie das bei der Erstellung verwendete Passwort in das entsprechende Feld ein.



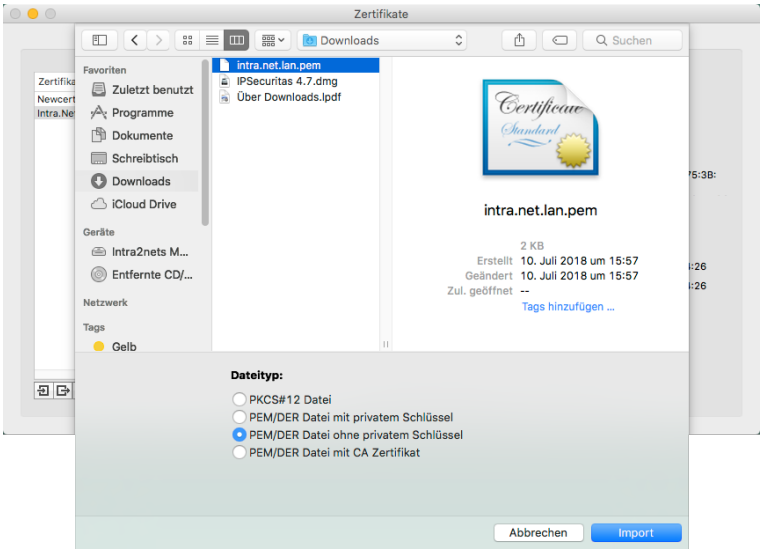
4. Das importierte Zertifikat wird im Zertifikatsmanager angezeigt.



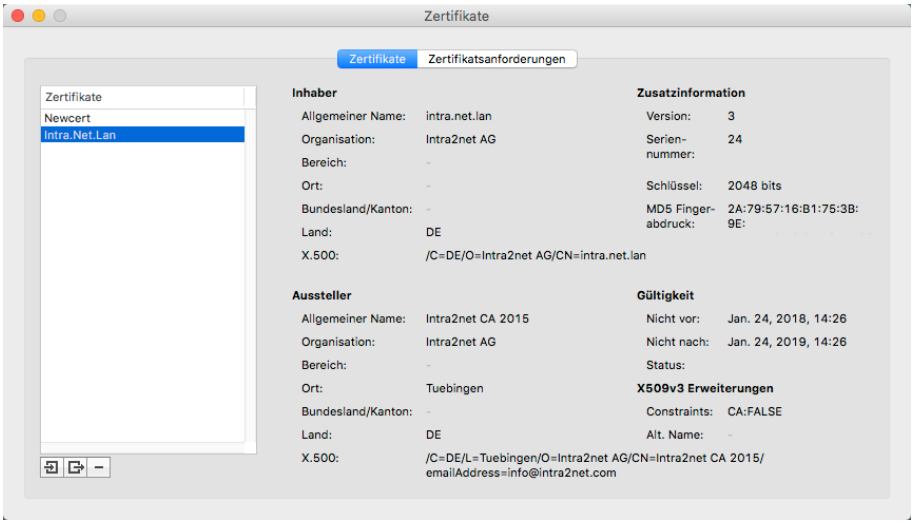
5. Öffnen Sie das eigene Zertifikat (z.B. `newcert.pem`) in einem Texteditor und übernehmen den Inhalt in die Zwischenablage. Öffnen Sie im Intra2net System das Menü "System > Schlüssel > Fremde Schlüssel" und legen einen neuen an. Geben Sie dem Schlüssel einen Namen (z.B. den des Benutzers) und kopieren Sie die Zertifikatsdaten aus der Zwischenablage in das Feld "Copy & Paste Schlüssel".

6. Öffnen Sie im Intra2net System 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.

7. Wählen Sie im Zertifikatsmanager von IPSecuritas wieder die "Import"-Funktion. Importieren Sie die eben vom Intra2net System gespeicherte Zertifikatsdatei und stellen den Typ auf "PEM/DER Datei ohne privaten Schlüssel".

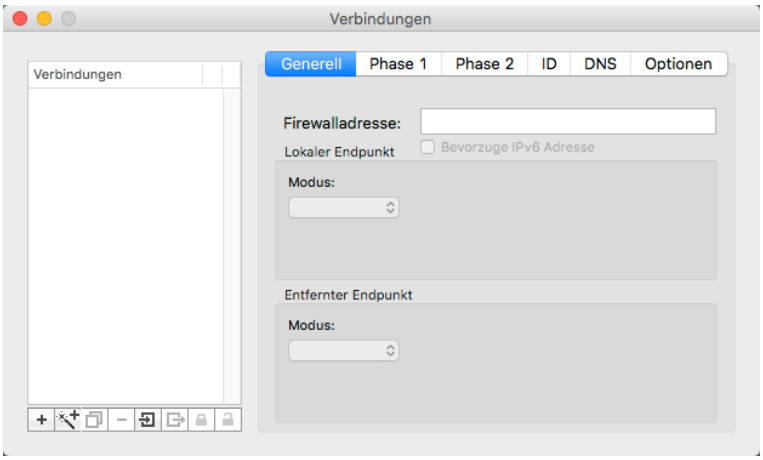


8. Das importierte Zertifikat wird im Zertifikatsmanager angezeigt.

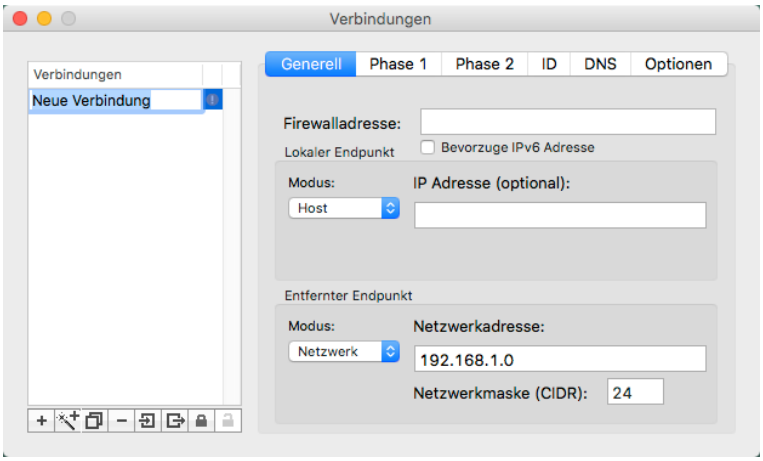


49.4. Verbindungen konfigurieren

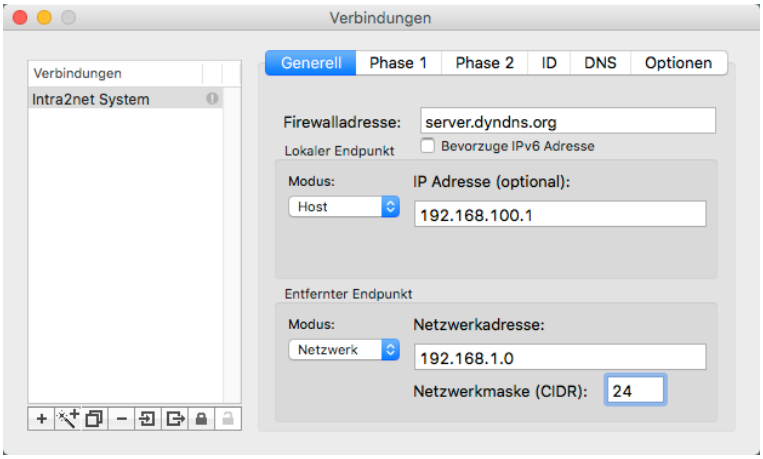
1. Öffnen Sie das Menü "Verbindungen", "Verbindungen bearbeiten" in IPSecuritas.



2. Legen Sie über das "Neu"-Symbol eine neue Verbindung an und geben ihr einen Namen (in diesem Beispiel **`Intra2net System`**).



3. Im Menü "Generell" tragen Sie unter "Firewalladresse" den DNS-Namen (bevorzugt) oder notfalls die externe IP-Adresse des Intra2net Systems ein.

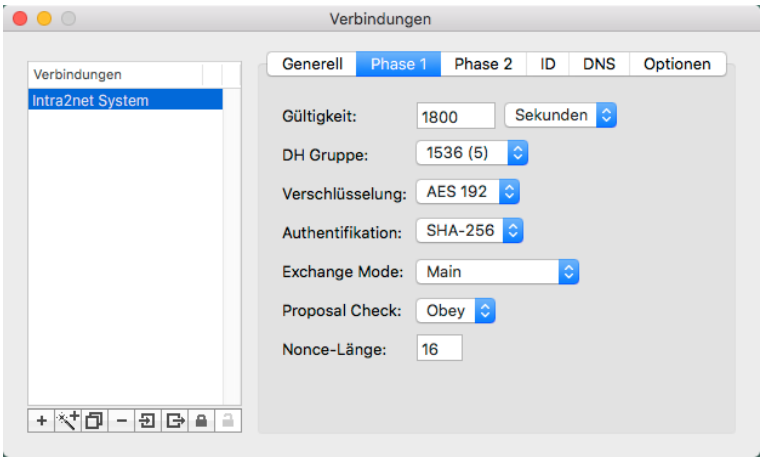


4. Stellen Sie bei "Lokaler Endpunkt" den "Modus" auf "Host" und geben die virtuelle IP ein, die der Mac-Client innerhalb des VPNs verwenden soll. Entgegen der Beschriftung des Feldes ist die IP auch bei Wahl von "mode-cfg" in der Konfiguration des Intra2net-Systems *nicht* optional und muss mit der dort angegebenen IP übereinstimmen.

5. Stellen Sie bei "Entfernter Endpunkt" den "Modus" auf "Network" und geben die Adresse des Netzes hinter dem Intra2net System ein. Die Netzmaske wird in CIDR-Notation eingegeben; **`24`** (Bit) entspricht **`255.255.255.0`**.

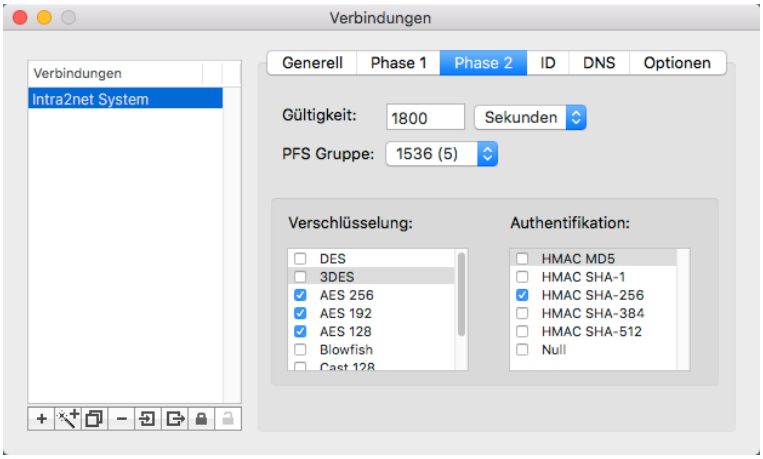
6. Im Menü "Phase 1" können Sie die Verschlüsselungsparameter für Phase 1 konfigurieren. Diese müssen zum auf dem Intra2net System gewählten Verschlüsselungsprofil passen.

   In der Standardeinstellung stellen Sie die "DH Gruppe" auf **`1536 (5)`**, "Verschlüsselung" auf **`AES 192`** und "Authentifikation" auf **`SHA-256`**.

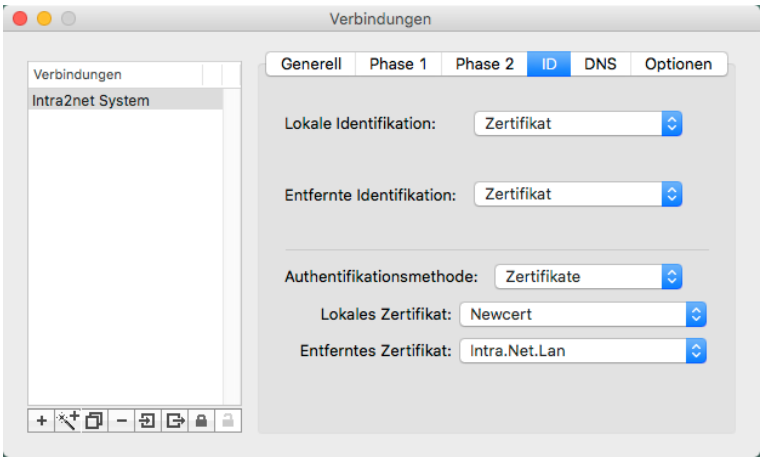


7. Im Menü "Phase 2" können Sie die Verschlüsselungsparameter für Phase 2 konfigurieren. Diese müssen zum auf dem Intra2net System gewählten Verschlüsselungsprofil passen.

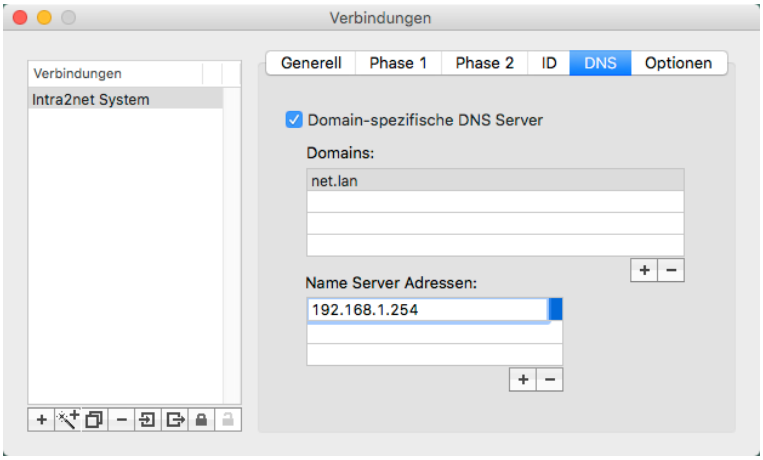
   In der Standardeinstellung stellen Sie die "PFS Gruppe" auf "1536 (5)" und aktivieren Sie unter "Verschlüsselung" nur die AES-Verschlüsselungsmethoden. Unter "Authentifikation" aktivieren Sie nur "HMAC SHA-256".



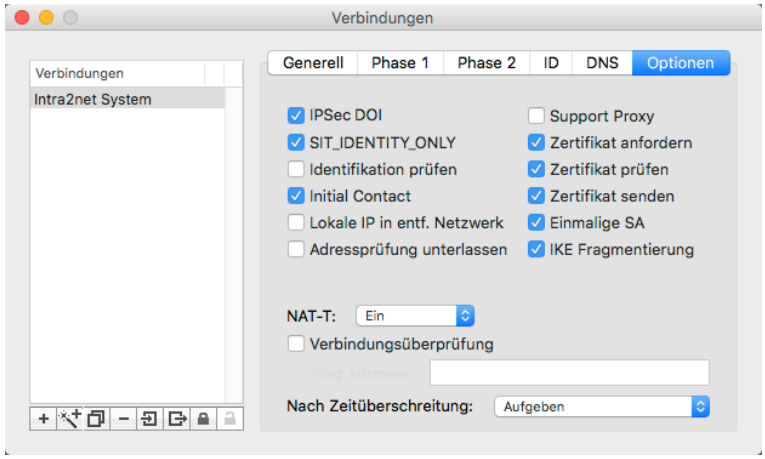
8. Stellen Sie im Menü "ID" bei "Lokale Identifikation" und "Entfernte Identifikation" jeweils "Zertifikat" ein. Wählen Sie "Zertifikate" als "Authentifizierungsmethode" und stellen die beiden vorher importierten Zertifikate ein.



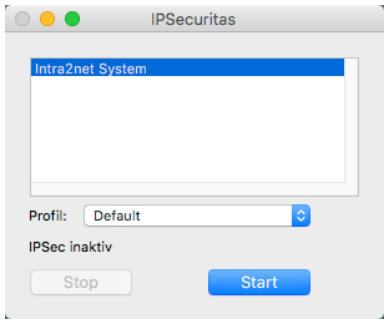
9. Im Menü "DNS" haben Sie die Möglichkeit, eine bestimmte Domain von einem Server im VPN (z.B. dem Intra2net System) auflösen zu lassen.



10. Stellen Sie im Menü "Optionen" die verschiedenen Optionen so ein, wie hier gezeigt.



11. Nun können Sie im Hauptfenster die Verbindung über den "Start"-Knopf aufbauen.



49.5. Intra2net System

Auf dem Intra2net System muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Clients wird dies im 46. Kapitel, „Anbinden von einzelnen PCs“ beschrieben.

50. Kapitel - VPN mit dem NCP Secure Entry macOS Client

Der NCP Secure Entry macOS Client wird über mehrere Distributoren vertrieben. Eine 30-tägige Testversion kann von der Homepage von NCP [https://www.ncp-e.com] heruntergeladen werden.

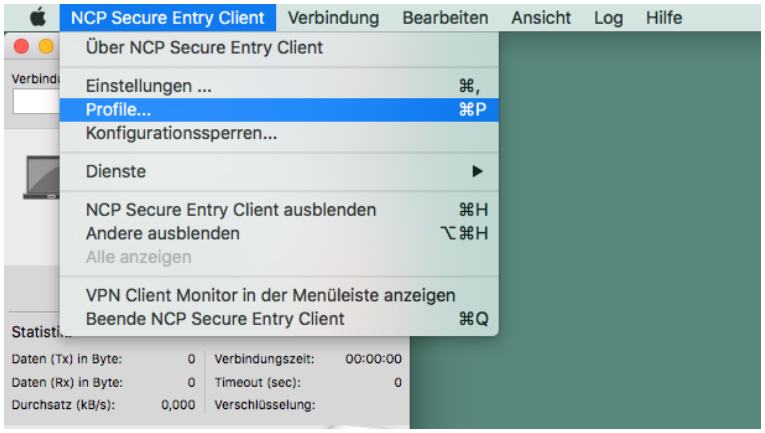
Bereiten Sie zuerst das Intra2net System auf eine Verbindung mit VPN-Clients vor wie in Abschnitt 46.2, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben. Danach kann die komplette Konfiguration für den Client durch das Intra2net System, wie in Abschnitt 46.3, „Automatische Konfiguration für Clients auf dem Intra2net System“ beschrieben, erzeugt werden.

Transferieren Sie die so erzeugte Konfigurationsdatei auf das macOS-Gerät, z.B. als E-Mail-Anhang. Übergeben Sie dem Benutzer das Passwort, mit dem der private Schlüssel geschützt ist, auf einem anderen Weg, z.B. persönlich vor Ort. Versenden Sie dieses Passwort aus Sicherheitsgründen nicht per E-Mail.

Gehen Sie dann auf dem macOS-Gerät wie folgt vor, um die Konfiguration zu importieren:

1. Die Konfiguration besteht aus mehreren einzelnen Dateien und wird als ZIP-Datei gepackt übertragen. Öffnen Sie die ZIP-Datei im Dateimanager von macOS und entpacken alle enthaltenen Dateien in ein Verzeichnis.

2. Starten Sie den VPN Client und gehen ins Menü "NCP Secure Entry Client > Profile".



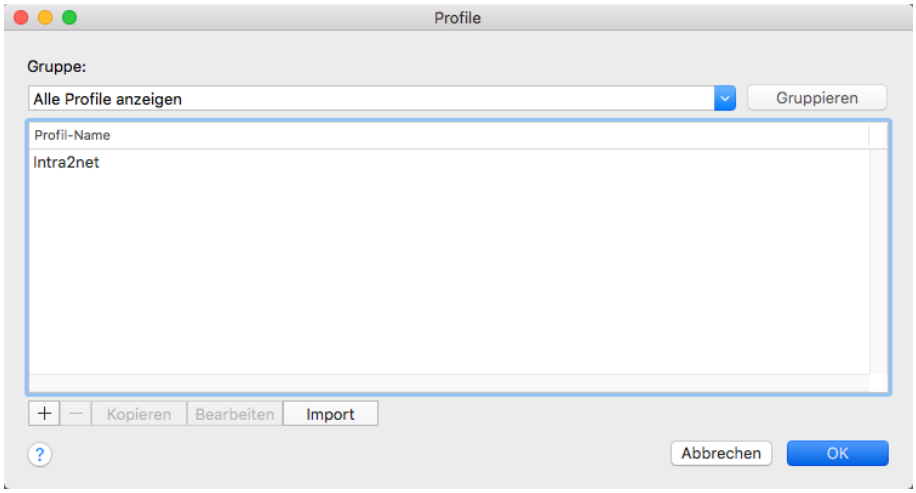
3. Klicken Sie auf "Import" und wählen die eben entpackte INI-Datei aus.



4. Klicken Sie auf "Weiter" um das Profil zu importieren. Das Profil sollte erfolgreich importiert werden können.



5. Die Profilübersicht enthält jetzt das neue Profil.



6. Als Nächstes muss die Datei mit dem Zertifikat des Intra2net Systems kopiert werden. Diese war in der vorher entpackten ZIP-Datei enthalten und trägt den externen DNS-Hostnamen des Intra2net Systems mit der Endung `.pem` als Dateinamen.

   Kopieren Sie diese mit dem Dateimanager von macOS ins Verzeichnis `Library/Application Support/NCP/Secure Client/cacerts`.

7. Als Nächstes muss die Datei mit dem privaten Schlüssel für den Client kopiert werden. Diese war in der vorher entpackten ZIP-Datei enthalten und trägt den Namen der Verbindung mit der Endung `.p12`.

   Kopieren Sie diese in das Verzeichnis `Library/Application Support/NCP/Secure Client/certs`.

Sie können die Verbindung jetzt durch das Umlegen des Schaltersymbols im NCP-Client aufbauen.

Für den Aufbau der Verbindung muss das Passwort, mit dem der private Schlüssel geschützt ist, eingegeben werden. Dieses Passwort wurde beim Erzeugen der Verbindung auf dem Intra2net System festgelegt.



51. Kapitel - VPN mit Apple iOS-Geräten

iOS enthält von Haus aus einen integrierten VPN-Client, der für die Verbindung zum Intra2net System genutzt werden kann.

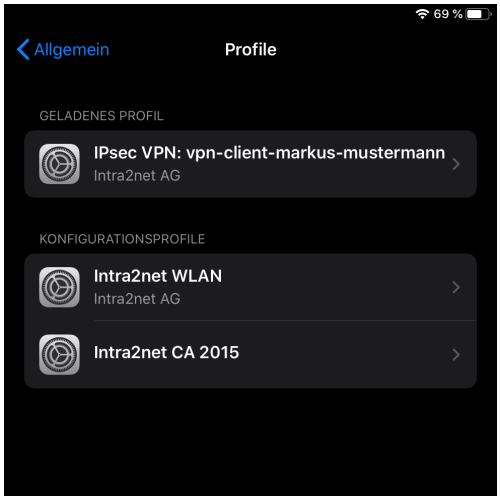
Bereiten Sie zuerst das Intra2net System auf eine Verbindung mit VPN-Clients vor wie in Abschnitt 46.2, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben. Danach kann die komplette Konfiguration für den Client durch das Intra2net System, wie in Abschnitt 46.3, „Automatische Konfiguration für Clients auf dem Intra2net System“ beschrieben, erzeugt werden.

Transferieren Sie die so erzeugte Konfigurationsdatei (Endung `.mobileconfig`) auf das iOS-Gerät, z.B. als E-Mail-Anhang. Übergeben Sie dem Benutzer das Passwort, mit dem der private Schlüssel geschützt ist, auf einem anderen Weg, z.B. persönlich vor Ort. Versenden Sie dieses Passwort aus Sicherheitsgründen nicht per E-Mail.

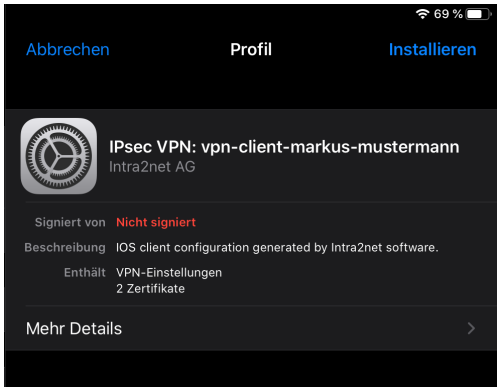
Gehen Sie dann auf dem iOS-Gerät wie folgt vor, um die Konfiguration zu importieren:

1. Tippen Sie die Konfigurationsdatei (Endung `.mobileconfig`) an, z.B. im E-Mail-Client. Sie wird dann als Profil im iOS-Gerät geladen, ist aber noch nicht installiert

2. Öffnen Sie das Menü "Einstellungen > Allgemein > Profile". Die VPN-Verbindung wird als geladen, aber noch nicht installiert, angezeigt.



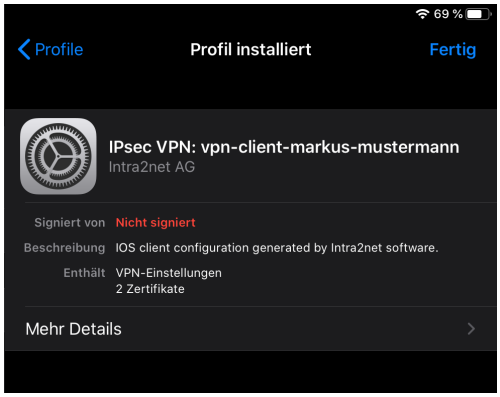
3. Tippen Sie die VPN-Verbindung an und gehen auf "Installieren".



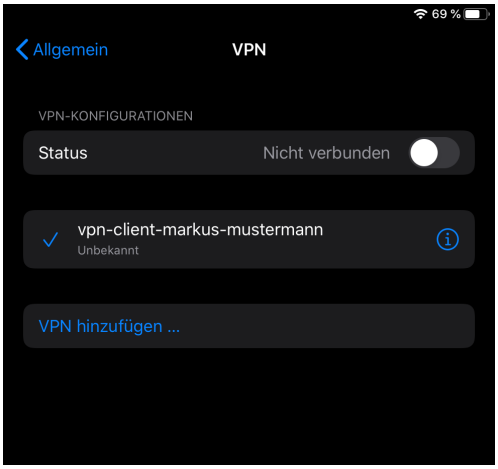
4. Sie müssen das Passwort des iOS-Geräts eingeben, um ein neues Profil installieren zu können. Danach bekommen Sie Sicherheitswarnungen angezeigt. Wählen Sie erneut "Installieren" und bestätigen Sie die Installation.

5. Sie müssen nun das Passwort, mit dem der private Schlüssel geschützt ist, einmalig eingeben. Dieses Passwort wurde beim Erzeugen der Verbindung auf dem Intra2net System festgelegt.

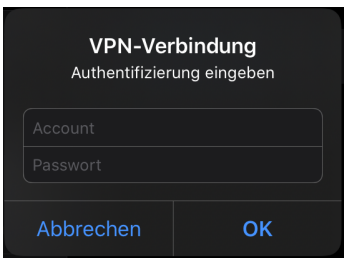
6. Das Profil wurde erfolgreich installiert. Schließen Sie den Vorgang mit "Fertig" ab.



Zum Aufbau der Verbindung öffnen Sie das Menü "Einstellungen > Allgemein > VPN" und legen Sie dann den Schalter zum Verbinden um.



Sie müssen jetzt Login und Passwort des Benutzers auf dem Intra2net System eingeben, um die Verbindung aufbauen zu können.



52. 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 Intra2net System aufbauen zu können. Zusätzliche Software, Rootrechte und ähnliches werden nicht benötigt.

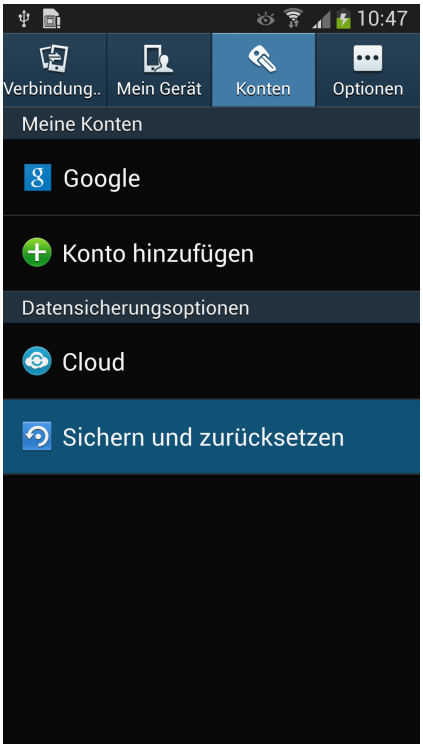
Geräte mit Android werden von vielen verschiedenen Herstellern angeboten. Jeder Hersteller hat die Möglichkeit, das Original-Android von Google auf seinen Geräten anzupassen. Daher können wir die Funktionsfähigkeit nicht für alle Geräte garantieren. Außerdem kann sich die Bedienung in Details von der hier vorgestellten unterscheiden. Diese Anleitung und Screenshots wurden mit einem Samsung Galaxy S4 erstellt.

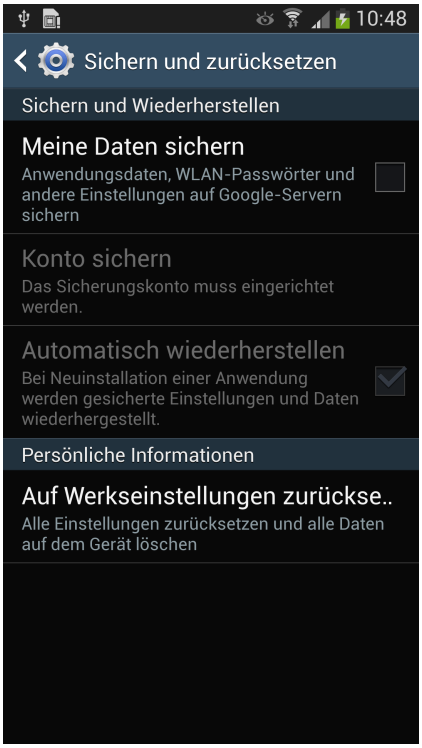
Zur erstmaligen Einrichtung wird ein PC mit einer USB-Verbindung zum Android-Gerät benötigt.

52.1. 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.

52.2. Verbindung auf dem Intra2net System

Bereiten Sie zuerst das Intra2net System auf eine Verbindung mit VPN-Clients vor wie in Abschnitt 46.2, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben. Danach kann die Verbindung wie in Abschnitt 46.3, „Automatische Konfiguration für Clients auf dem Intra2net System“ beschrieben, vorbereitet werden. Wählen Sie dabei "Natives Android" als VPN-Client-Typ.

52.3. Zertifikate

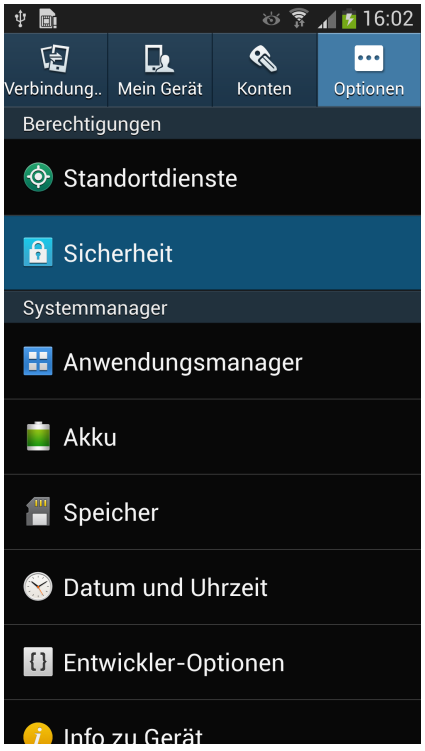
1. Beim Erstellen der Verbindung auf dem Intra2net System wird eine Datei mit dem privaten Schlüssel für den Android-Client (Endung `.p12`) erstellt und exportiert.

2. 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.

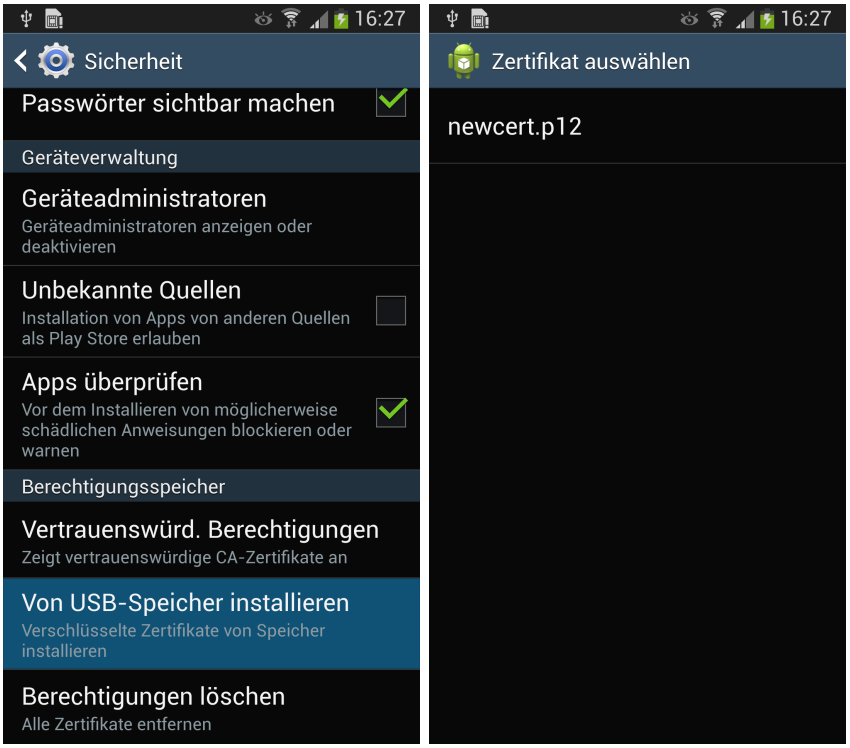
3. Kopieren Sie nun (z.B. mit dem Windows Explorer) die vorher exportierte `.p12`-Datei auf das Android-Gerät.

4. Trennen Sie die Verbindung zwischen PC und Android-Gerät ordnungsgemäß über die Trennen-Funktion in der Taskleiste von Windows.

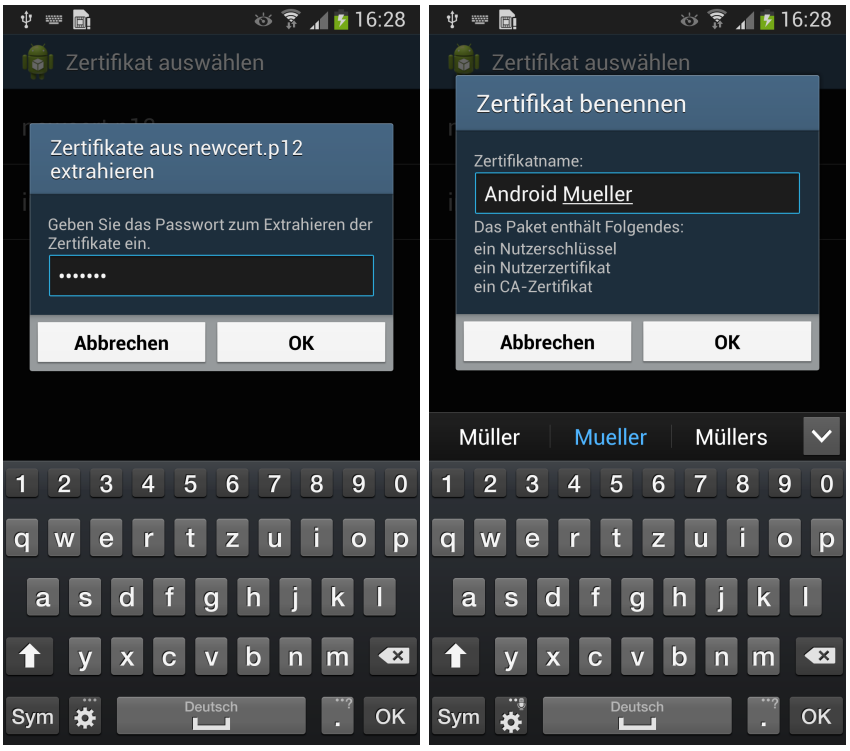
5. Öffnen Sie auf dem Android-Gerät die "Einstellungen", Reiter "Optionen", "Sicherheit".



6. Öffnen Sie in der Kategorie "Berechtigungsspeicher" den Menüpunkt "Von USB-Speicher installieren".

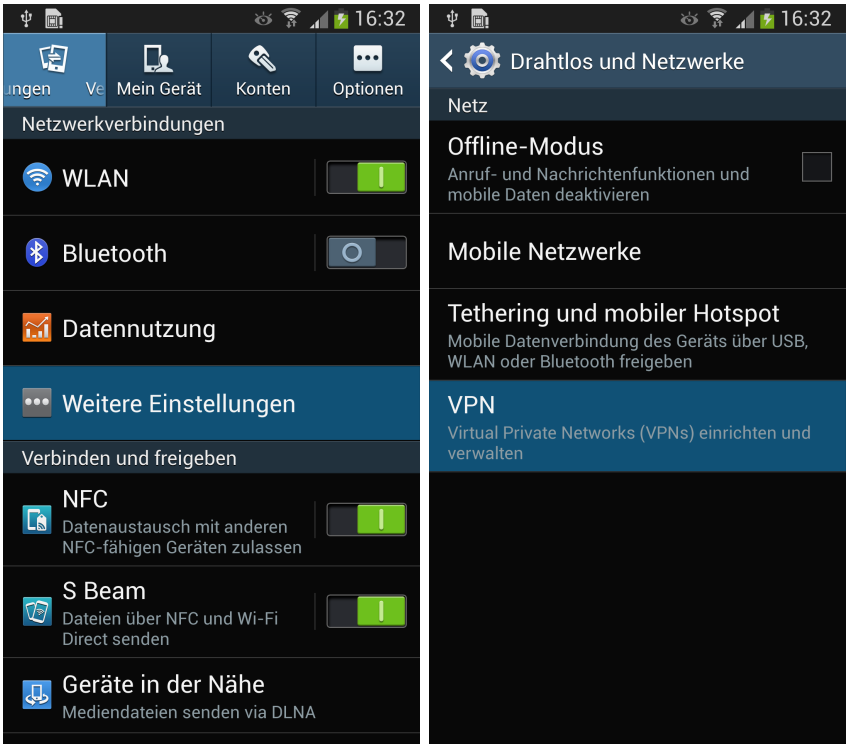


7. Klicken Sie den privaten Schlüssel (Dateiname `newcert.p12`) an um diesen zu importieren. Sie werden nach dem auf dem Intra2net System vergebenen Passwort gefragt und bekommen dann die Möglichkeit, einen passenden Namen für das Zertifikat zu vergeben.



52.4. 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.

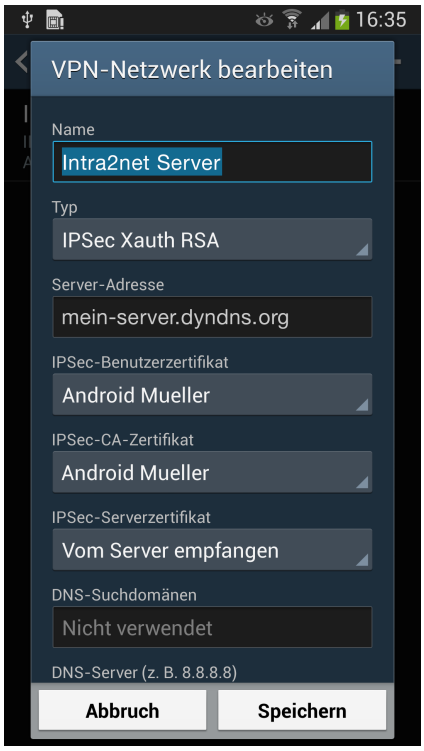
3. Wählen als Typ für das VPN "IPSec Xauth RSA" aus.

4. "Server-Adresse" ist der extern erreichbare, offizielle DNS-Name Ihres Intra2net Systems (besser) oder zur Not seine externe, feste IP.

5. Wählen Sie nun das "IPSec-Benutzerzertifikat", welches Sie vorhin vom PC importiert haben.

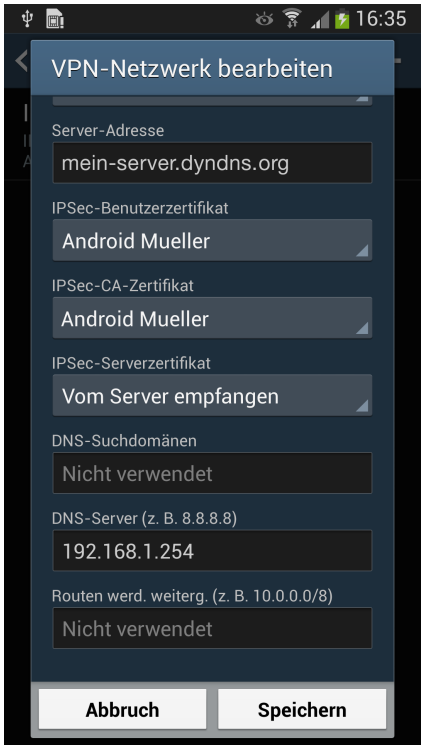
6. Wählen Sie bei "IPSec-CA-Zertifikat" auch das vorher importierte Zertifikat aus.

7. Das "IPSec-Serverzertifikat" lassen Sie auf der Voreinstellung (`Vom Server empfangen`).



8. Aktivieren Sie "Erweiterte Optionen anzeigen".

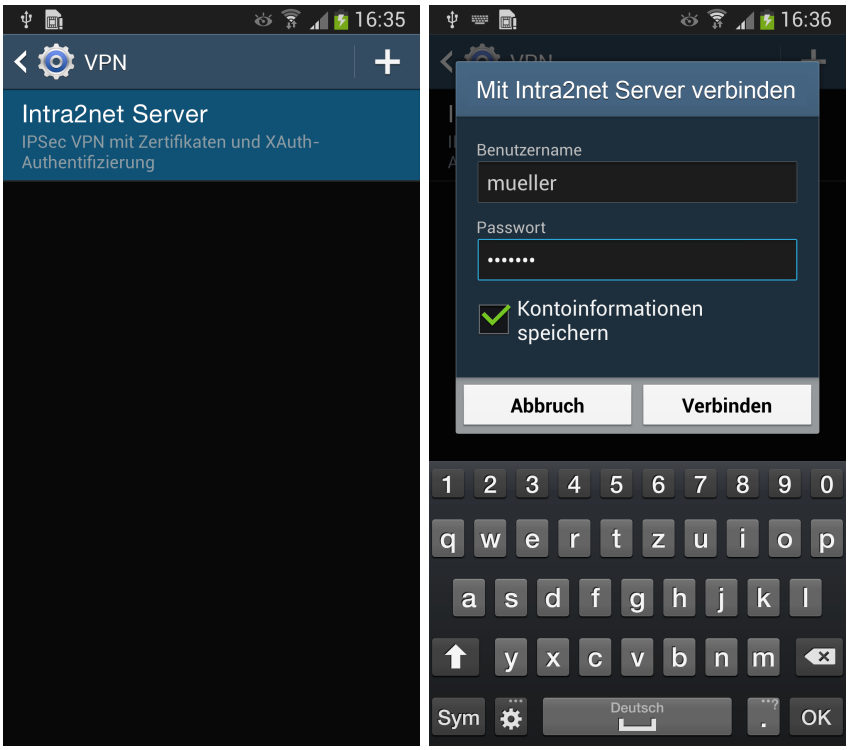
9. Tragen Sie bei "DNS-Server" die interne IP Ihres Intra2net Systems ein.



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 Intra2net System im Benutzermanager hinterlegt. Der Benutzer muss sich auf dem

Intra2net System in einer Benutzergruppe befinden, die das Recht hat sich am VPN mit XAUTH anzumelden.

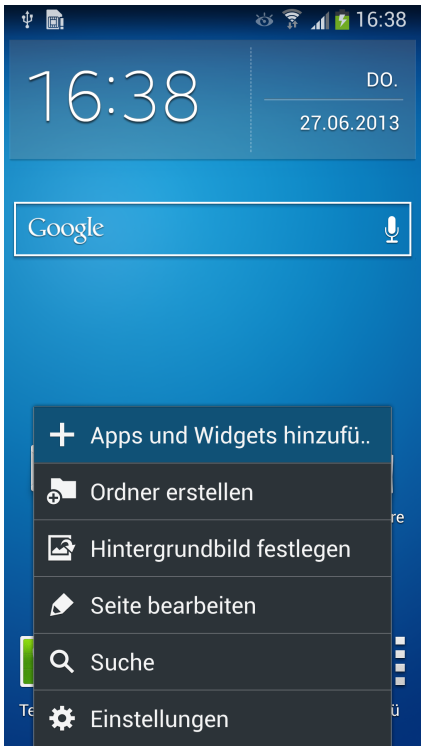


12. War der Verbindungsaufbau erfolgreich, wird oben links in der Statusleiste ein Schlüsselsymbol angezeigt.

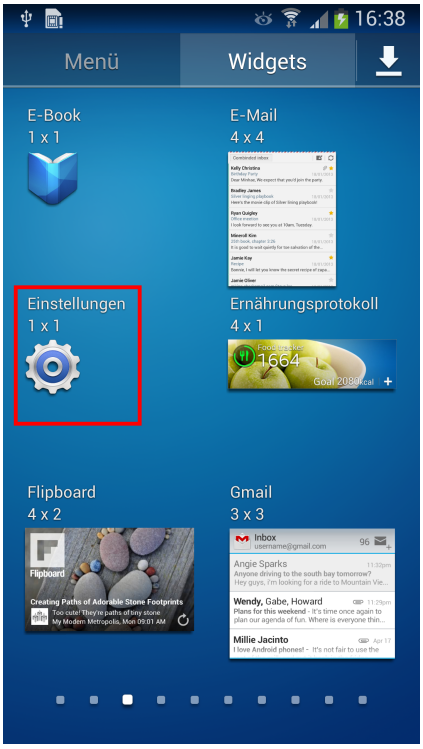
52.5. Verbindungsaufbau vereinfachen

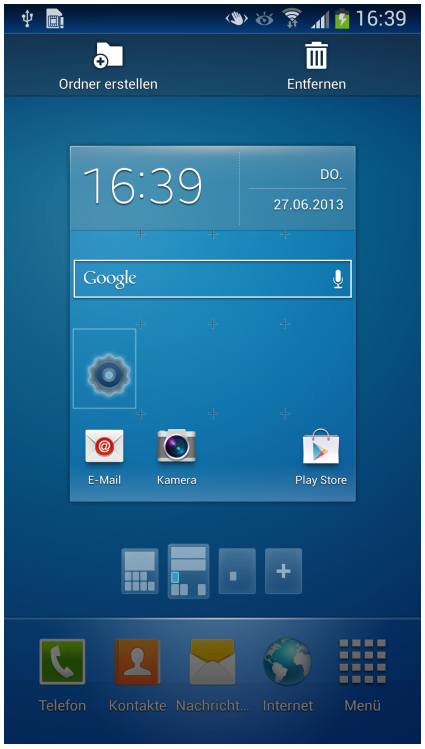
Die Verbindung wird immer über das VPN-Menü aufgebaut. Damit dies einfacher aufgerufen werden kann, gehen Sie wie folgt vor:

1. Gehen Sie auf den Hauptbildschirm und wählen "Apps und Widgets hinzufügen".

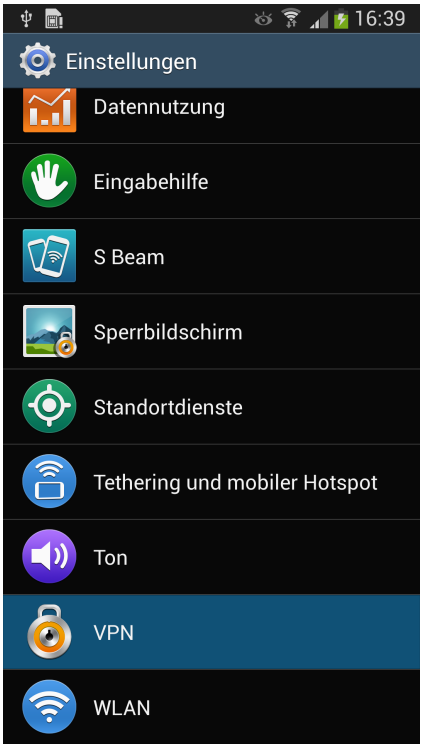


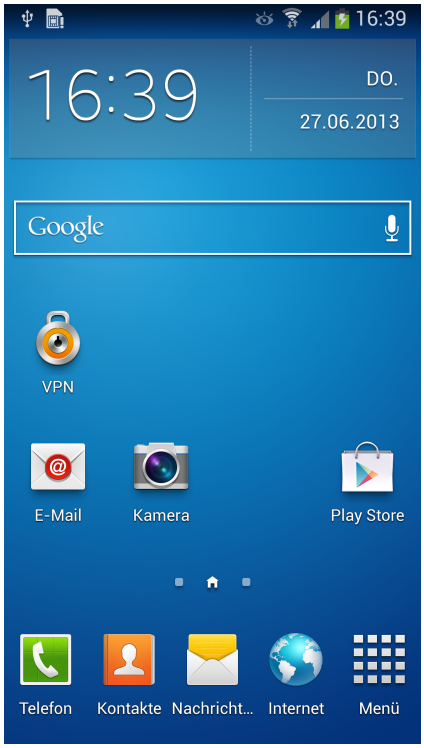
2. Öffnen Sie den Reiter "Widgets" und suchen die "Einstellungen". Halten Sie Ihren Finger auf den Einstellungen gedrückt bis der Hauptbildschirm angezeigt wird. Schieben Sie nun das Einstellungen-Widget auf einen freien Platz und lassen los.





3. Wählen Sie nun "VPN". Das VPN-Menü ist nun direkt vom Hauptbildschirm erreichbar.


16:39
Einstellungen
Datennutzung
Eingabehilfe
S Beam
Sperrbildschirm
Standortdienste
Tethering und mobiler Hotspot
Ton
VPN
WLAN


16:39
16:39
DO.
27.06.2013
Google
VPN
E-Mail
Kamera
Play Store
Telefon
Kontakte
Nachricht...
Internet
Menü

53. Kapitel - VPN mit dem NCP Secure Android Client Premium

Der NCP Secure Android Client Premium kann über den Google Play Store bezogen werden.

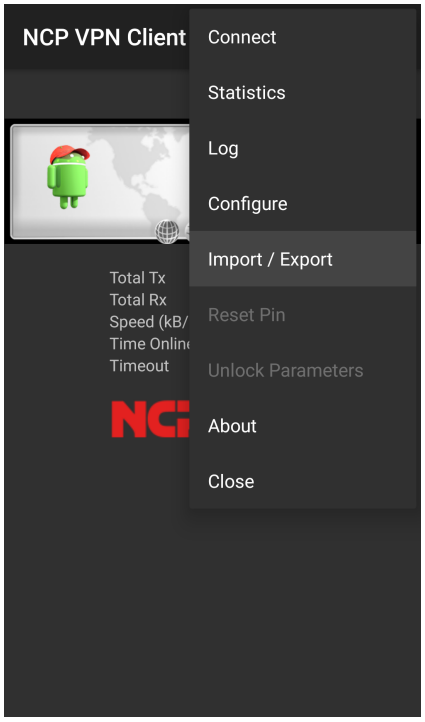
Bereiten Sie zuerst das Intra2net System auf eine Verbindung mit VPN-Clients vor wie in Abschnitt 46.2, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben. Danach kann die komplette Konfiguration für den Client durch das Intra2net System, wie in Abschnitt 46.3, „Automatische Konfiguration für Clients auf dem Intra2net System“ beschrieben, erzeugt werden.

Transferieren Sie die so erzeugte Konfigurationsdatei auf das Android-Gerät, z.B. als E-Mail-Anhang. Übergeben Sie dem Benutzer das Passwort, mit dem der private Schlüssel geschützt ist, auf einem anderen Weg, z.B. persönlich vor Ort. Versenden Sie dieses Passwort aus Sicherheitsgründen nicht per E-Mail.

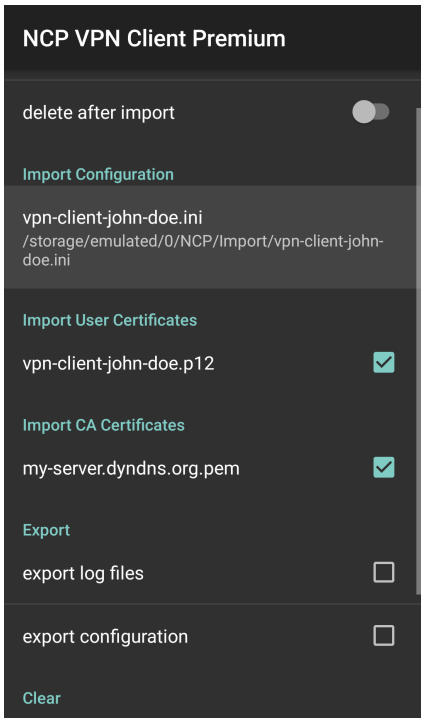
Gehen Sie dann auf dem Android-Gerät wie folgt vor, um die Konfiguration zu importieren:

1. Die Konfiguration besteht aus mehreren einzelnen Dateien und wird als ZIP-Datei gepackt übertragen. Öffnen Sie die ZIP-Datei im Dateimanager von Android, markieren alle enthaltenen Dateien und entpacken Sie sie in das Verzeichnis `NCP/Import` auf dem internen Speicher des Geräts.

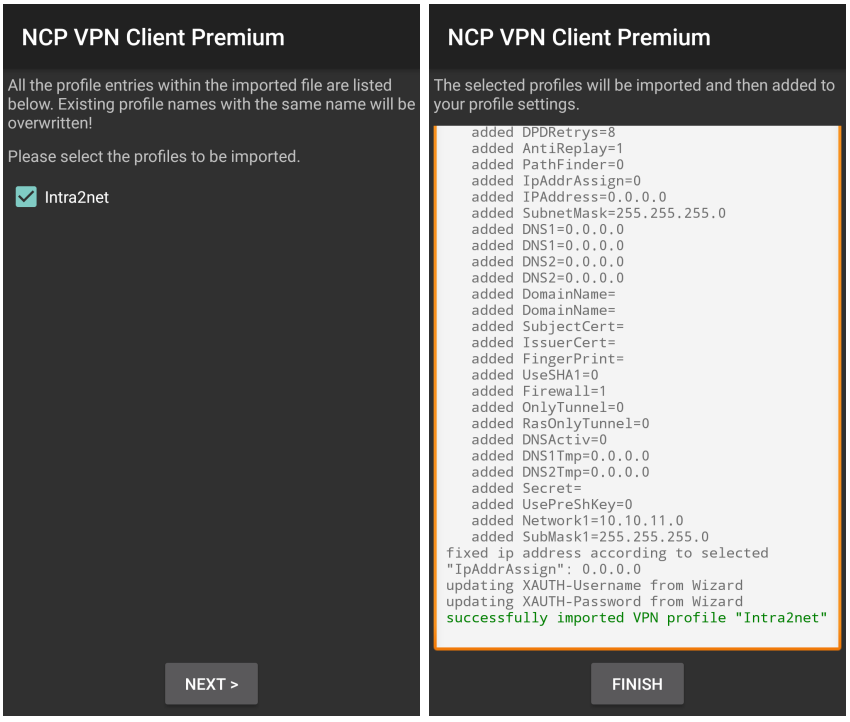
2. Starten Sie den VPN Client und gehen ins Menü "Import / Export".



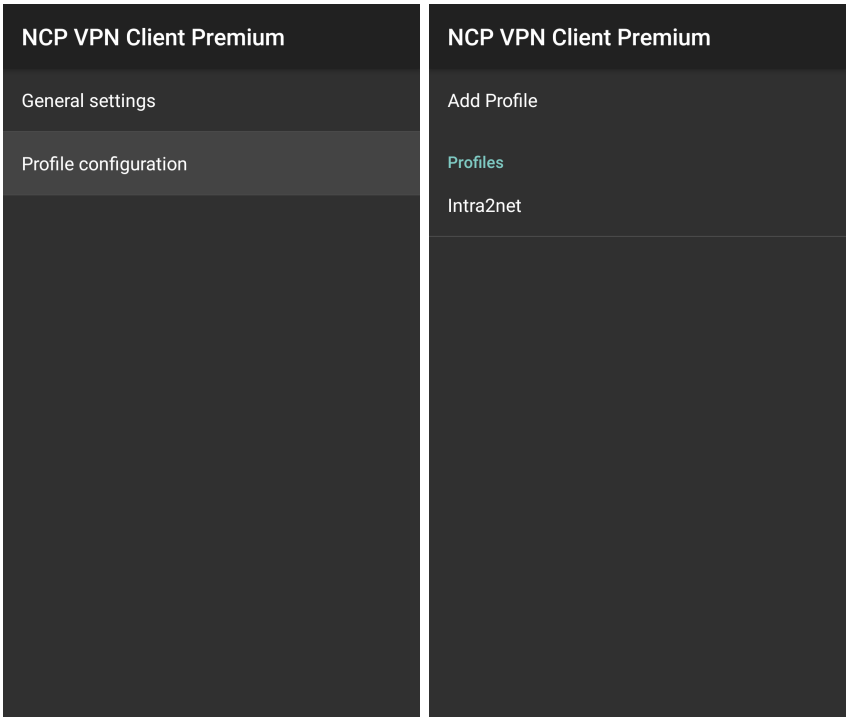
3. Wählen Sie unter "Import Configuration" die eben entpackte INI-Datei aus und starten den Import.



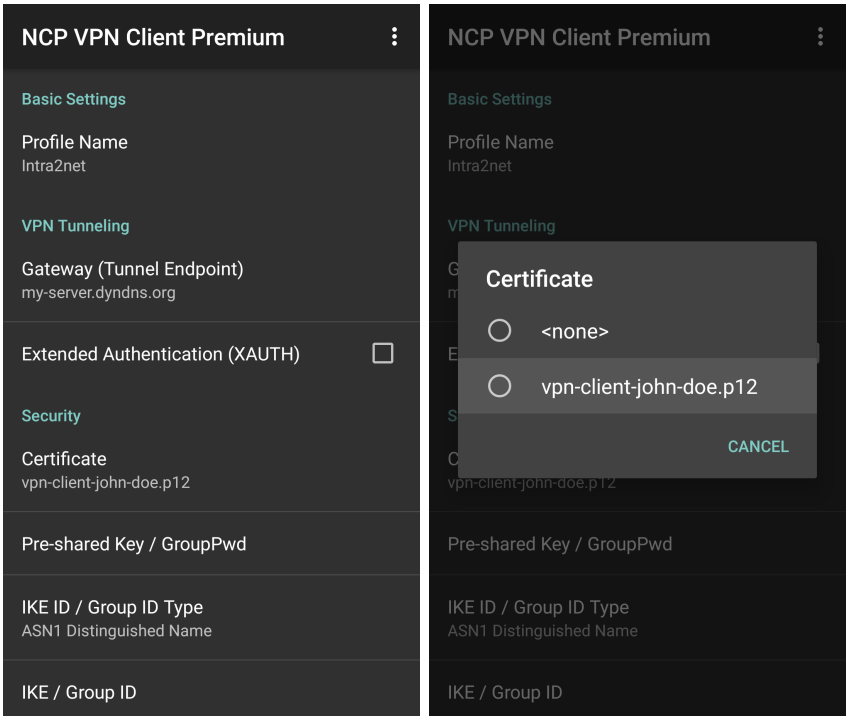
4. Bestätigen Sie, dass das Profil importiert werden soll. Das Profil sollte erfolgreich importiert werden können.



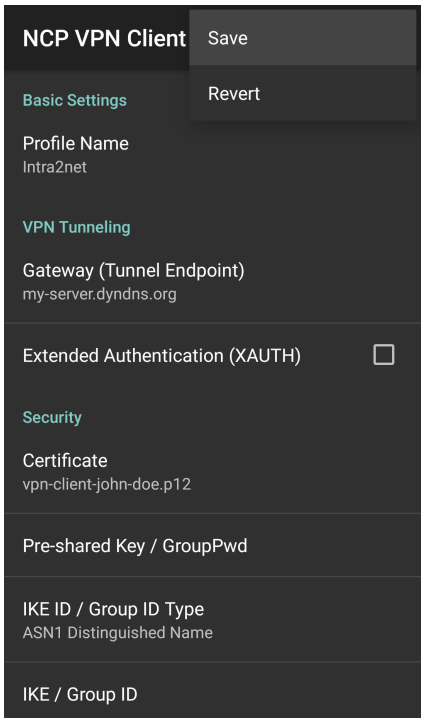
5. Gehen Sie ins Menü "Configure > Profile configuration" und öffnen das Profil "Intra2net".



6. Öffnen Sie den Menüpunkt "Certificate" und bestätigen die Verwendung des importierten Schlüssels für dieses Verbindung.

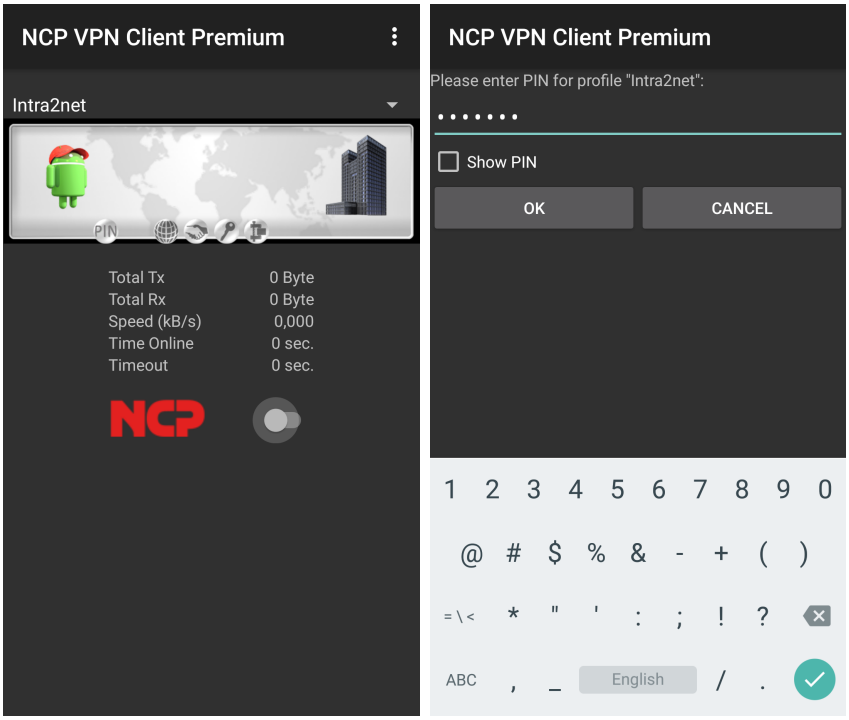


7. Speichern Sie das Verbindungsprofil.



Sie können die Verbindung jetzt durch das Umlegen des Schaltersymbols im VPN-Client aufbauen.

Für den Aufbau der Verbindung muss das Passwort, mit dem der private Schlüssel geschützt ist, eingegeben werden. Dieses Passwort wurde beim Erzeugen der Verbindung auf dem Intra2net System festgelegt.

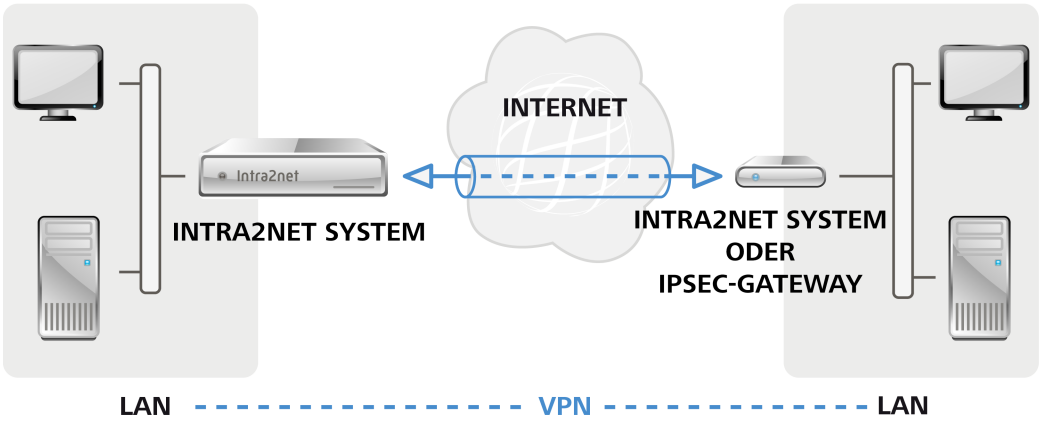


54. Kapitel - Anbinden von kompletten Netzen

54.1. Konzept

Wenn in einem entfernten Netz mehrere Rechner mit einem Netz hinter dem Intra2net System 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 Intra2net System und einem IPSec Gateway vor dem anderen Netz aufgebaut. Dieses IPSec Gateway kann ein Intra2net System 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 das Intra2net System 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 Intra2net System konfigurierte Verbindung gilt für die Verbindung von einem Netz auf Seite der Gegenstelle und einem Netz hinter dem Intra2net System. 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.

54.2. Konfiguration auf dem Intra2net System

54.2.1. Voraussetzungen

Als Erstes müssen Sie dafür sorgen, dass jede Seite über einen eigenen Schlüssel verfügt und die Gegenseite den öffentlichen Schlüssel der Gegenseite hat. Es empfiehlt sich, auf jedem System einen eigenen Schlüssel nur für VPNs anzulegen.

Wenn Sie auf dem Intra2net System 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 45. Kapitel, „Schlüsselmanagement“.

54.2.2. Grundeinstellungen

Im Menü Dienste > VPN > Verbindungen können Sie VPN-Verbindungen im Intra2net System konfigurieren. Legen Sie eine neue Verbindung an und wählen den Typ "IPSec: Site-to-Site oder eigene Konfiguration".

Auf der ersten Seite stellen Sie die Gegenstelle ein. Die Gegenstelle ist die offizielle IP, unter der das Intra2net System 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 Intra2net System 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 44.5, „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.

54.2.3. Authentifizierung

Wählen Sie den eigenen und den Schlüssel der Gegenseite aus.

Wir raten aus den in Abschnitt 44.6, „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.

54.2.4. 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 Intra2net Systems gewählt. Wählen Sie bei der Option "Lokale Netze" eines der direkt an das Intra2net System 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 58. Kapitel, „Lösen von IP-Adresskonflikten in VPNs durch NAT“ erklärt.

54.2.5. 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 9.3, „Zugriffsrechte eines Netzwerkobjekts“.

54.2.6. Aktivierung

In diesem Menü wird konfiguriert, wann die Verbindung aufgebaut und bestehende Sitzungen verlängert werden.

Beim passiven oder manuellen Start wartet das Intra2net System, bis entweder die Gegenseite die Verbindung aufbaut oder der Benutzer über die Hauptseite die Verbindung manuell aufbaut. Wird die Verbindung immer gestartet, versucht das Intra2net System 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 das Intra2net System 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.

55. Kapitel - VPN mit ZyXEL ZyWALL USG

55.1. 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 44.6, „Einschränkungen“ beschriebenen Einschränkungen umgehen.

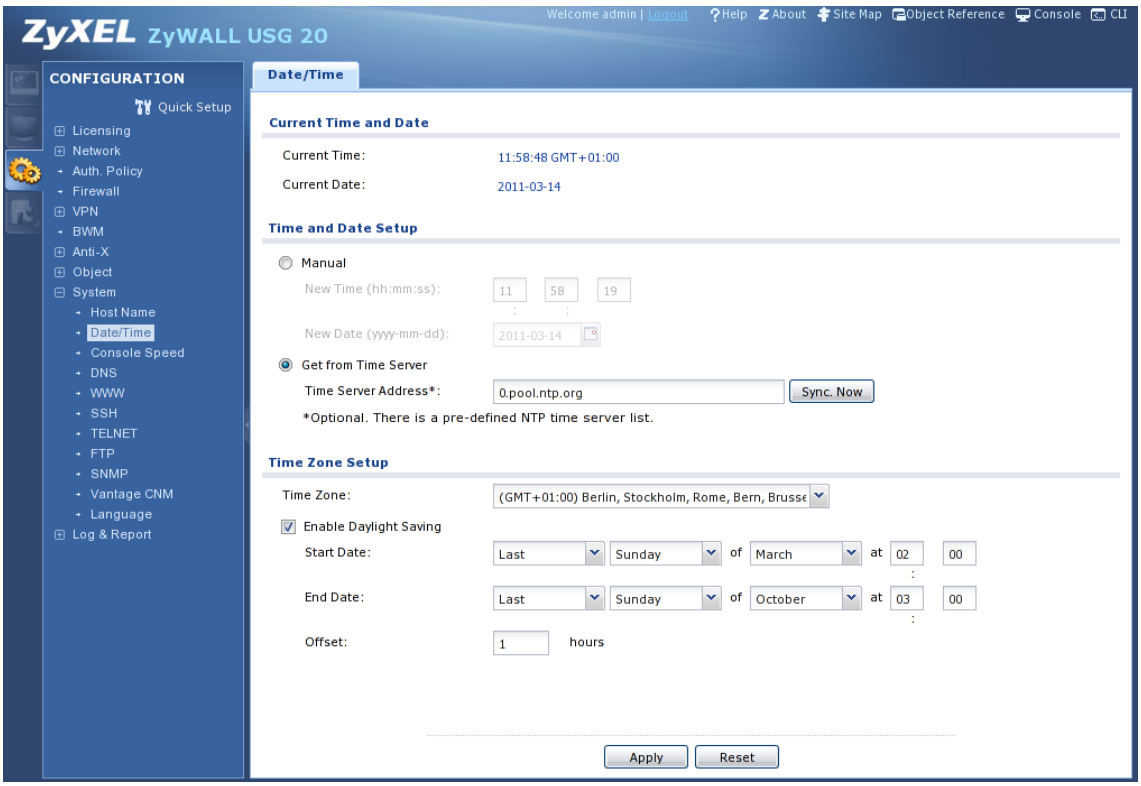
Der Router unterstützt selbstsignierte Zertifikate und kann diese auch selbst erstellen. Die Einrichtungszeit wird dadurch deutlich verkürzt.

Selbstverständlich unterstützt das Intra2net System 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.

55.2. 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.

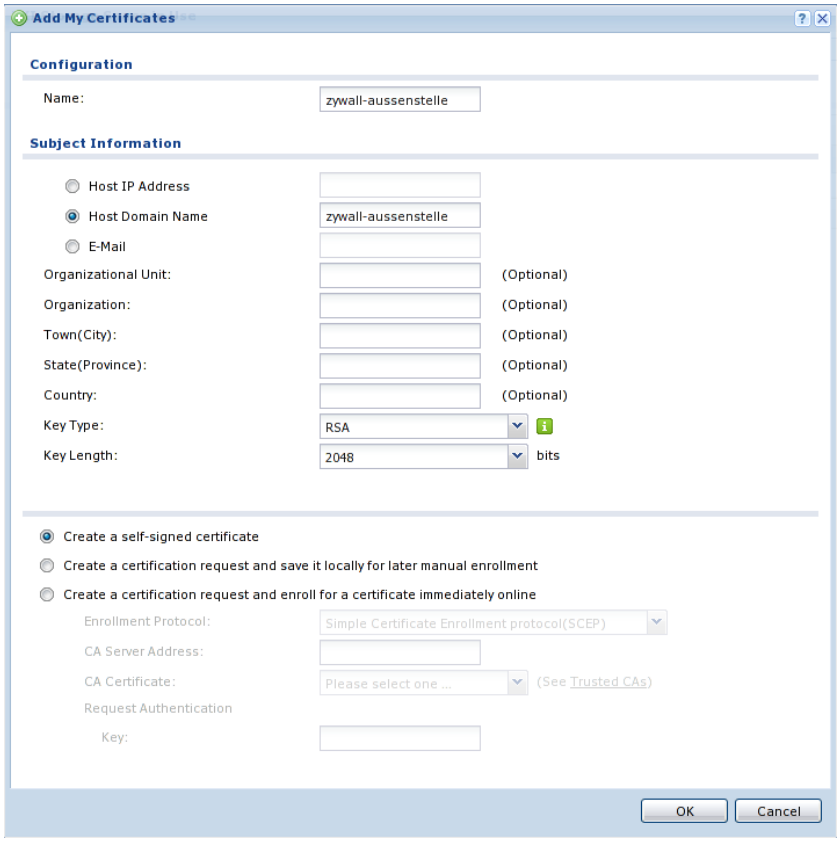
Der Router aktualisiert seine Zeit über das NTP-Protokoll. Dies kann im Menü "Configuration > System > Date/Time" überprüft und konfiguriert werden. Öffnen Sie das Menü und stellen Sie Zeitzone und Sommerzeitumstellung (Daylight Saving) korrekt ein. Testen Sie über den Knopf "Sync Now" ob die Synchronisation per NTP wirklich funktioniert.



55.3. Zertifikate

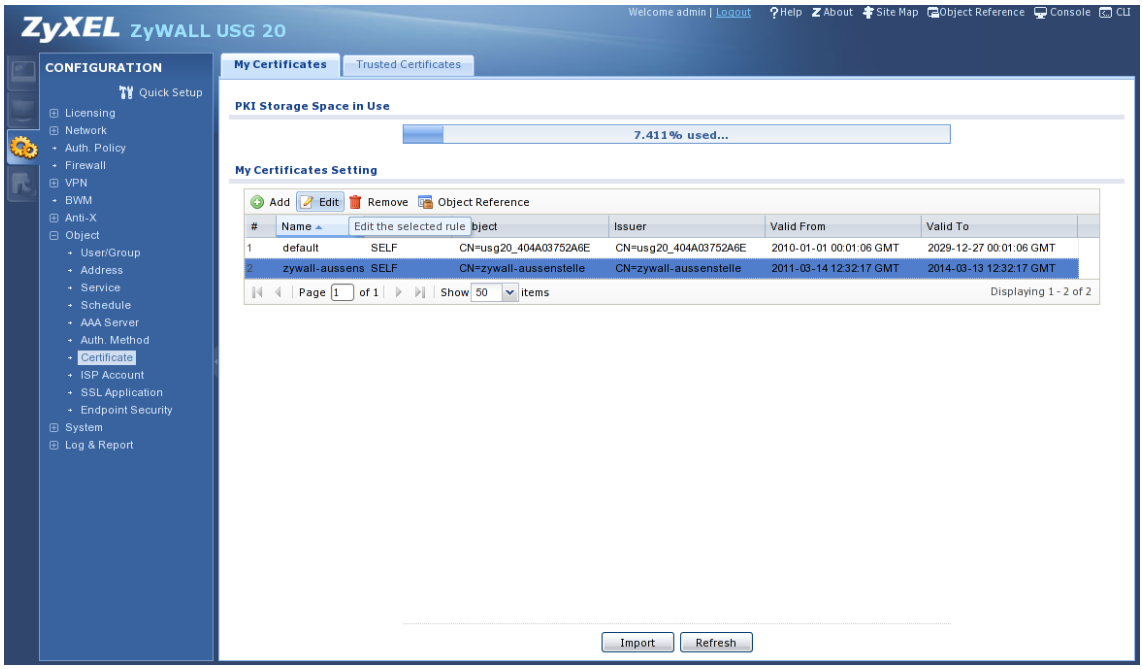
1. Öffnen Sie das Menü "Configuration > Object > Certificates". Über den Menüpunkt "Add" können Sie ein neues Zertifikat anlegen.

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.

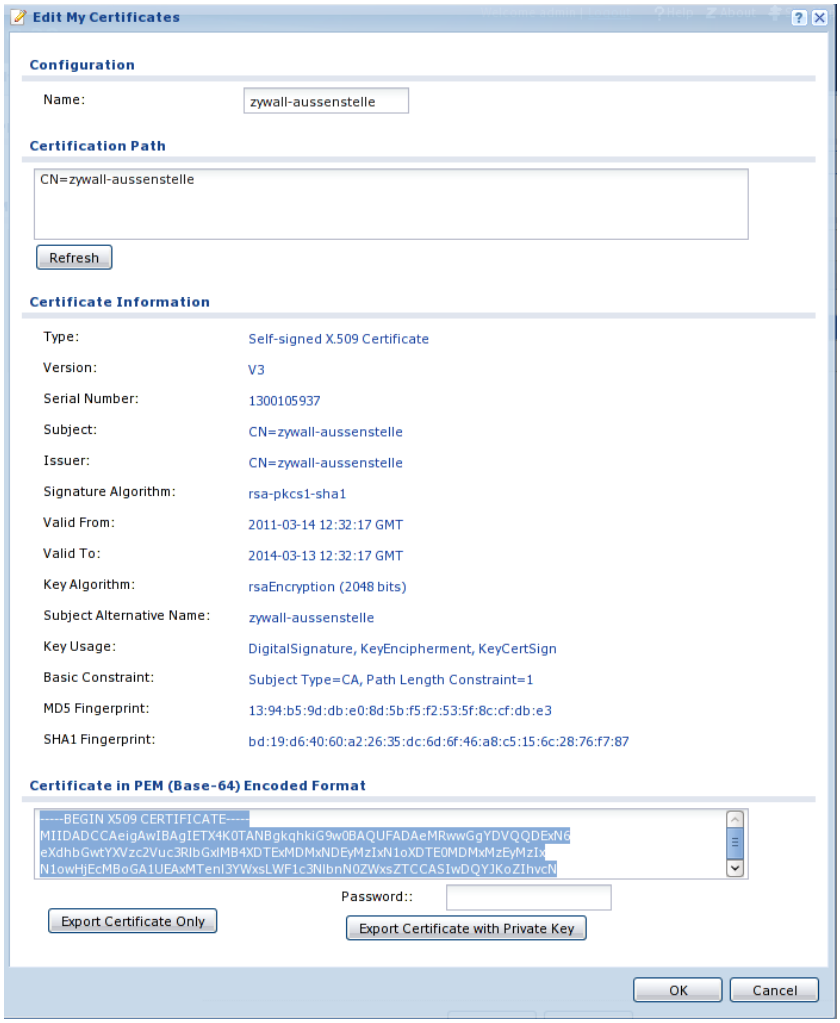


3. Das Erstellen des Zertifikats dauert bis zu 5 Minuten.

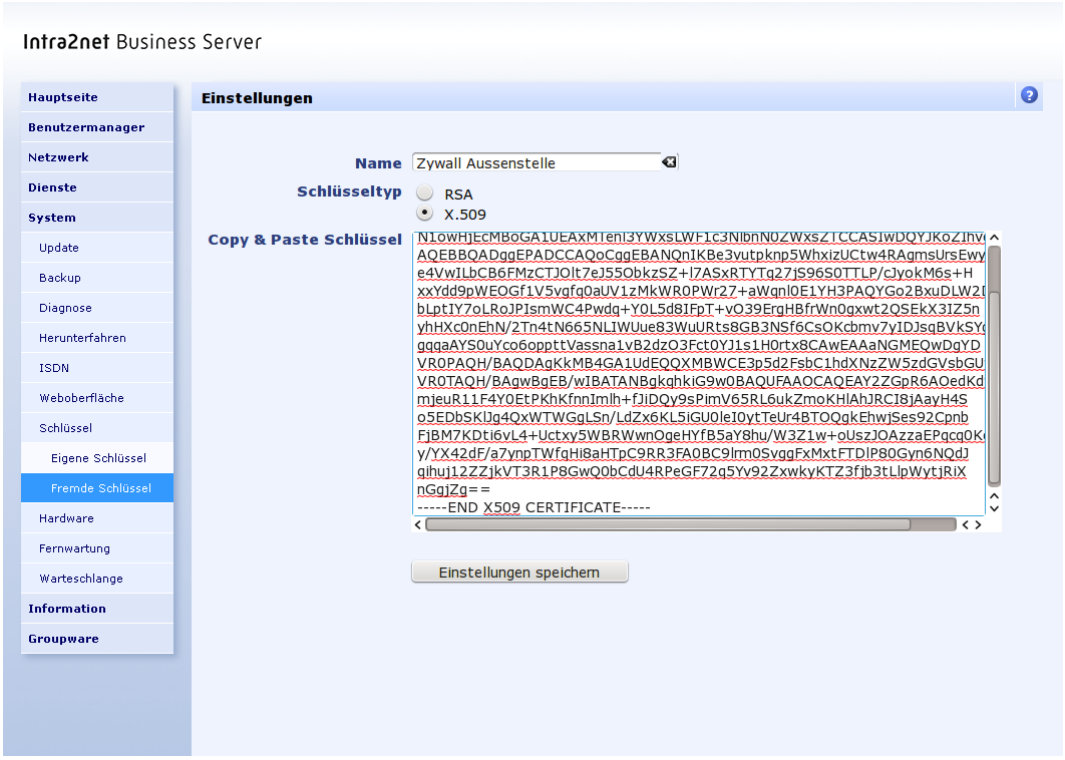
4. Öffnen Sie die Detail-Daten des Zertifikats über die Option "Edit".



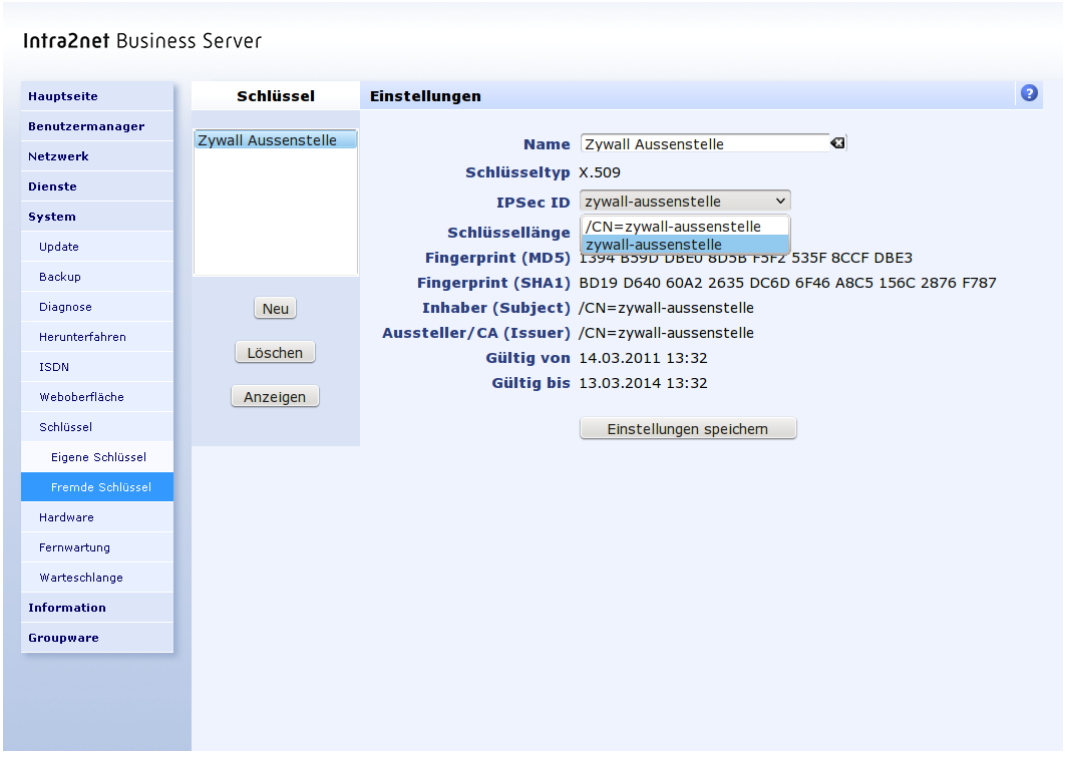
5. Übernehmen Sie das Zertifikat im PEM-Format in die Zwischenablage.



6. Importieren Sie das Zertifikat aus der Zwischenablage in das Intra2net System über das Menü "System > Schlüssel > Fremde Schlüssel".



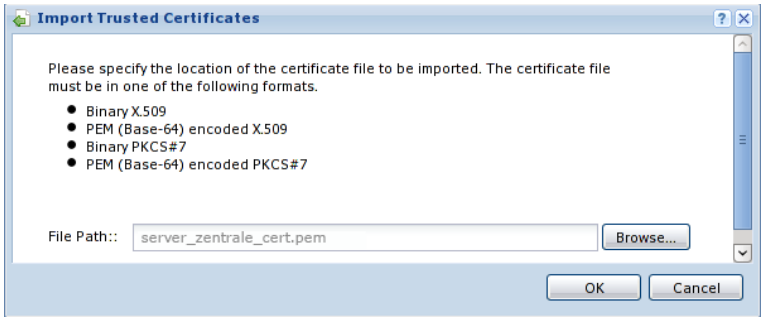
7. Wählen Sie unter IPSec ID den puren DNS-Hostnamen, nicht den Inhaber des Zertifikats ("/CN=" etc.).



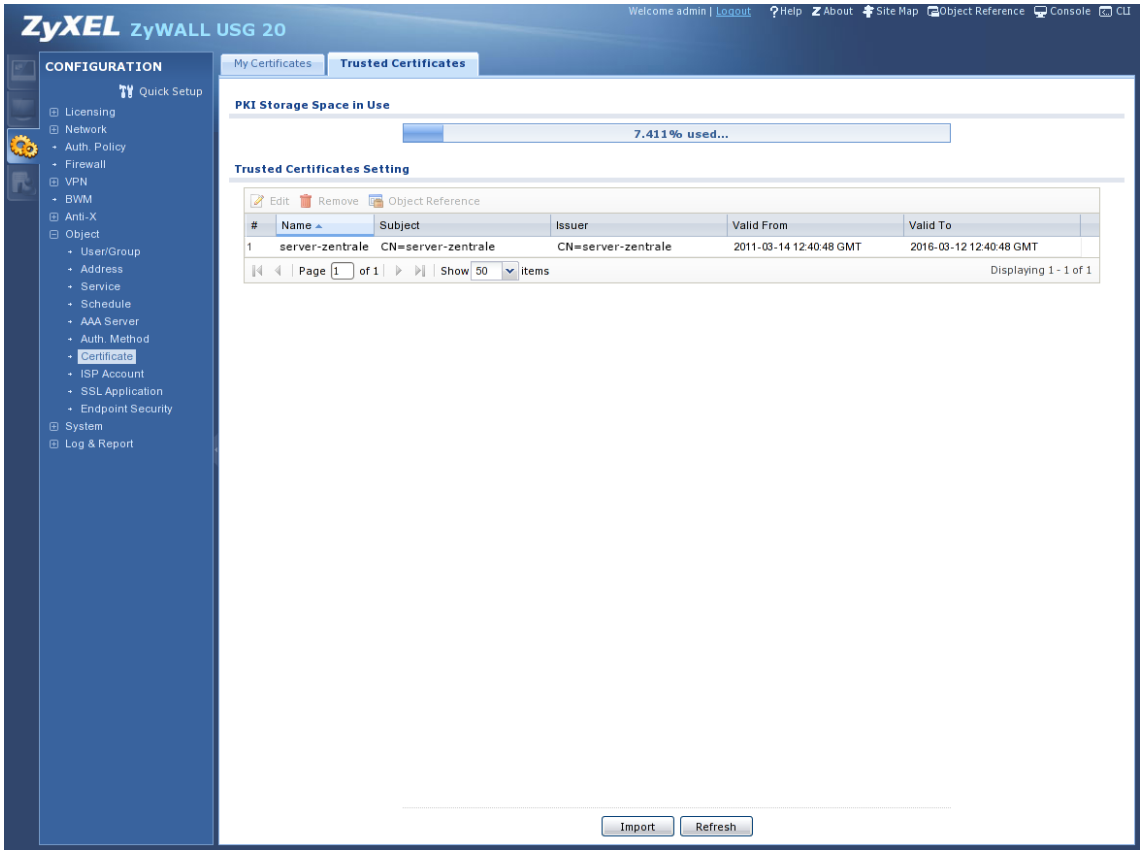
8. Exportieren Sie das eigene Zertifikat des Intra2net Systems als .pem-Datei (Menü "System > Schlüssel > Eigene Schlüssel", Reiter Daten.

9. Importieren Sie das Zertifikat des Intra2net Systems 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 Intra2net Systems gespeichert haben.



11. Das Zertifikat des Intra2net Systems wird nun als Trusted Certificate angezeigt.



55.4. Verbindung

55.4.1. IKE / Phase 1

1. Öffnen Sie das Menü "Configuration > VPN > IPSec VPN, Reiter VPN Gateway". Legen Sie mit "Add" eine neue IKE-Verbindung zu einer Gegenstelle an.

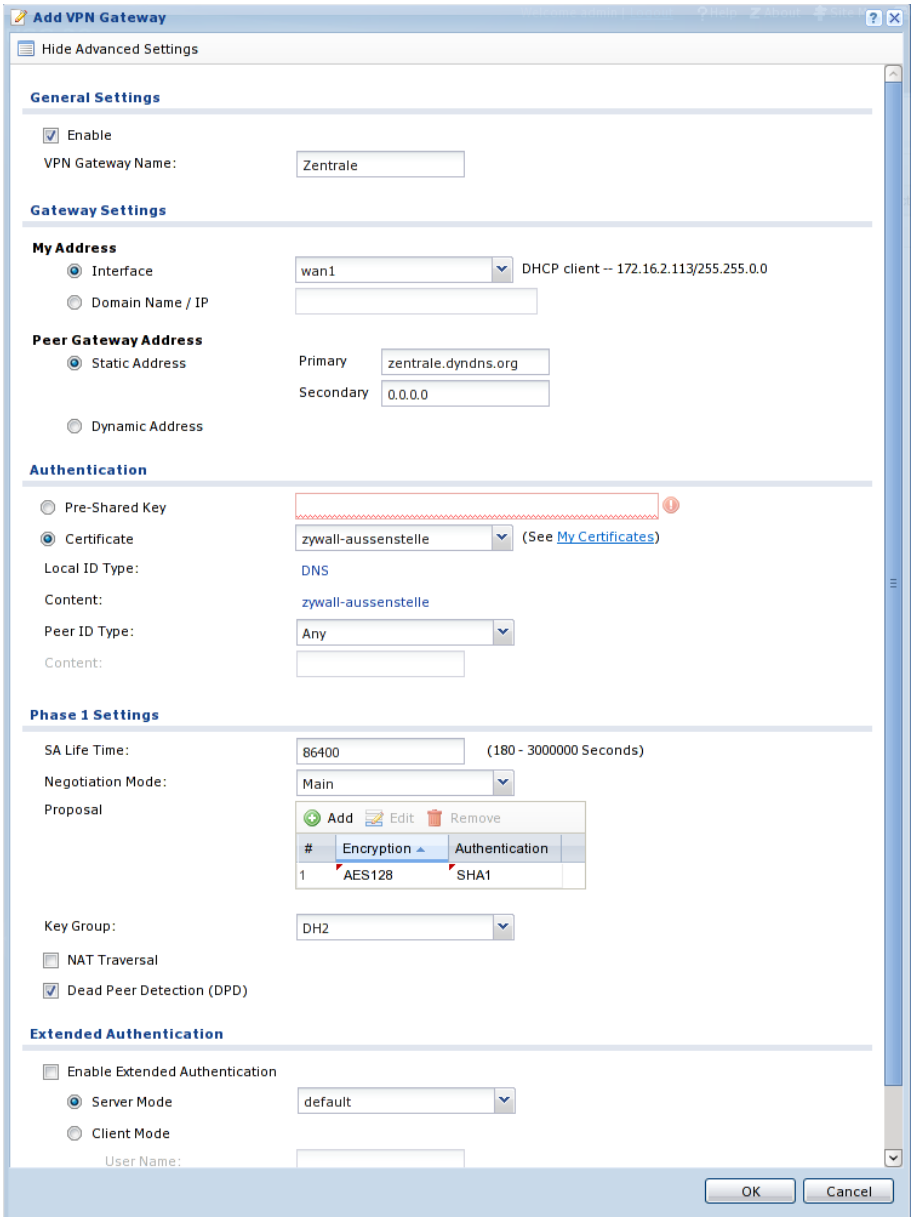
2. Klicken Sie auf "Show Advanced Settings", um alle nötigen Felder angezeigt zu bekommen.

3. Geben Sie die IP oder den DNS-Namen des Intra2net Systems als Peer Gateway Address ein. Auch wenn das Intra2net System eine dynamische IP mit DynDNS verwendet, müssen Sie "Static Address" wählen.

4. 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.

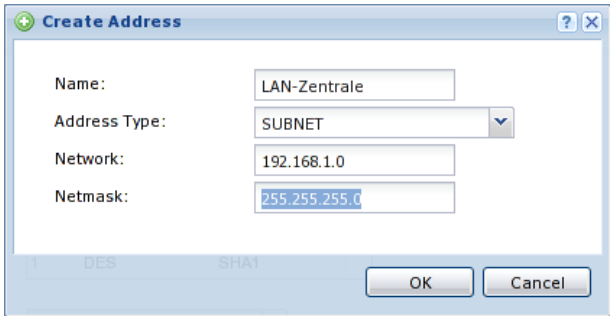
6. Sollte sich die Zywall oder das Intra2net System hinter einem NAT-Router befinden, müssen Sie die Option "NAT Traversal" aktivieren.



55.4.2. 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.



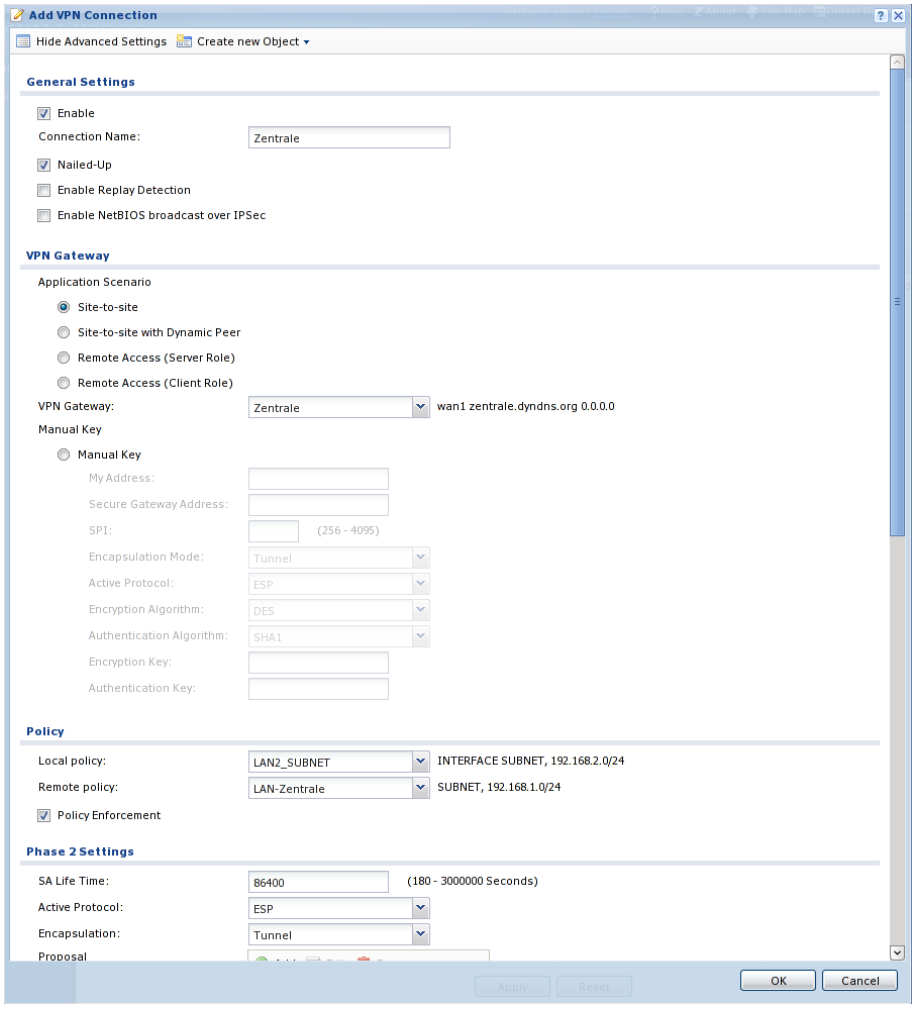
3. Klicken Sie auf "Show Advanced Settings", um alle nötigen Felder angezeigt zu bekommen.

4. Stellen Sie die Verbindung auf Nailed Up, damit die ZyWALL die Verbindung von sich aus offen hält.

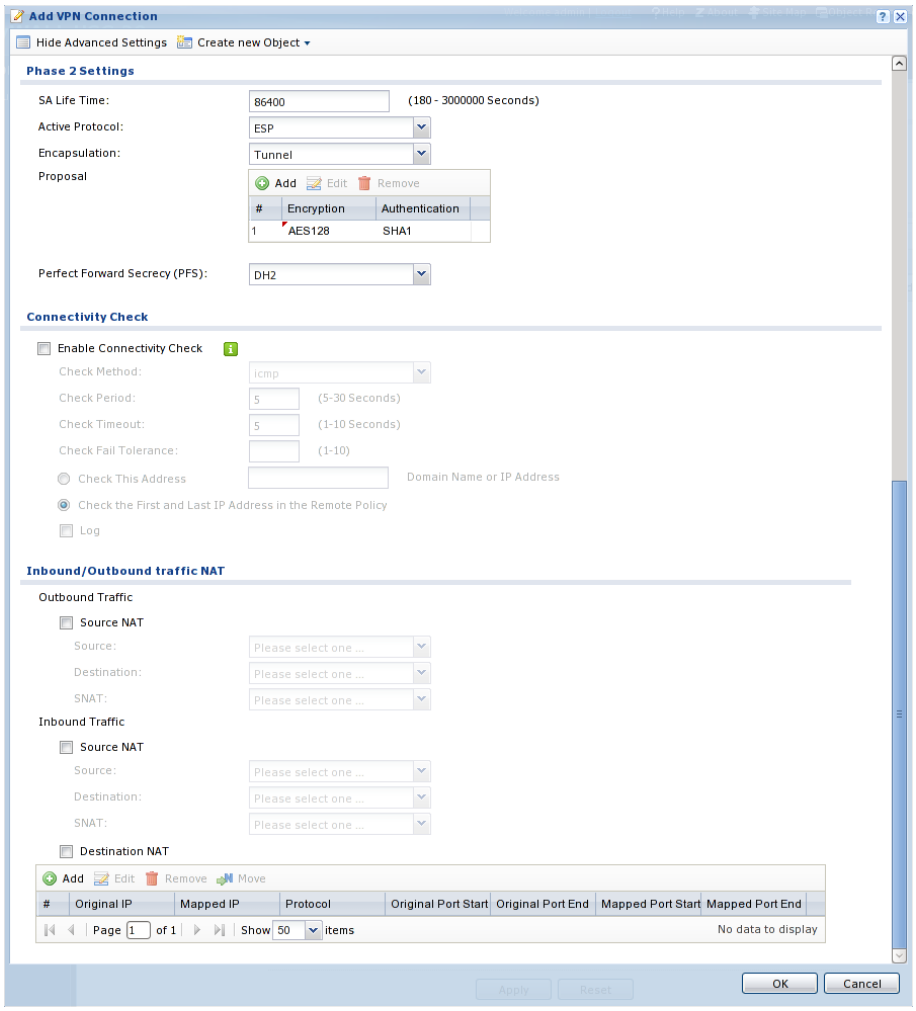
5. Wählen Sie Site-to-site und wählen als Gateway die eben angelegte IKE-Verbindung zum Intra2net System.

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 Intra2net Systems.

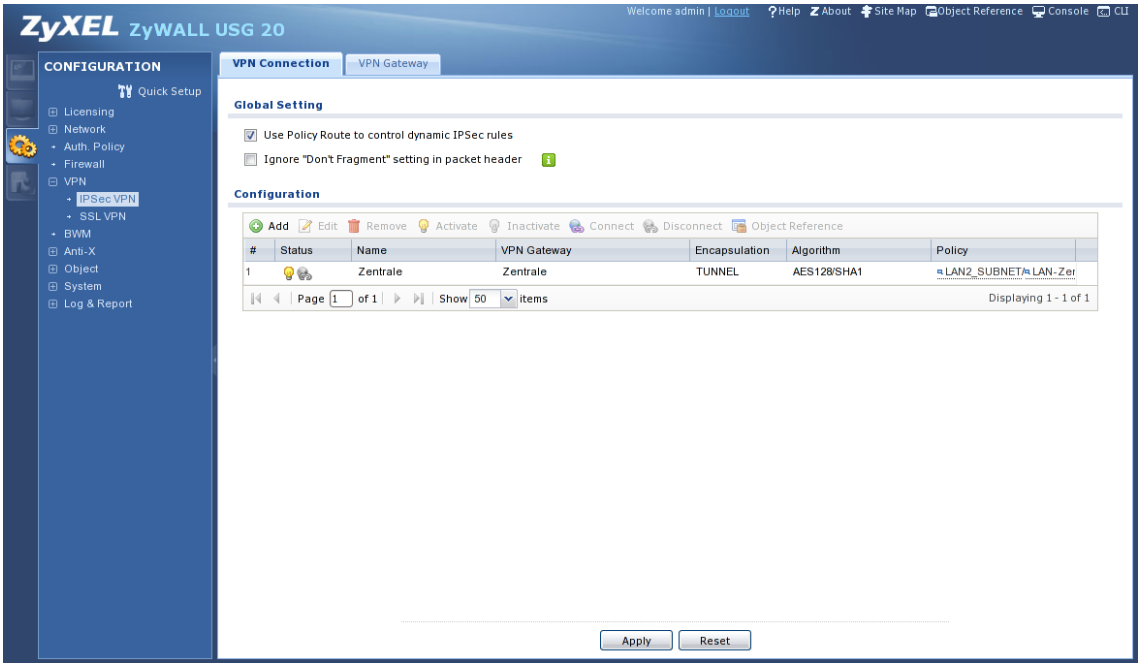
7. Aktivieren Sie "Policy Enforcement", um die Sicherheit der Verbindung gegen Netzmanipulationen zu gewährleisten.



8. 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.

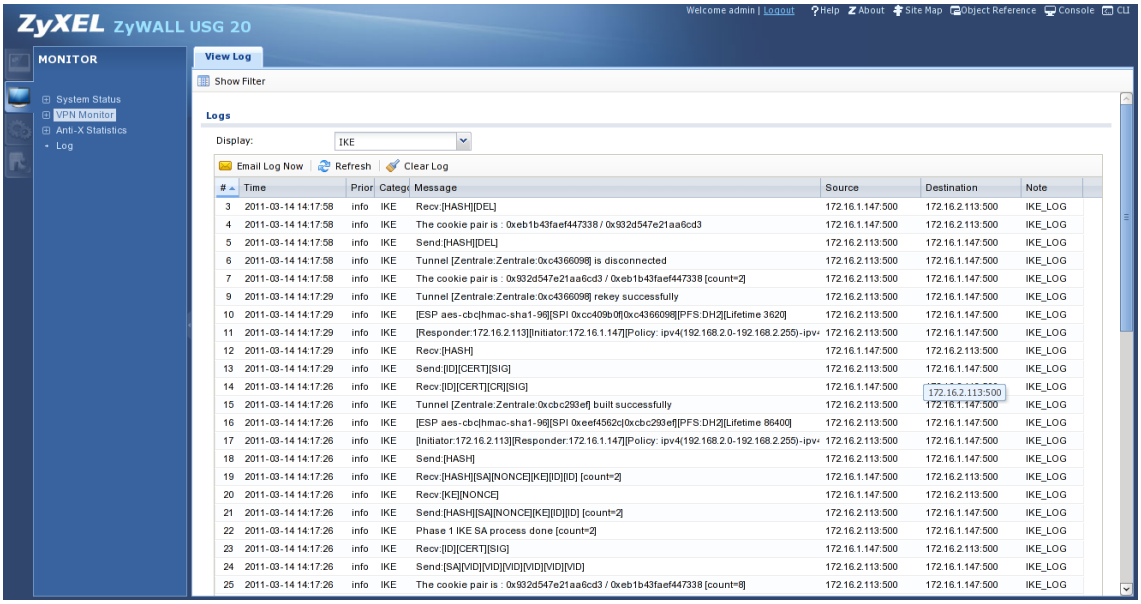


55.5. Intra2net System

Auf dem Intra2net System muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Router wird dies im 54. Kapitel, „Anbinden von kompletten Netzen“ beschrieben.

55.6. 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`.



56. Kapitel - VPN mit Lancom Routern

56.1. Überblick

VPN-fähige Router von Lancom können ab LCOS Version 6 Verbindungen mit Zertifikaten aufbauen und sind mit dem Intra2net System kompatibel. Diese Anleitung wurde für Version 8.84 erstellt. An der VPN-Konfiguration ändert sich aber in den meisten Versionen erfahrungsgemäß nicht viel.

56.2. Zertifikat für das Lancom-Gerät

1. Laden Sie vom Intra2net System 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 Intra2net System) 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
```

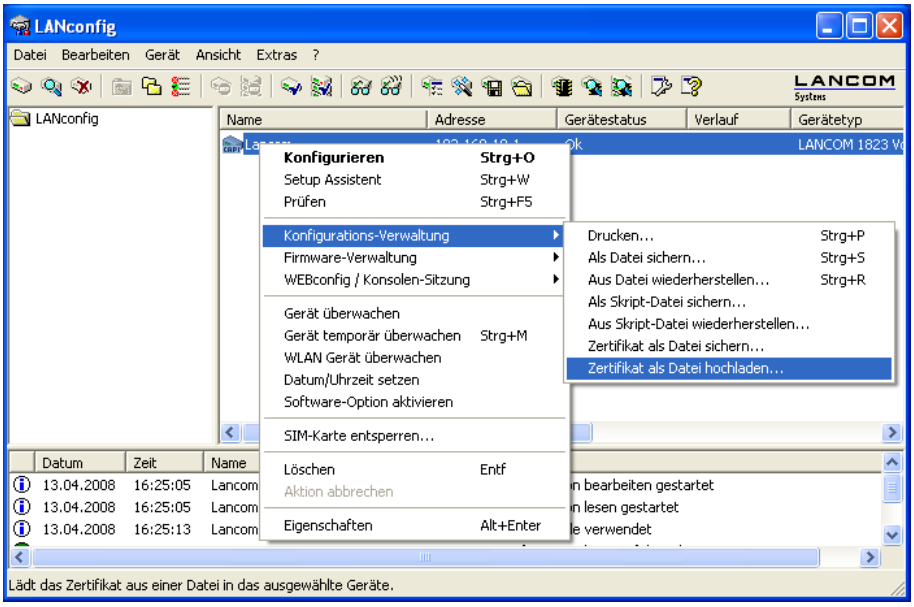
4. Wählen Sie ein Transportpasswort, mit dem die Schlüsseldatei auf dem Weg zum Router geschützt wird. Das Passwort muss mindestens 3 Zeichen lang sein.

```
Enter Export Password:
Verifying password - Enter Export Password:

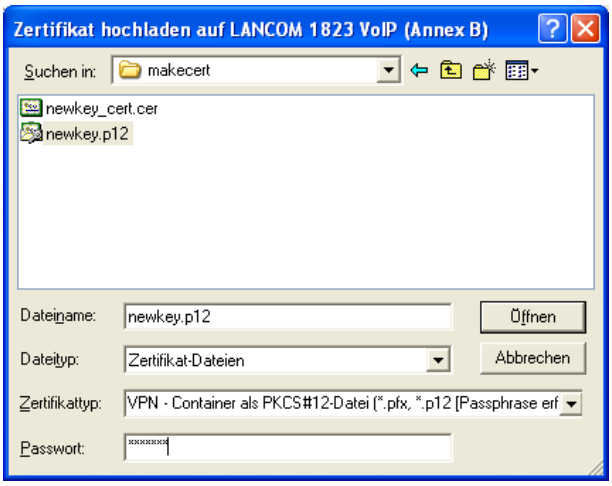
C:\makecert>del privatekey.pem
```

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 `newkey.p12` aus, die Sie eben mit dem makecacert-Programm erzeugt haben. Stellen Sie den Zertifikattyp auf "VPN - Container als PKCS#12-Datei" und geben das vorhin gewählte Transportpasswort ein.



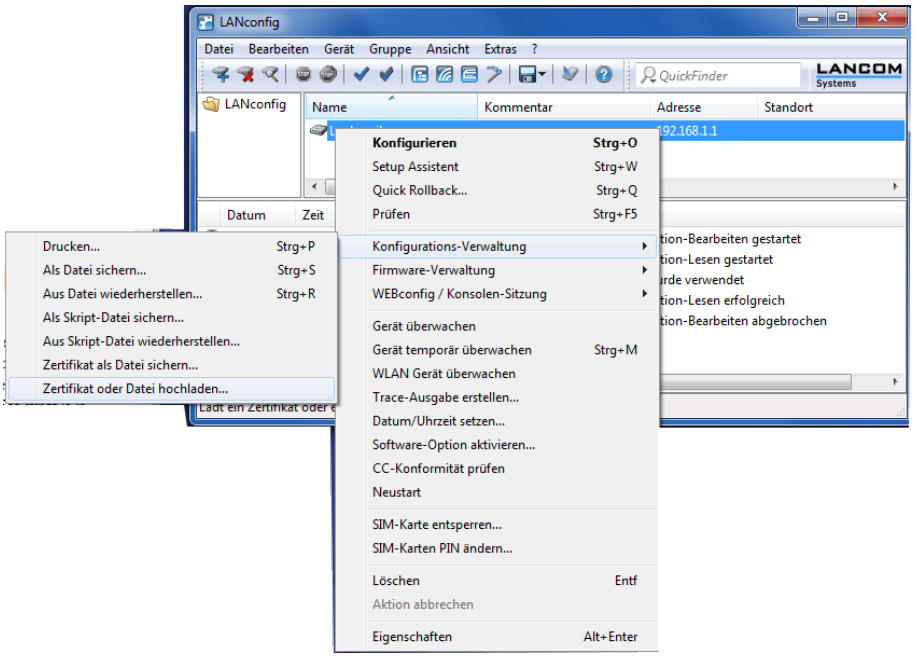
8. Öffnen Sie die Datei `newkey_cert.cer` in einem Texteditor (z.B. write) und übernehmen den Inhalt in die Zwischenablage. Öffnen Sie im Intra2net System das Menü System > Schlüssel > Fremde Schlüssel und legen einen neuen an. Vergeben Sie einen Namen für den Schlüssel (z.B. den Namen des Routers) und fügen dann die Zertifikatsdaten aus der Zwischenablage in das Feld "Copy > Paste Schlüssel" ein.

56.3. Zertifikat für das Intra2net System

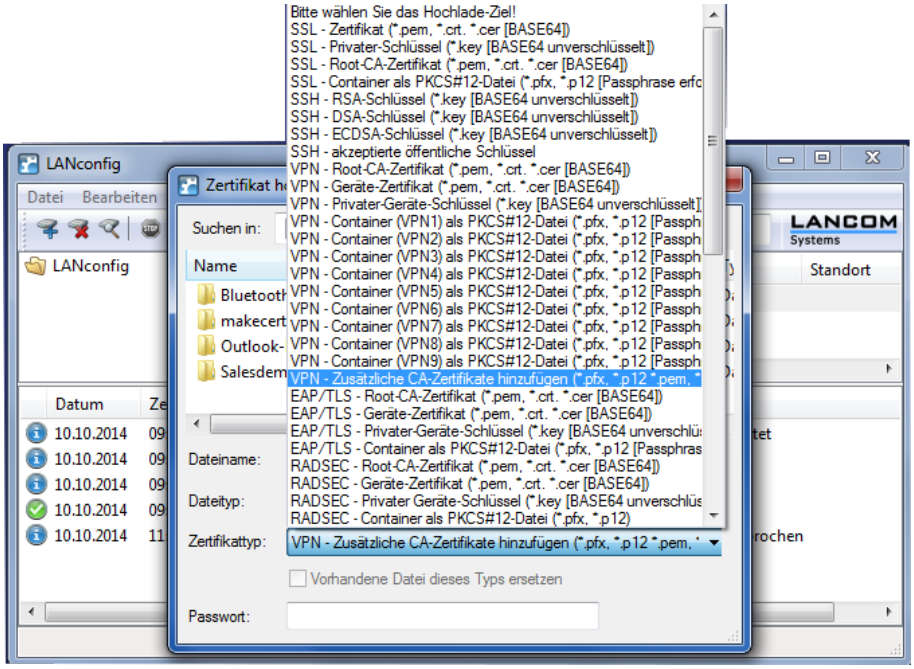
1. Der Lancom-Router erfordert eine besondere Konfiguration des Zertifikats auf dem Intra2net System. Seit den 8-er Versionen der LCOS-Firmware werden keine selbstsignierten Schlüssel mehr akzeptiert, sondern nur von einer eigenständigen CA signierte Zertifikate. Im folgenden wird gezeigt, wie ein solcher Schlüssel auf dem Intra2net System erzeugt und signiert wird.

2. Zunächst muss das Zertifikat für die CA erstellt werden: Öffnen Sie im Intra2net System 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 **`server-ca`** (einzutragen in den Feldern "Name" sowie "Rechername (CN)").

3. Dem Lancom-Router muss nun dieses CA-Zertifikat übermittelt werden. Dazu exportieren Sie es aus dem Intra2net System 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.



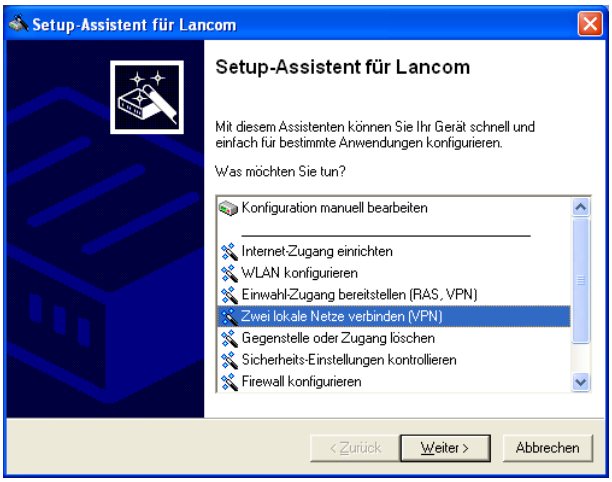
4. Wenden Sie sich nun wieder dem Intra2net System zu, unter dem Menü System > Schlüssel > Eigene Schlüssel : Daten. Legen Sie einen weiteren Schlüssel als Grundlage für das VPN-Zertifikat an. Bei der Erstellung ist zu beachten, dass der Wert des Feldes "Rechnername (CN)" (also der "Common Name" eines 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 Intra2net System zum Menü System > Schlüssel > Eigene Schlüssel : CA und wählen Sie hier den soeben erstellten VPN-Schlüssel des Intra2net Systems aus. Im Abschnitt "Schlüssel mit einem anderen Schlüssel signieren" wählen Sie den in den vorangehenden Schritten erzeugten CA-Schlüssel aus (**`server-ca`**) und klicken anschließend auf "Signieren".

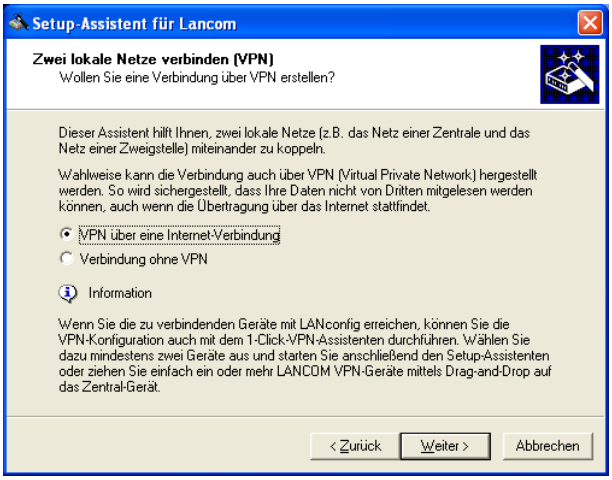
   Überprüfen Sie nun unter System > Schlüssel > Eigene Schlüssel : Daten den Wert "Aussteller/CA". In diesem sollte die bei der Erstellung des CA-Zertifikats angegebenen Daten zusammengefaßt sein. (Wenn Sie obigem Beispiel gefolgt sind, enthält dieses Feld die Zeichenkette **`CN=server-ca`**.) Der Schlüssel kann nun zum Aufbau einer VPN-Verbindung eingesetzt werden.

56.4. Verbindung

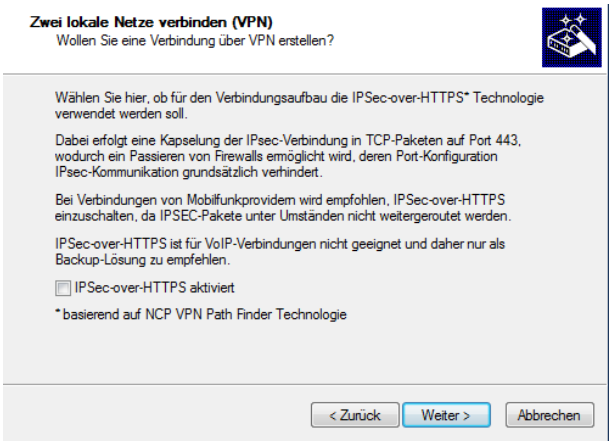
1. Starten Sie den Setup-Assistenten und wählen "Zwei lokale Netze verbinden (VPN)".



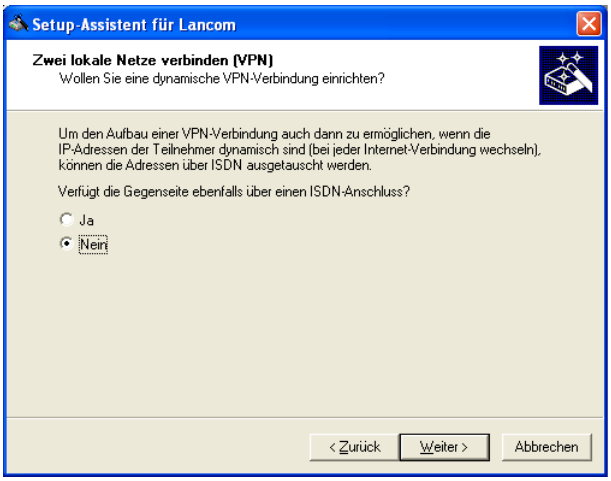
2. Die VPN-Verbindung soll über eine Internet-Verbindung laufen.



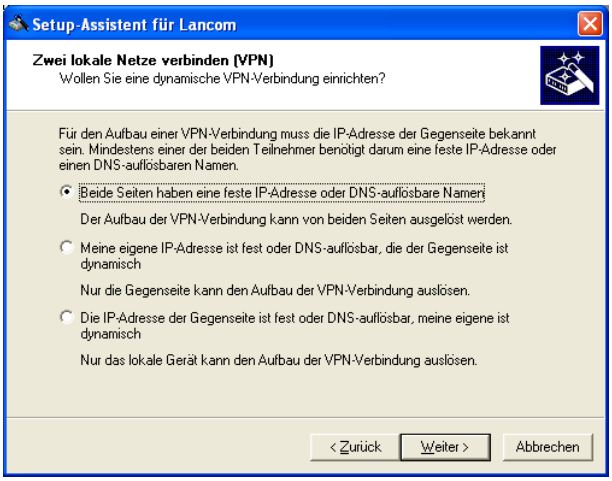
3. Der VPN-Typ muß bei IPSec belassen werden.



4. Verwenden Sie keinen ISDN-Anschluss, denn dafür wird ein Lancom-eigenes Protokoll verwendet.

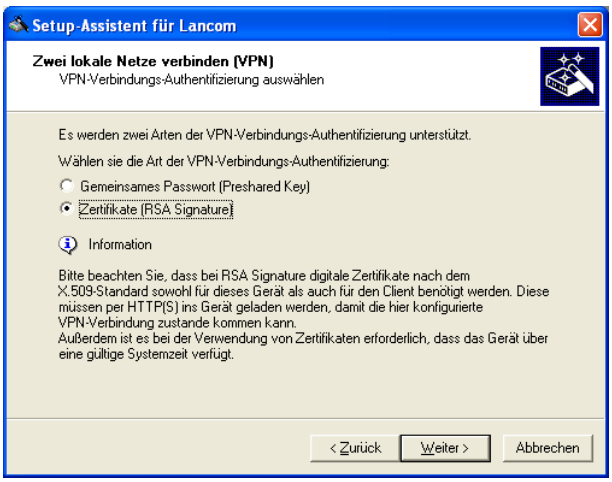


5. Die Verbindung wird über feste IP-Adressen oder Dyndns-Namen hergestellt.

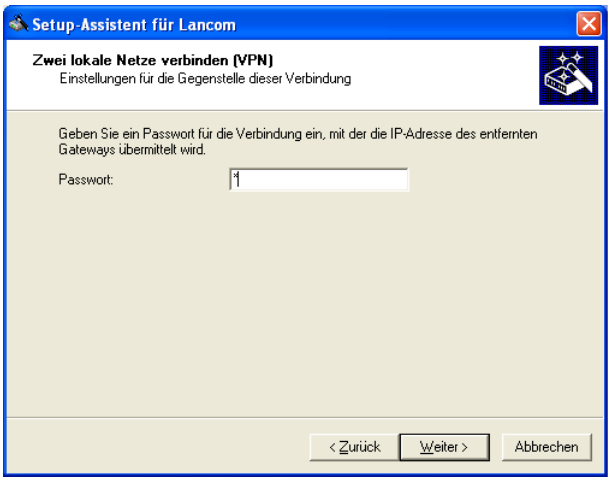


6. Geben Sie der eigenen Seite sowie der Gegenseite einen Namen. Der Name ist für die Verbindung nicht relevant, er muss nur eindeutig sein.

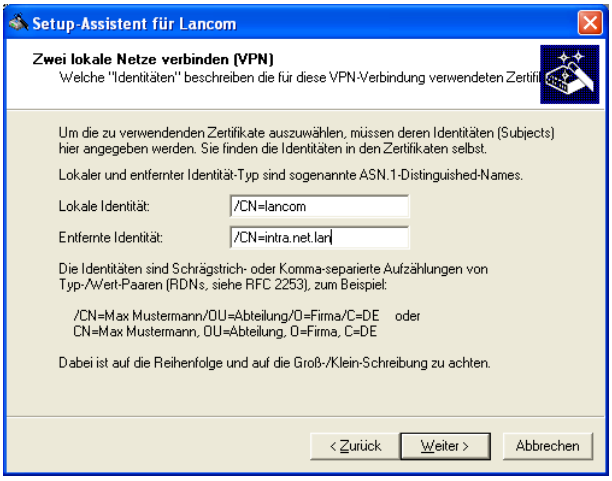
7. Verwenden Sie Zertifikate (RSA) für die Authentifizierung der Verbindung.



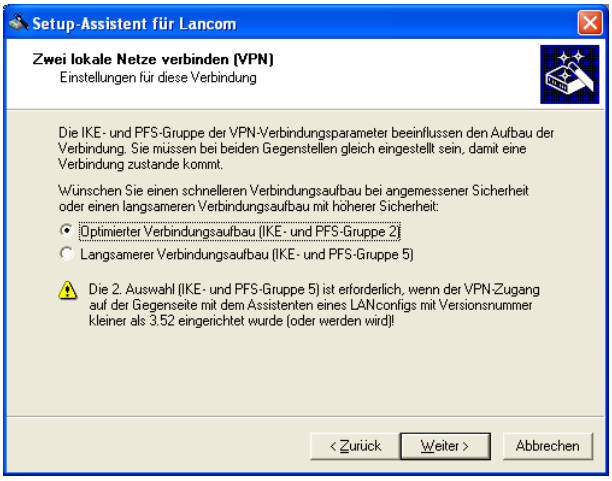
8. Tragen Sie ein beliebiges Passwort ein. Dieses Passwort wird nicht benötigt, es würde nur für das hier nicht verwendete Lancom-eigene ISDN-Protokoll gebraucht werden.



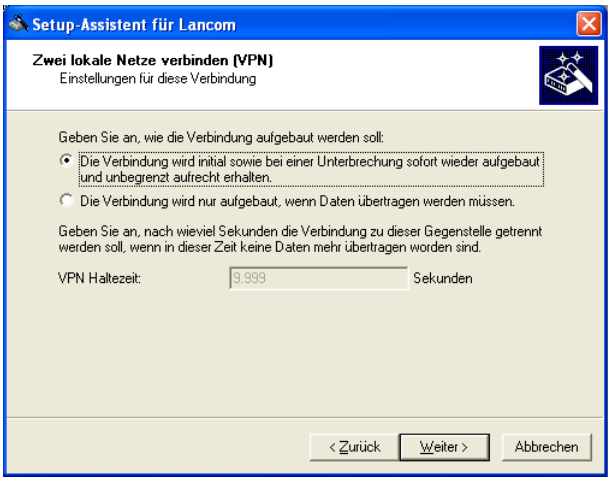
9. Geben Sie die Identität (=Inhaber) der Zertifikate für die eigene (Lancom) und entfernte (Intra2net System) Seite ein. Die Werte für die Distinguished Names finden Sie z.B. auf dem Intra2net System im Menü System > Schlüssel > Eigene Schlüssel bzw. Fremde Schlüssel, jeweils im Feld "Inhaber (Subject)". Die einzelnen Datenblöcke müssen in der umgekehrten Reihenfolge wie im Intra2net System angezeigt eingegeben werden.



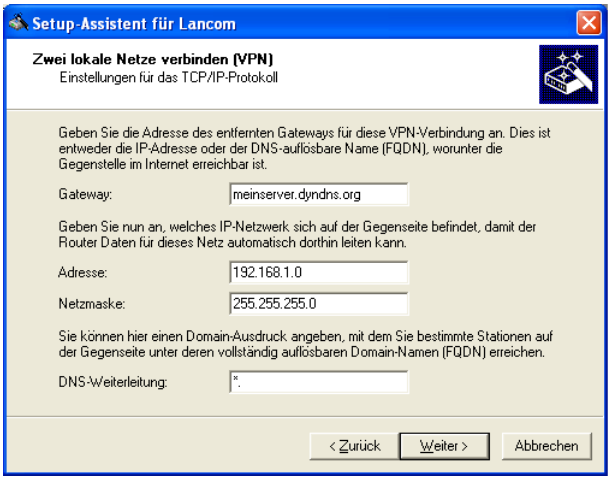
10. Verwenden Sie den optimierten Verbindungsaufbau (IKE- und PFS-Gruppe 2).



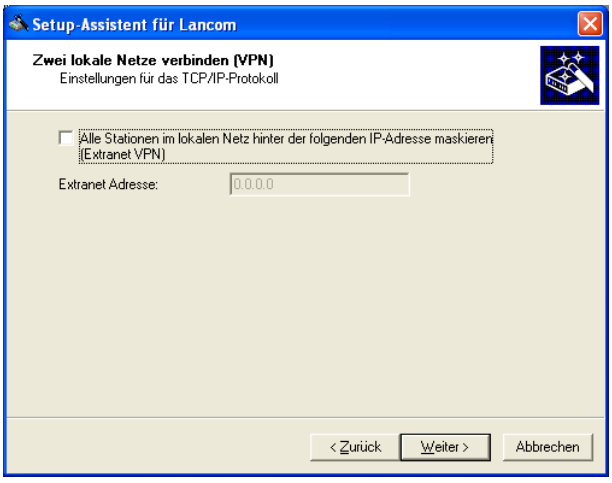
11. Sie können die Verbindung entweder ständig aufgebaut lassen, oder nur bei Bedarf starten. Stellen Sie am besten das Intra2net System auch entsprechend ein.



12. Tragen Sie als "Gateway" die feste IP oder den Dyndns-Namen des Intra2net Systems ein (im Beispiel **`meinserver.dyndns.org`**). Geben Sie dann IP und Netzmaske des Netzes hinter dem Intra2net System ein, im Beispiel **`192.168.1.0 / 255.255.255.0`**.

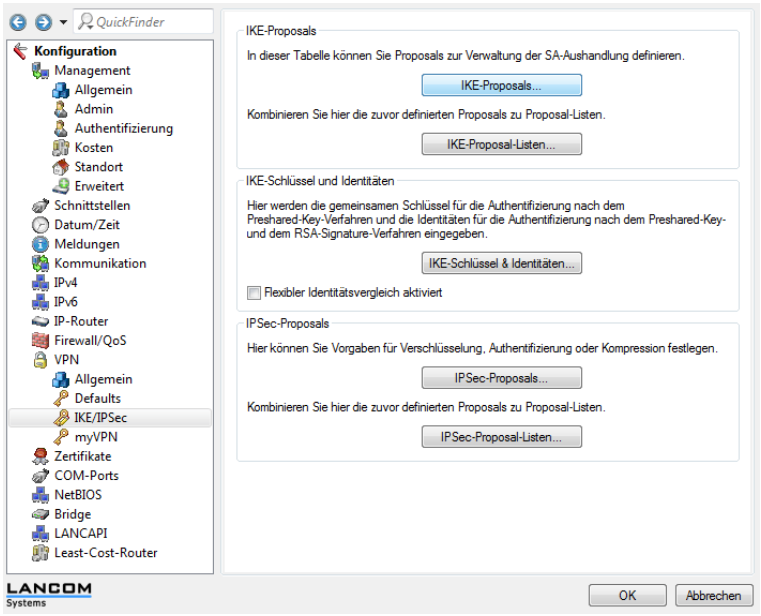


13. Der Lancom-Router kann alle IPs des eigenen Netzes per NAT auf eine einzige Adresse umschreiben. Dies kann unter Umständen helfen, wenn auf beiden Seiten derselbe Netzbereich verwendet wird. Lassen Sie diese Funktion im Zweifel deaktiviert.

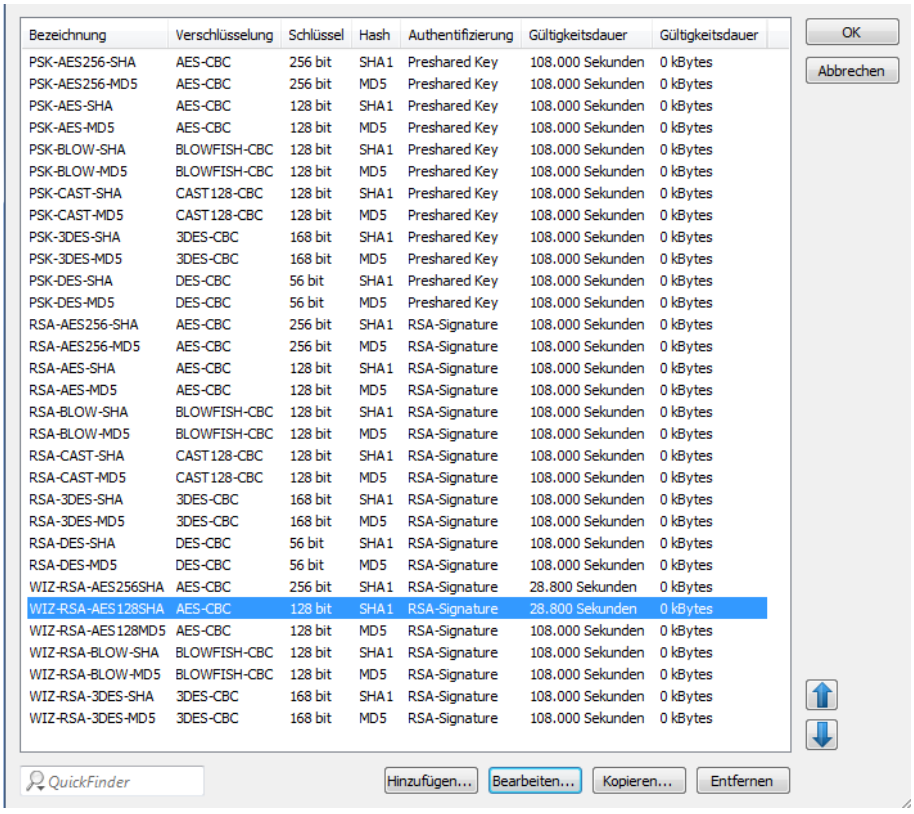


14. Deaktivieren Sie auf jeden Fall die NetBIOS-Option. Sie basiert auf einem proprietärem Lancom-Protokoll und verhindert den Verbindungsaufbau. Sie wird normalerweise nicht mehr benötigt, da moderne Windows-Fileserver CIFS über IP verwenden.

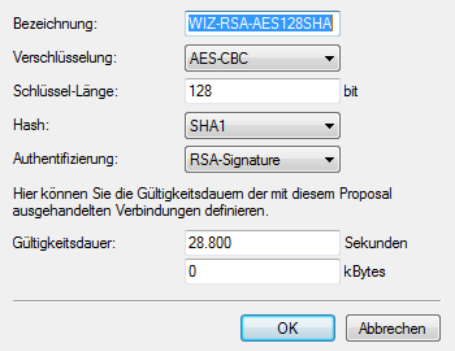
15. Schließen Sie den Assistenten ab und starten die Konfiguration des Routers ohne Assistenten. Wechseln Sie zu den "VPN"-Einstellungen, Reiter "IKE-Param." und klicken auf "IKE-Proposals".



16. Bearbeiten Sie das IKE-Proposal mit dem Namen "WIZ-RSA-AES128SHA".



17. Tragen Sie bei Gültigkeitsdauer einen Wert kleiner als 86400 ein, da dies der Maximalwert ist, den das Intra2net System akzeptiert. Es empfiehlt sich, hier 28800 zu verwenden. Denn das entspricht der Standard-Lebensdauer für IKE/Phase 1 von 480 Minuten im Intra2net System.



56.5. Intra2net System

Auf dem Intra2net System muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Router wird dies im 54. Kapitel, „Anbinden von kompletten Netzen“ beschrieben.

56.6. Zertifikate löschen

Hat ein bisher installiertes Zertifikat die selben Inhaberdaten (ID) wie ein neues Zertifikat, kann es zu Konflikten kommen. Spätestens in diesem Fall muss das bisherige Zertifikat gelöscht werden. VPN-Verbindungen können aus dem Lancom-Router über die Konfigurations-Oberfläche wieder gelöscht werden falls sie nicht mehr benötigt werden. Zertifikate können dagegen 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_add_cas` und `vpn_pkcs12`. Sie können jetzt über den Befehl **`del vpn_add_cas`** z.B. das Zertifikat der Gegenstelle löschen.

57. Kapitel - VPN mit Linux

57.1. Überblick

Um eine VPN-Verbindung mit einer Linux-Gegenstelle aufzubauen, benötigen Sie eines der beiden Programmpakete 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.

57.2. 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 das Intra2net System unter System > Schlüssel > Fremde Schlüssel.

6. Öffnen Sie im Intra2net System 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/intra2netserver.pem`.

57.3. 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 **`intra2netserver`** verwendet.

4. Legen Sie eine Datei mit dem Namen `/etc/ipsec.d/intra2netserver.conf` (bzw. Ihrem Verbindungsnamen) an und öffnen sie in einem Texteditor (z.B. nano oder vi).

5. Die Konfigurationsdatei beginnt mit der Zeile **`conn intra2netserver`** (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 intra2netserver
   auto=start
   keyingtries=0
   type=tunnel
   auth=esp
   authby=rsasig
   ike=aes128-sha-modp1024!
   esp=aes128-sha1!
   pfs=yes
   ikelifetime=480m
   keylife=60m
   rekey=yes
   #
   # left: our side
   left=%defaultroute
   leftid="/C=DE/ST=BW/L=Tuebingen/O=Intra2net/CN=MeinRechnerName"
   leftrsasigkey=%cert
   leftcert=/etc/ipsec.d/cert.pem
   leftsubnet=192.168.10.0/24
   leftfirewall=yes
   #
   # right: intra2net system side
   right=mein-server.dyndns.org
   rightid="/CN=intra.net.lan"
   rightrsasigkey=%cert
   rightcert=/etc/ipsec.d/intra2netserver.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 das Intra2net System). 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 Intra2net Systems vorkommen.
`esp`	Verschlüsselungsalgorithmus für Phase 2. Die verwendete Kombination muss im Verschlüsselungsprofil des Intra2net Systems 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 Intra2net System 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 Intra2net System 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/intra2netserver.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 intra2netserver`** (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`.

57.4. Intra2net System

Auf dem Intra2net System muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Router wird dies im 54. Kapitel, „Anbinden von kompletten Netzen“ beschrieben.

58. Kapitel - Lösen von IP-Adresskonflikten in VPNs durch NAT

58.1. 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 das Intra2net System 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.

58.2. Konfiguration

Für jede VPN-Verbindung können im Menü Dienste > VPN > Verbindungen, Reiter Tunnel individuelle Einstellungen für die Adressumschreibung festgelegt werden.

Lokale IPs umschreiben	Das lokale Netz dieses Intra2net Systems wird für die Gegenseite auf einen anderen IP-Bereich umgeschrieben. Das hier gewählte Netz wird als lokales Netz dieses Intra2net Systems an die Gegenseite übermittelt. Es muss daher auf der Gegenseite als Netz hinter dem Intra2net System eingetragen werden. 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. 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.
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 Intra2net Systems und ist von der Gegenseite aus nicht erkennbar. Der Gegenseite wird beim Verbindungsaufbau ausschließlich das unter "Netz auf Gegenseite" eingestellte Netz übermittelt.
Gegenseiten-IPs bei Internet-zugriff umschreiben	Siehe Abschnitt 46.4.4, „Tunnel konfigurieren“

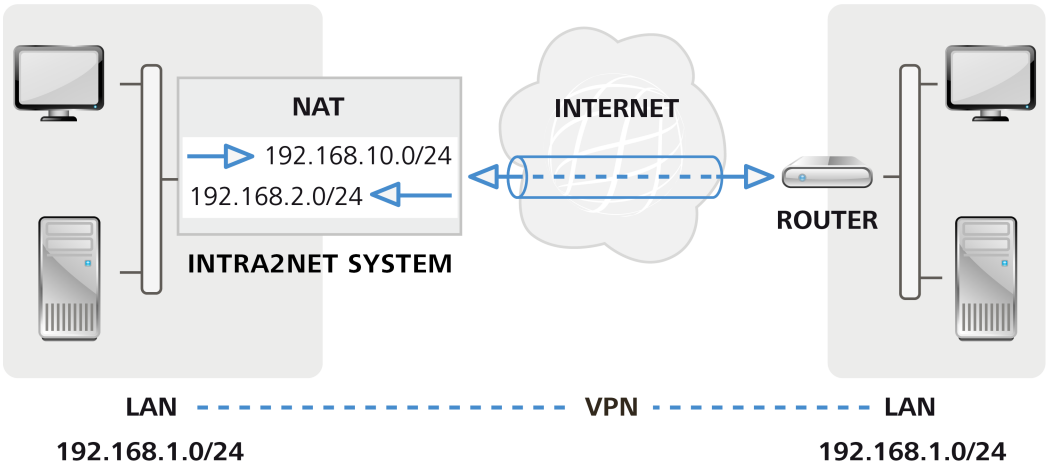
58.3. Gleiche IPs in LAN und auf der Gegenseite

Das lokale Netz des Intra2net Systems und der Gegenseite verwenden einen identischen oder zumindest überlappenden Netzbereich. In diesem Beispiel ist dies 192.168.1.0/24.

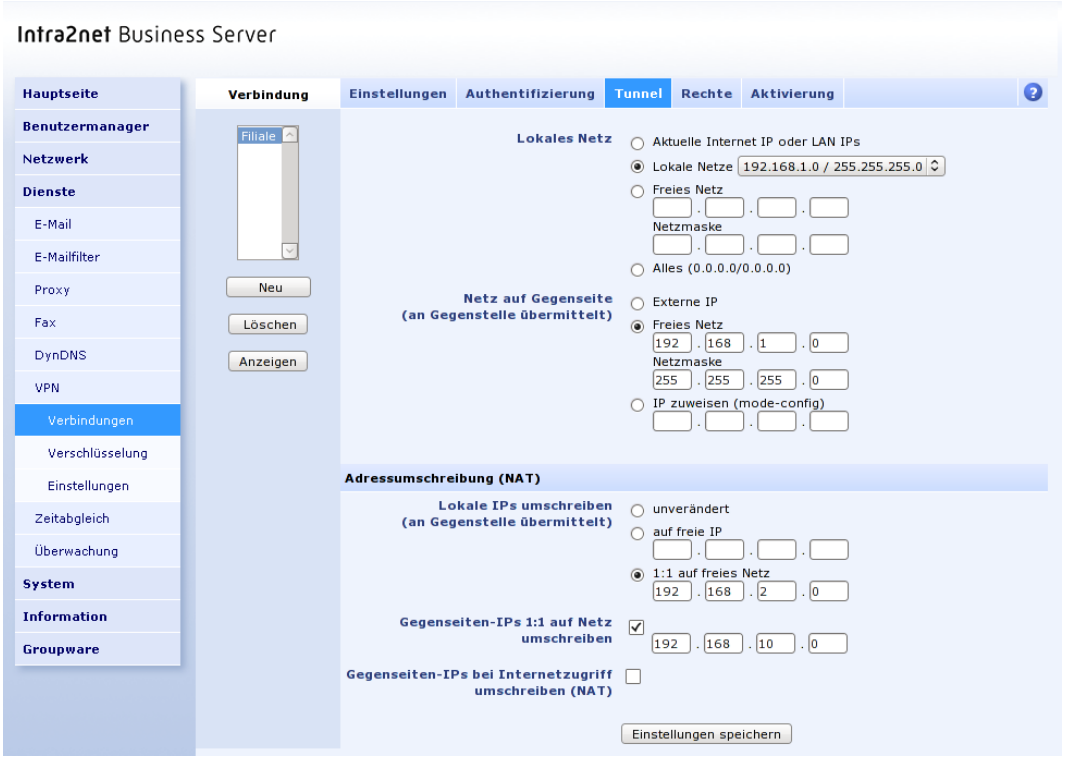
Um den Adresskonflikt zu lösen, wird das lokale Netz der Gegenseite auf 192.168.10.0/24 umgeschrieben. Möchte ein Rechner aus dem LAN des Intra2net Systems also die Gegenseite erreichen, muss er die entsprechende IP im Netz 192.168.10.0/24 ansprechen anstatt 192.168.1.0/24 zu verwenden.

Gleichzeitig ist das LAN des Intra2net Systems für die Gegenseite unter 192.168.2.0/24 zu erreichen.

Beide Adressumschreibungen finden auf dem Intra2net System statt, die Gegenseite bekommt davon nichts mit. Wird auf beiden Seiten des VPNs ein Intra2net System verwendet, darf die Adressumschreibung nur auf einer Seite eingestellt werden.



58.3.1. Umsetzung

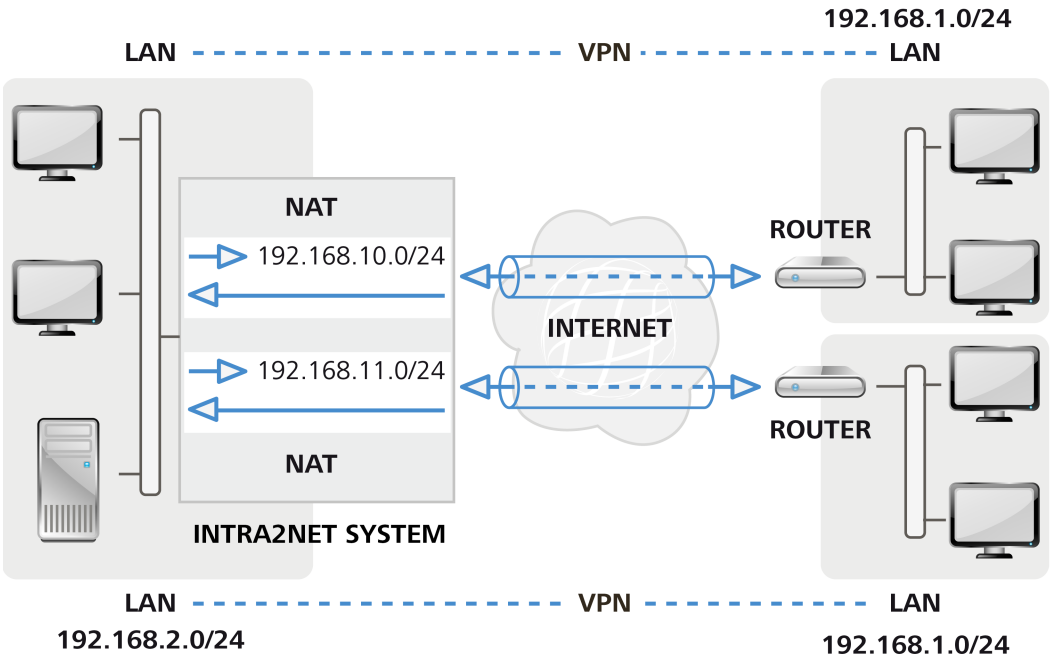


58.4. Mehrere Gegenstellen mit gleichen IPs

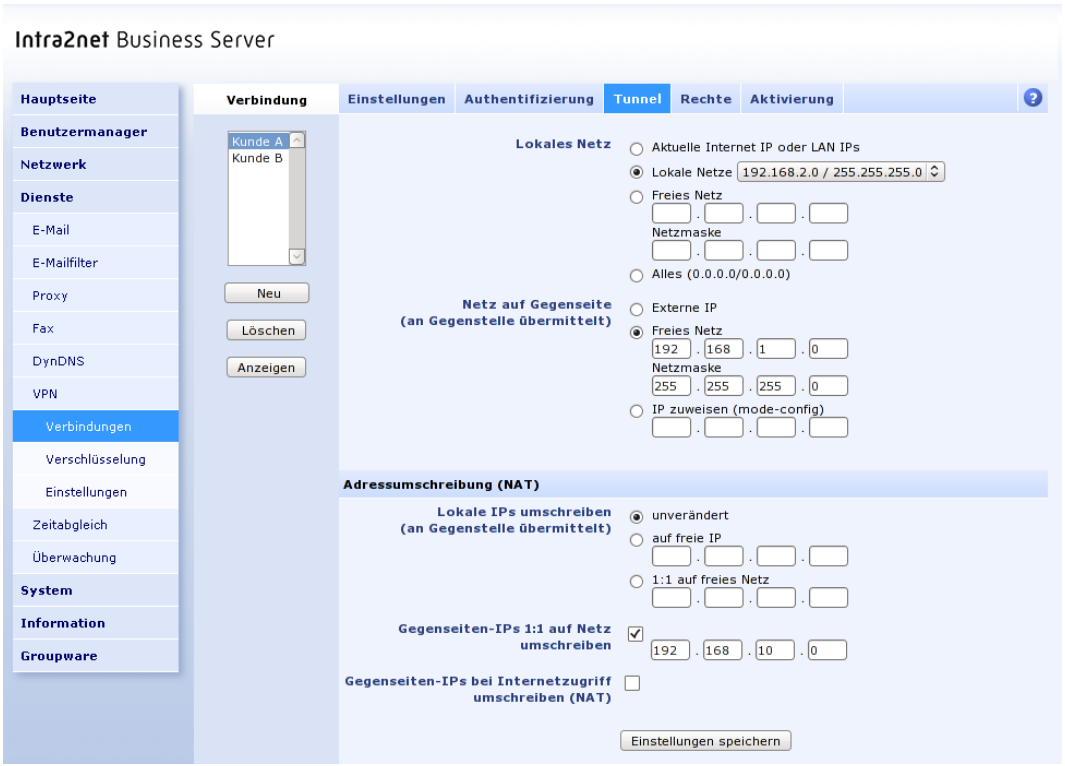
Von einem Intra2net System aus sollen gleichzeitig VPNs zu mehreren Gegenstellen aufgebaut werden. Beispielsweise für Fernwartung von unterschiedlichen Kunden oder Standorten. Mehrere dieser Gegenstellen verwenden das gleiche IP-Netz, in diesem Beispiel 192.168.1.0/24.

Wenn sich das LAN des Intra2net Systems nicht mit einem Netz der Gegenseiten überschneidet, ist es nicht notwendig, die lokalen IPs des Intra2net Systems 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.



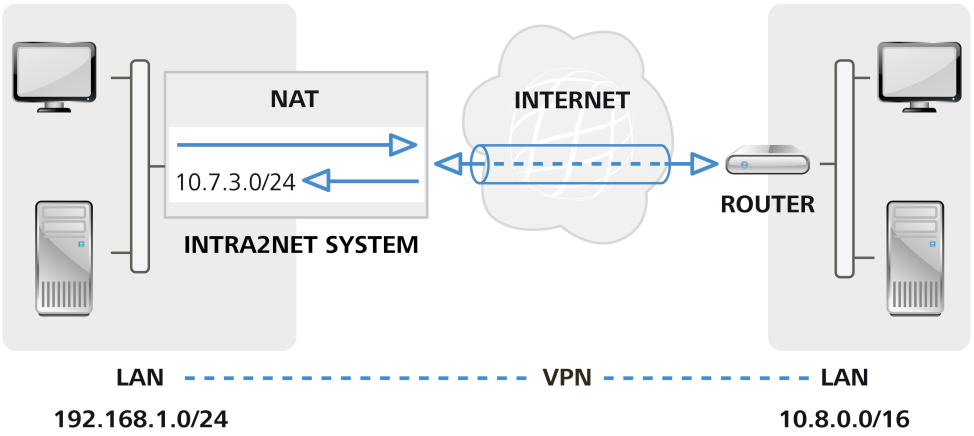
58.4.1. Umsetzung



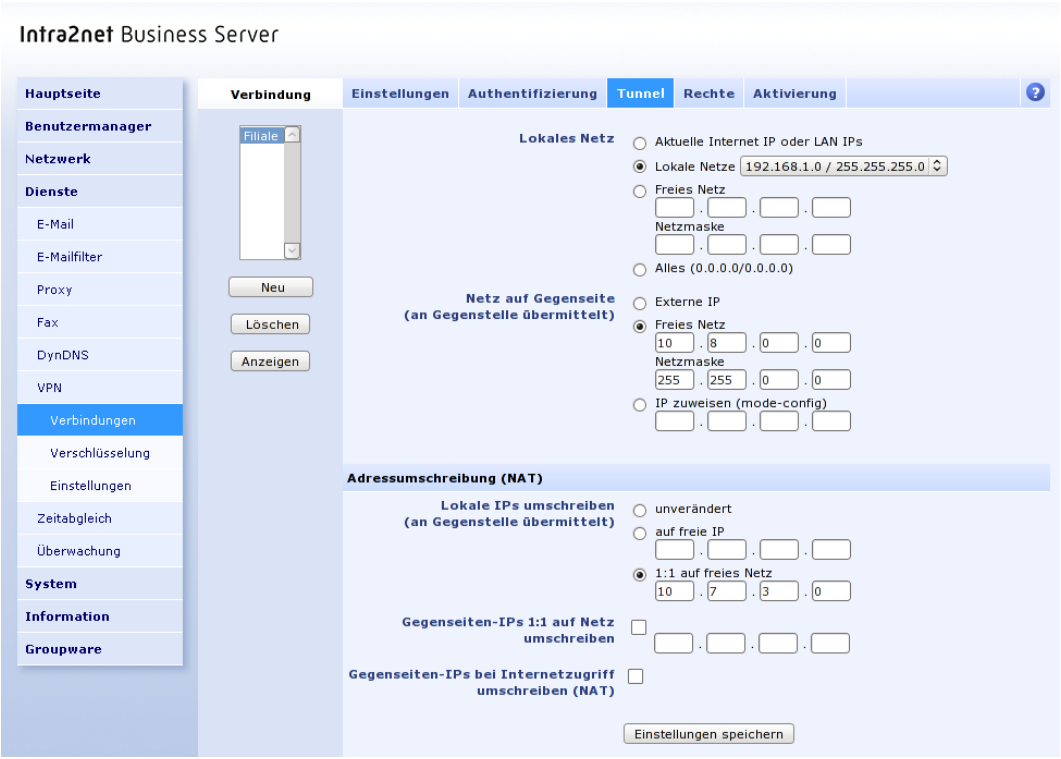
58.5. Lokale IPs festgelegt durch Fernwartungs-Dienstleister

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.



58.5.1. Umsetzung



59. Kapitel - Fehlerdiagnose

59.1. 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 Intra2net System 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.

59.2. Das Protokollformat des Intra2net Systems

Ein Beispiel für eine Zeile aus einer System-Logdatei:

```
Nov  5 10:54:40 intra 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
`intra`	Rechnername des Intra2net Systems
`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 das System bekommt. Liste der Verbindungskennungen zu finden unter „Information > System > VPN“
`192.168.1.200`	IP der Gegenstelle. Wird nur angezeigt bei Verbindungstyp „Dynamische IP“
`responding to ...`	Nachricht

59.3. 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 192.168.1.200:500: received Vendor ID payload [draft-ietf-
    ipsec-nat-t-ike-00]
packet from 192.168.1.200:500: 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 das Intra2net System 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'
```

Das Intra2net System sendet daher eine kurze Fehlerinformation an die Gegenstelle:

```
sending encrypted notification INVALID_KEY_INFORMATION to 192.168.1.200:500
```

Baut das Intra2net System 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.

Versucht die Gegenstelle eine Verbindung mit einem falschen Authentifizierungsverfahren aufzubauen, oder wird von dieser Gegenstellen-IP keine Verbindung erwartet, so wird folgendes protokolliert:

```
initial Main Mode message received on 192.168.1.254:500 but no connection
        has been authorized with policy=PUBKEY
```

Statt "policy=PUBKEY" können auch "policy=PSK" oder "policy=XAUTHRSASIG+XAUTHSERV" vorkommen wenn die Gegenstelle eine entsprechende Authentifizierung gewählt hat. Kontrollieren Sie die eingestellten Authentifizierungsverfahren, die IP der Gegenstelle sowie die Tunnelkonfiguration, da letztere Auswirkungen auf die IPs hat, von denen eine Verbindung erwartet wird.

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 das Intra2net System 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 Intra2net System 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
```

59.4. 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=server-vpn]...192.168.1.200[CN=client1]
```

`192.168.2.0/24`	Netz hinter dem Intra2net System mit dem die Gegenseite die Verbindung aufbauen möchte
`192.168.1.254`	IP des Intra2net Systems die die Verbindung entgegengenommen hat
`[CN=server-vpn]`	IPSec-ID des Intra2net Systems
`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=server-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 Intra2net System 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 einfachem 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 Verbindungsaufbau wird dagegen so protokolliert:

```
IPsec SA established
```

Teil 7. WireGuard VPN

60. Kapitel - WireGuard Grundlagen

60.1. Das WireGuard Protokoll

WireGuard ist ein VPN-Protokoll, welches mit dem Ziel entwickelt wurde die Komplexität von VPNs deutlich zu reduzieren. Diese Vereinfachung geht so weit, dass auch auf Funktionen verzichtet wird, die andere VPN-Protokolle bieten.

Ein wichtiger Teil dabei ist, dass nur ein Satz an im Protokoll festgelegten kryptographischen Algorithmen verwendet wird. Es findet daher keinerlei Aushandlung von Algorithmen beim Verbindungsaufbau statt. Dies vereinfacht den Verbindungsaufbau und verhindert Downgrade-Angriffe. Es wird X25519 ECDH für den Schlüsselaustausch, ChaCha20 für die Verschlüsselung der Nutzdaten und Poly1305 für die Authentifizierung der Nutzdaten verwendet.

Da X25519 ECDH evtl. in Zukunft durch Quantencomputer erfolgreich angegriffen werden könnte, verfügt WireGuard über eine zusätzliche Schutzebene. Hierfür wird die Schlüsselaushandlung noch mit einem auf beiden Seiten identisch hinterlegten Schlüssel (Pre-Shared Key) zusätzlich symmetrisch verschlüsselt. Quantencomputer bieten nach heutigem Wissensstand keinen Vorteil gegen die hier eingesetzte symmetrische Verschlüsselung.

Die Verschlüsselung der Nutzdaten per ChaCha20-Poly1305 ist weniger rechenintensiv als das bei anderen Protokollen oft verwendete AES-GCM. Daher erreicht WireGuard oft einen höheren Datendurchsatz als z.B. IPSec mit AES. Da allerdings viele CPUs über eine Beschleunigung für AES in Hardware verfügen, nicht aber für ChaCha20-Poly1305, gilt dies nicht in allen Fällen.

Der Aufbau einer WireGuard-Verbindung ist im Vergleich zu anderen VPN-Protokollen besonders schlank und schnell. Es muss nur jeweils ein UDP-Paket zur Gegenseite und von dieser zurück gesendet werden. Dies ist der sog. Handshake. In ihm wird die komplette Authentifizierung und das Aushandeln von Sitzungsschlüsseln für die Nutzdaten umgesetzt.

Die UDP-Pakete für den Handshake sind kleiner als 1259 Bytes und kommen daher ohne Fragmentierung durch die allermeisten Internetanbindungen. Da einige Router und NAT-Implementationen Schwierigkeiten mit fragmentierten UDP-Paketen haben, ist der Verzicht auf UDP-Fragmentierung ein wichtiger Vorteil.

Der Handshake wird nur ausgeführt, wenn tatsächlich Nutzdaten übertragen werden müssen oder wenn in der Konfiguration das sog. Keepalive aktiviert ist. Das Keepalive hält die Verbindung offen um z.B. mit NAT-Routern im Verbindungsweg umgehen zu können. Der Handshake wird, wenn ständig Nutzdaten übertragen werden, in etwa alle 2 Minuten gemacht. Das ist wesentlich häufiger als es für den Verbindungsaufbau bei anderen VPN-Protokollen wie z.B. IPSec üblich ist.

Da der Verbindungsaufbau so schnell geht, kann WireGuard auf ein komplexeres Management des Verbindungsstatus verzichten. WireGuard merkt sich nur, ob der letzte erfolgreiche Handshake innerhalb des erlaubten Zeitrahmens stattgefunden hat und startet bei anstehendem Datentransfer rechtzeitig vorher einen neuen.

Sowohl die Handshakes als auch die Nutzdaten werden als UDP-Pakete übertragen. Die UDP-Portnummern werden dabei für beides gemeinsam verwendet. Die UDP-Portnummern sind grundsätzlich frei wählbar und können auf beiden Gegenseiten unterschiedlich sein. Die Portnummer 51820 findet man oft für WireGuard verwendet. Intra2net hat hier aber

Konflikte sowohl mit anderen WireGuard nutzenden Routern als auch mit Quellports für ausgehende Pakete anderer Verbindungen beobachtet und empfiehlt daher Port 800 für VPN-Router und -Firewalls sowie zufällige Portnummern oberhalb von 1024 für VPN-Clients.

WireGuard sieht keine Festlegung der Verbindung auf eine bestimmte Gegenstellen-IP vor. Es kann eine IP oder ein DNS-Hostname hinterlegt werden, zu der die Verbindung grundsätzlich neu aufgebaut wird. Wenn sich die Gegenstelle mit gültigen Schlüsseln aber von einer anderen IP aus per Handshake meldet, wird das akzeptiert und die Verbindung läuft ab diesem Moment mit dieser anderen IP. Dies ist hilfreich u.a. für mobile Clients, die z.B. zwischen WLAN und Mobilfunk wechseln, oder für das Umschalten auf eine Fallback-Internetleitung.

Der WireGuard-Handshake tauscht keine Informationen über die zu verbindenden IP-Netze aus. In der Konfiguration wird lediglich hinterlegt, welche Quelladressen von einer bestimmten Gegenstelle aus genutzt werden dürfen (*AllowedIPs*). Jede Seite blockiert eingehende IP-Pakete, die nicht zu dieser Konfiguration passen. Dies ist aber unabhängig von den Handshakes und man kann von erfolgreichen Handshakes nicht auf eine korrekte Konfiguration der IP-Netze schließen.

Für die Übertragung von Konfigurationsdaten und Schlüsseln hat sich bei WireGuard ein gemeinsames Dateiformat etabliert ("wg-quick"-Format) und kann herstellerübergreifend genutzt werden. Es kann auch als QR-Code dargestellt und mit der Kamera von Mobilgeräten fotografiert werden. Auf diese Weise kann die VPN-Konfiguration besonders leicht und sicher auf Mobilgeräte übertragen werden.

60.2. Anpassungen durch Intra2net

Intra2net hat einige Anpassungen an WireGuard vorgenommen, um die Funktion zu verbessern. Diese Anpassungen betreffen nicht das Protokoll auf der Leitung, Intra2net Systeme sind daher mit anderen WireGuard-Gegenstellen kompatibel.

Verbindungsstatus: Für jede WireGuard-Verbindung wird ein klarer Verbindungsstatus geführt und protokolliert. Ob eine Verbindung on- oder offline ist wird auf der Hauptseite angezeigt. Zu Dokumentations- und Prüfzwecken lässt sich jeder Verbindungsaufbau in den Systemmeldungen nachvollziehen.

Um den Verbindungsstatus verlässlich erkennen zu können, sollte die Keepalive-Funktion aktiviert sein. Wenn für eine Verbindung nach spätestens 180 Sekunden zzgl. der eingestellten Keepalive-Zeit kein erfolgreicher Handshake zustande kam, wird sie als offline geführt.

Detaillierte Protokolle: Es wird nicht nur der Statuswechsel Online/Offline protokolliert, sondern u.a. auch Aufbauversuche mit falschen Schlüsseln, nicht antwortende Gegenstellen, Wechsel von IP-Adressen oder Portnummern und Pakete von falschen IP-Adressen innerhalb des Tunnels. Diese Daten sind sowohl für die Fehlersuche als auch für Dokumentations- und Prüfzwecke hilfreich.

Verbindungsaufbau unabhängig von Keepalive: In der normalen Implementation von WireGuard bedeutet ein konfiguriertes Keepalive, dass eine Verbindung immer versucht wird aufzubauen. Bei Verbindungen zu VPN-Clients ist zwar Keepalive sinnvoll, aber in den Zeiten in denen der Client nicht läuft, stören die ständigen Verbindungsaufbauversuche und ihre Fehlermeldungen. Daher trennt das Intra2net System die grundsätzliche Aktivierung einer Verbindung von dem Keepalive, sobald die Verbindung einmal Online ist.

Kontinuierliche DNS-Auflösung: Konfiguriert man als WireGuard-Gegenstelle einen DNS-Hostnamen, so aktualisiert das Intra2net System jede Minute dessen DNS-Auflösung. Dadurch können auch dynamische IPs mit DynDNS oder Fallback-Internetleitungen problemlos als Gegenstellen verwendet werden. Dennoch wird beim Wechsel der DNS-Auflösung eine bestehende WireGuard-Verbindung nicht unterbrochen. Die neu aufgelöste IP wird nur für einen neuen Verbindungsaufbau verwendet, wenn Handshakes zur aktuell verwendeten IP-Adresse erfolglos bleiben und daher die Verbindung offline geht.

Festlegung lokaler IP-Netze: WireGuard sieht an sich nur die Konfiguration der Netze der Gegenseite vor (*AllowedIPs*, siehe oben). Dies erschwert die Konfiguration feingranularer Zugriffsrechte, da hier dann für die lokalen Netze zusätzliche Firewall-Regellisten manuell konfiguriert werden müssten. Daher sieht das Intra2net System vor, dass sowohl für die lokale Seite als auch für die Gegenseite die beteiligten IP-Netze konfiguriert werden. Die Firewall beschränkt dann automatisch den Zugriff auf die konfigurierten Netze. Außerdem ermöglichen diese Daten die Vorbereitung vollständiger WireGuard-Konfigurationsdateien für die Gegenseite.

Es ist nicht notwendig wie bei IPSec jedes einzelne Paar von Quell- und Zielnetz separat zu konfigurieren. Das einfache Auflisten aller lokalen IP-Netze und der der Gegenseite reicht aus um alle diese Netze untereinander zu verbinden.

60.3. Vergleich mit IPSec

Bei WireGuard sind die verwendeten kryptographischen Algorithmen im Protokoll fest verankert, bei IPSec werden diese dagegen bei jedem Verbindungsaufbau zwischen den Gegenstellen dynamisch ausgehandelt. WireGuard ist daher einfacher und schneller, IPSec erlaubt aber eine schrittweise Evolution und Anpassung der Kryptographie ohne das Protokoll grundsätzlich verändern zu müssen. Auch ältere Gegenstellen können bei IPSec ohne Änderung weiterhin angebunden bleiben und so ist eine langsame, bruchfreie Migration möglich. Sollten die bei WireGuard festgelegten kryptographischen Algorithmen eines Tages nicht mehr als ausreichend angesehen werden, wäre ein harter Bruch und ein grundlegend neues und inkompatibles Protokoll nötig.

IPSec ist für den Verbindungsaufbau auf UDP-Port 500 festgelegt. Dieser Port kann aber flexibel für alle Verbindungen, Verbindungs- und Portokollvarianten und mehrere eigene Schlüssel verwendet werden. Das vereinfacht z.B. das Einrichten von Portforwardings. Bei WireGuard wird pro eigenem privatem Schlüssel eine separate Portnummer benötigt. Diese Portnummer kann aber frei gewählt werden.

Durch das Aushandeln der Protokollvarianten und Algorithmen benötigt IPSec den Austausch mehrerer Pakete für einen Verbindungsaufbau. Dieser ist daher langsamer und benötigt größere UDP-Pakete die dann u.U. fragmentiert werden müssen. WireGuard kommt mit einem Paket hin und zurück für den Verbindungsaufbau aus und dieses Paket ist klein genug, sodass es normalerweise nicht fragmentiert werden muss. Dies erhöht die Geschwindigkeit und Funktionsfähigkeit an eingeschränkten Internetzugängen bei WireGuard.

Da bei IPSec ein eindeutiger Verbindungsaufbau am Anfang stattfindet und dieser normalerweise nur im Zeitraum mehrerer Stunden wiederholt werden muss, können die für die Authentifizierung nötigen privaten Schlüssel auf externe Geräte wie Smartcards oder USB-Tokens ausgelagert werden und müssen niemals im Arbeitsspeicher des Client-PCs vorliegen. Dies ermöglicht eine volle Mehr-Faktor-Authentifizierung mit echtem Ausleseschutz der privaten Schlüssel. Auch wenn der private Schlüssel auf dem Client-PC abgelegt wird,

ist es bei IPSec-Clients üblich diesen mit einem speziellen Kennwort zu verschlüsseln und dieses vor jedem Verbindungsaufbau abzufragen. Für die Übertragung von privaten Schlüsseln an Clients kommt bei den meisten Clients PKCS#12 zum Einsatz, welches den Schlüssel für die Übertragung mit einem Passwort schützt.

Bei WireGuard findet der Handshake mit Authentifizierung etwa alle 2 Minuten statt. Es ist nicht vorgesehen oder realistisch, die privaten Schlüssel dafür auf externe Hardware auszulagern. Das etablierte Austauschformat für WireGuard-Konfigurationen ("wg-quick Format") sieht es nicht vor den privaten Schlüssel mit einem Passwort zu sichern. Die meisten Clients für WireGuard sehen auch nicht vor, dies nachträglich für den lokalen Speicher der Schlüssel hinzuzufügen und verlassen sich hierfür auf evtl. vom Betriebssystem bereitgestellte Funktionen.

IPSec nutzt standardisierte X.509-Zertifikate und kann damit leicht an vorhandene Zertifizierungsstellen und -infrastruktur angebunden werden. WireGuard verwendet sein eigenes Schlüsselformat, welches ausschließlich für WireGuard genutzt wird.

Die bei IPSec verwendeten X.509-Zertifikate haben ein Ablaufdatum, das bei der Erstellung festgelegt wird. Hierüber lässt sich eine regelmäßige Überprüfung der Berechtigung und der Nutzung angemessenser Kryptographiestandards von vorneherein festlegen und sicherstellen. Ein regelmäßiger Wechsel der Schlüssel dämmt den Schaden bei nicht sofort erkanntem Schlüsselverlust oder der Zugriff durch nicht mehr berechtigte Personen ein. Die bei WireGuard verwendeten Schlüssel haben kein Ablaufdatum und der Nutzer muss eigene Prozesse implementieren, um sicherzustellen, dass die genannten Punkte im richtigen Zeitintervall geprüft werden. Das Intra2net System zeigt bei WireGuard-Schlüsseln den Zeitpunkt an, zu dem ein Schlüssel erstellt oder importiert wurde, um solche Prozesse zu unterstützen.

Bei IPSec werden die zu verbindenden Quell- und Zielnetze am Anfang beim Verbindungsaufbau zwischen den Gegenseiten abgeglichen. Eine Verbindung kommt nur zustande, wenn diese exakt identisch sind. Konfigurationsfehler werden daher direkt beim Verbindungsaufbau ersichtlich und es wird auf einer zur Firewall zusätzlichen Ebene sichergestellt, dass nur die gewünschten Netze miteinander verbunden sind. Da aber jedes Paar an Quell- und Zielnetz einzeln konfiguriert werden muss, kann die Konfiguration aufwendiger werden.

Bei WireGuard sind die IP-Netze nicht Teil des Verbindungsaufbaus und werden zwischen den Gegenseiten nicht abgeglichen. Ein Konfigurationsfehler an dieser Stelle fällt also nicht bereits beim Verbindungsaufbau auf und muss evtl. erst durch den Vergleich der Einstellungen und Protokolle von beiden Seiten identifiziert werden. Es ist aber einfacher die Konfiguration zu erstellen und anzupassen, da keine Paare an Quell- und Zielnetzen festgelegt werden müssen.

Bei IPSec gibt es kein etabliertes Dateiformat für den Austausch von Konfigurationsdaten. Für die Authentifizierung kommen die gängigen Formate PEM und PKCS#12 zum Einsatz. Die von unterschiedlichen Gegenstellen geforderten Details der Zertifikate wie z.B. Subject-CN vs. SubjectAlternativeName, Vertrauenskette oder CRL unterscheiden sich allerdings. Dies kompliziert die Konfiguration von IPSec-Verbindungen zwischen verschiedenen Gegenstellen und fordert detaillierte Kenntnis der jeweiligen Produkte von den Administratoren. Das fehlende gemeinsame Austauschformat für Konfigurationsdaten erschwert die Kommunikation, vor allem wenn die Gegenseiten von verschiedenen Organisationen betrieben und betreut werden.

Bei WireGuard hat sich ein herstellerübergreifendes Format für den Austausch der Konfigurationsdaten und Schlüssel etabliert. Dies kann von den meisten WireGuard Clients zumindest importiert werden und vereinfacht die Konfiguration wesentlich.

Bei IPSec wird in den meisten Fällen AES zur Verschlüsselung der Nutzdaten verwendet. Dies ist zwar rechenintensiver, wird aber bei vielen CPU-Modellen mit spezieller Hardwarebeschleunigung unterstützt. Das ChaCha20-Poly1305 von WireGuard ist einfacher, wird aber rein in Software umgesetzt. Welches der beiden Verfahren letztlich den höheren Datendurchsatz liefert, ist daher stark von der konkret verwendeten CPU, Mainboard und Netzwerkkarten abhängig und ohne konkrete Tests schwer vorherzusagen.

IPSec ist seit vielen Jahren am Markt etabliert und hat daher eine breite, herstellerübergreifende und untereinander kompatible Unterstützung bei Router- und Firewallprodukten. WireGuard ist ein neuerer VPN-Standard und ist daher, insbesondere bei Firewallprodukten, noch nicht so weit verbreitet. Dort wo WireGuard unterstützt wird, wurden von uns aber noch keine Kompatibilitätsprobleme zwischen verschiedenen Implementationen beobachtet. Hier ist die Festlegung auf einen Kryptographiestandard hilfreich.

Für WireGuard werden für alle gängigen Plattformen kostenlose Clientprogramme angeboten. Bei IPSec sind für einige Plattformen nur kostenpflichtige Clientprogramme empfehlenswert.

Als Fazit ergibt sich daraus, dass beide Standards ihre individuellen Stärken und Daseinsberechtigung haben. Es sollte für jeden Einsatzzweck individuell entschieden werden, welches der beiden Protokolle besser passt.

61. Kapitel - Vorbereiten der Konfiguration auf dem Intra2net System

Im folgenden finden Sie die Schritte beschrieben, die Sie einmalig umsetzen müssen bevor Sie WireGuard nutzen können.

61.1. Eigener Schlüssel und Schnittstelle

WireGuard benötigt auf jeder beteiligten Gegenstelle ein Paar aus privatem und öffentlichem Schlüssel. Dieses wird dann mit einer virtuellen WireGuard-Schnittstelle verknüpft.

1. Gehen Sie in das Menü "System > Schlüssel > Eigene Schlüssel" und legen einen neuen Schlüssel vom Typ "WireGuard "Curve 25519" privater Schlüssel" an.

2. Gehen Sie in das Menü "Dienste > VPN > WireGuard Interfaces" und legen eine neue virtuelle Schnittstelle an. Weisen Sie dabei den eben erzeugten eigenen Schlüssel zu.

Jedes WireGuard-Interface benötigt eine eigene UDP-Portnummer über die es von außen angesprochen werden kann. Diese Portnummern können grundsätzlich frei gewählt werden. Es wird aber empfohlen dem Intra2net System Portnummern von 800 an aufsteigend zuzuweisen, denn mit der bei anderen Systemen oft verwendeten Portnummer 51820 wurden Konflikte mit anderen WireGuard-fähigen Routern sowie mit Quellports für andere ausgehende UDP-Verbindungen wie z.B. DNS beobachtet.

Jedes WireGuard-Interface benötigt eine IP-Adresse um kommunizieren zu können. Das Intra2net System kann dabei die IP-Adressen anderer Schnittstellen wiederverwenden, um mögliche IP-Konflikte mit anderen Netzen zu vermeiden. Wählen Sie dafür die Schnittstelle, mit der hinterher die meisten VPN-Gegenstellen verbunden werden. Also z.B. das primäre lokale Netz.

Auch die Schnittstellen deren IP hier nicht mitgenutzt werden, können problemlos über WireGuard verbunden werden. Vom Intra2net System selbst ausgehende und in die VPN-Verbindung hinein laufende Verbindungen verwenden diese IP aber als Quelladresse. Damit diese Verbindungen funktionieren können, muss die Quelladresse daher von der VPN-Gegenseite akzeptiert werden. Wenn sowieso bereits eine Verbindung für das Netz dieser IP konfiguriert wurde, sind keine weiteren Schritte nötig.



Hinweis

Es wird ausdrücklich empfohlen nur ein einziges WireGuard-Interface für alle VPN-Verbindungen gemeinsam anzulegen.

Sie können zwar problemlos mehrere WireGuard-Interfaces anlegen, diese belegen allerdings im System begrenzte Ressourcen. Daher sollte dies nur bei wirklichem Bedarf gemacht und kritisch hinterfragt werden.

61.2. Externe Adresse und Firewall

1. Das Intra2net System sollte für die VPN-Clients über einen DNS-Namen im Internet adressierbar sein.

   Hat das Intra2net System eine feste IP, richten Sie für diese einen DNS-Eintrag in der eigenen offiziellen Domain ein. Das System ist dann unter einem Namen wie z.B. **`intra.kundenname.de`** oder **`mail.example.com`** erreichbar. Dies kann normalerweise

beim Webspace-Provider, der die Domain verwaltet, kostenlos und zeitnah eingerichtet werden.

Bekommt das Intra2net System bei jeder Interneteinwahl eine andere IP zugewiesen, muss zur Adressierung ein DynDNS-Dienst eingerichtet werden. Siehe hierfür Abschnitt 11.13, „DynDNS“.

Es ist zwar möglich für WireGuard eine feste IP direkt und ohne DNS-Eintrag zu verwenden, der DNS-Eintrag wird aber eindeutig empfohlen. Denn eine Änderung der IP bei Provider- oder Vertragswechsel wäre sonst aufwendig. Außerdem benötigen andere, auf TLS basierende, Dienste des Intra2net Systems ein Zertifikat, welches Zertifizierungsstellen nur auf DNS-Hostnamen ausstellen. Dieser kann dann für das VPN mitgenutzt werden.

2. Gehen Sie in das Menü "Netzwerk > DNS > Einstellungen" und hinterlegen diesen extern erreichbaren DNS-Namen im Feld "Vollständiger Rechnername für Verbindungen aus dem Internet".

3. Prüfen Sie, wie das Intra2net System 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 Intra2net System 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 den UDP-Port des WireGuard-Interface (siehe Abschnitt 61.1, „Eigener Schlüssel und Schnittstelle“) auf die IP des Intra2net Systems konfiguriert werden.

4. 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 "VPN-Verbindungen" aktiviert sein. Wird eine vollständige Firewall-Regelliste verwendet, muss der Zugriff auf den vordefinierten Dienst "WireGuard-Interfaces" erlaubt sein.

61.3. Standardeinstellungen für neue Verbindungen

Im Menü "Dienste > VPN > Einstellungen" können Sie die Standardeinstellungen für neu erstellte VPN-Verbindungen festlegen. Die dort hinterlegten Einstellungen gelten sowohl für IPSec- als auch WireGuard-Verbindungen.

Bei der Server-Adresse wird empfohlen, den vollständigen Rechnername für Verbindungen aus dem Internet zu verwenden.

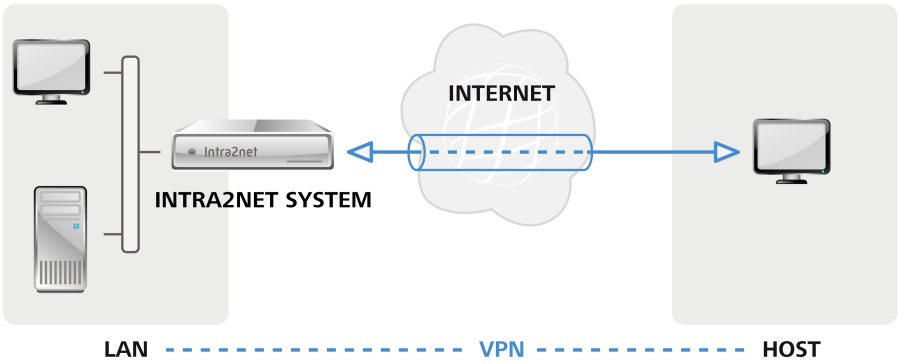
Wählen Sie eine Firewallregelliste, die den für VPN-Clients üblicherweise gewünschten Zugriff ins lokale Netz erlaubt.

Jeder VPN-Client bekommt für die VPN-Verbindung eine individuelle, virtuelle IP zugewiesen. Diese muss außerhalb aller lokalen Netze, Routings und anderen VPN-Verbindungen liegen. Tragen Sie unter "Basis-IP-Adresse für einzelne Endgeräte" die IP für den ersten VPN-Client ein. Alle weiteren VPN-Clients erhalten fortlaufende IPs.

62. Kapitel - Anbinden von einzelnen PCs

62.1. Konzept

Um einen einzelnen Rechner mit dem Firmennetz zu verbinden, kann man eine WireGuard-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 Intra2net System 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.

Für die meisten unterstützten Clients kann das Intra2net System automatisch passende Konfigurationsdateien vorbereiten, die im Client nur noch importiert werden müssen. Eine manuelle Konfiguration ist aber auch immer möglich.

62.2. Automatische Konfiguration für Clients auf dem Intra2net System

Für die meisten VPN-Clientprogramme kann das Intra2net System aus der VPN-Konfiguration auf dem Intra2net System direkt fertige Konfigurationsdateien erzeugen. Diese müssen auf dem Client nur noch importiert werden. Gehen Sie dafür wie folgt vor:

1. Stellen Sie sicher dass die vorbereitenden Schritte alle wie im 61. Kapitel, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben durchgeführt wurden.

2. Gehen Sie in das Menü "Dienste > VPN > Verbindungen" und legen eine neue Verbindung an. Wählen Sie den Typ "WireGuard: Einzelnes Endgerät".

3. Geben Sie der Verbindung einen aussagekräftigen Namen, z.B. den Namen des Mitarbeiters oder Geräts, welches sich verbinden soll. Hat ein Mitarbeiter mehrere Geräte, die VPN-Verbindungen aufbauen können sollen, benötigen Sie für jedes Gerät eine eigene Verbindungkonfiguration.

4. Wählen Sie die lokalen Netze, in die der VPN-Client die Verbindung aufbauen soll.

Sie haben hier die Wahl ob nur die Pakete in definierte Netze durch den VPN-Tunnel laufen, oder ob jegliche Verbindungen vom Client, in die lokalen Netze und das Internet, durch den VPN-Tunnel und das Intra2net System laufen sollen. Wählen Sie für Letzteres bei "Lokale Netze" die Option "Alles (0.0.0.0/0.0.0.0)", für alle anderen Fälle die gewünschten Netze.

5. Anschließend wird automatisch ein Schlüssel für den Client, die Verbindungskonfiguration und die passende Konfigurationsdatei für den Client erstellt. Sie können die Konfigurationsdatei für den Client entweder als Datei herunterladen und zum Client übertragen oder den angezeigten QR-Code mit dem Client fotografieren.

Bei Bedarf können Sie die Konfiguration für den Client auch später über den "Download"-Link erneut exportieren bzw. den QR-Code anzeigen.



Achtung

Die Konfigurationsdatei und der QR-Code enthalten den privaten Schlüssel für den Client und den Pre-Shared Key für die Verbindung. Achten Sie daher darauf, den Zugriff strikt zu kontrollieren und die Datei ausschließlich verschlüsselt zu übertragen.

63. Kapitel - WireGuard Clients

63.1. Installation

Das WireGuard VPN-Clientprogramm kann für die verschiedenen Plattformen von https://www.wireguard.com/install/ heruntergeladen werden. Dort finden Sie auch Links in die App Stores der jeweiligen Plattformen sowie die zur Installation auf der jeweiligen Plattform nötigen Befehle.

63.2. Konfiguration

Erzeugen Sie auf dem Intra2net System eine Konfigurationsdatei wie in Abschnitt 62.2, „Automatische Konfiguration für Clients auf dem Intra2net System“ beschrieben und übertragen sie zum Client.

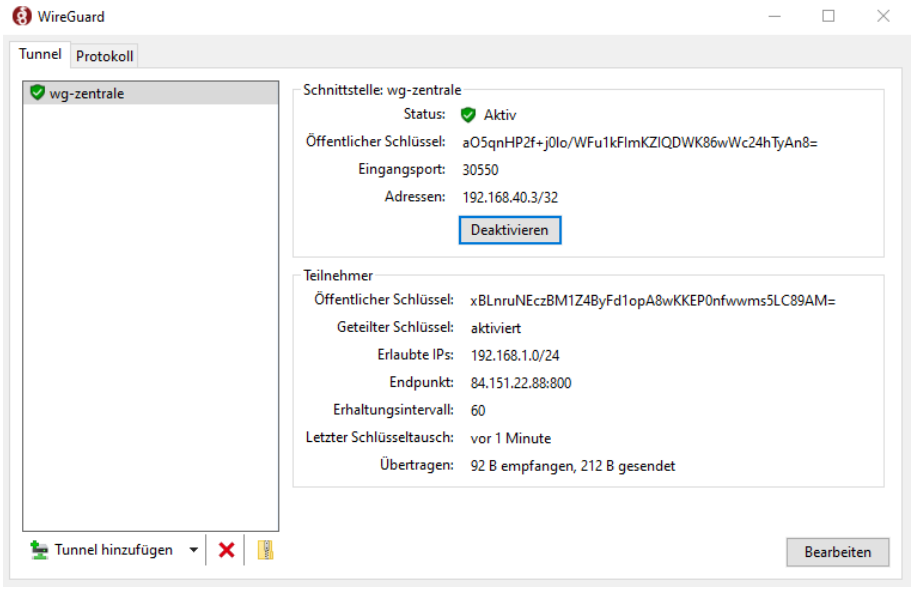
Achten Sie darauf, den Zugriff auf die Datei strikt zu kontrollieren und die Datei nur verschlüsselt zu übertragen da sie private Schlüssel enthält.

Importieren Sie die Datei auf dem Client über die Schaltfläche "Importiere Tunnel aus Datei".

Bei Client-Geräten mit Kamera können Sie alternativ direkt den QR-Code vom Bildschirm abfotografieren.

63.3. Bedienung des Clients

Auf der linken Seite werden die verfügbaren Verbindungen angezeigt. Über einen Klick auf "Aktivieren" wird die jeweilige Verbindung gestartet.



Hinweis

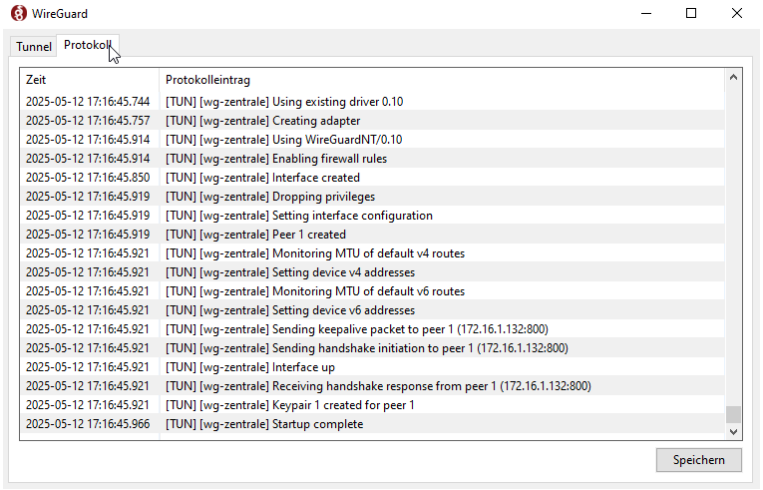
Beachten Sie unbedingt, dass die Angeige "Status: Aktiv" *nicht* bedeutet dass eine Verbindung erfolgreich aufgebaut wurde. Sie bedeutet nur, dass der Client bei Bedarf eine Verbindung versucht herzustellen.

Auch wenn sich die Anzeige der übertragenen Datenmenge in beide Richtungen erhöht, erlaubt dies keinen Rückschluss auf eine tatsächlich bestehende Verbindung. Denn auch unvollständige Handshake-Versuche und deren Antworten zählen mit zur übertragenen Datenmenge.

Ob eine Verbindung tatsächlich zustande gekommen ist oder nicht, erkennen Sie ausschließlich an der Anzeige "Letzter Schlüsseltausch". Wenn dort ein erfolgreicher Handshake innerhalb der letzten 3 Minuten angezeigt wird, ist von einer tatsächlich bestehenden Verbindung auszugehen.

63.3.1. Logdateien

Über den Reiter "Protokolle" kann ein detailliertes Protokoll des Verbindungsfortschritts eingesehen und bei Bedarf exportiert werden. Dies ist zur Fehlersuche hilfreich.



63.3.2. DNS-Namensauflösung

63.3.2.1. Gegenstelle/Endpunkt

Wird wie empfohlen der vollständige Rechnername des Intra2net Systems für Verbindungen aus dem Internet als Gegenstelle/Endpunkt konfiguriert, löst der WireGuard-Client beim Aktivieren der Verbindung diesen DNS-Namen einmalig auf.

Sollte sich die hinter dem DNS-Hostnamen stehende IP-Adresse ändern, z.B. bei einer dynamischen IP mit DynDNS, so muss die VPN-Verbindung im Client kurz deaktiviert und dann neu aktiviert werden, um die Namensauflösung zu aktualisieren.

63.3.2.2. DNS-Hostnamen im VPN-Netz

Das Intra2net System fügt beim Erstellen der VPN-Konfiguration seine eigene IP innerhalb des VPN-Netzes als DNS-Server hinzu. Diese wird vom Client dann beim Verbindungsaufbau als weiterer DNS-Server im System hinzugefügt. DNS-Anfragen werden dann nach der normalen Logik des Client-Betriebssystems durch den VPN-Tunnel gesendet.

Achten Sie darauf, dass DNS-Anfragen in den VPN-Tunnel immer die vollständige Domain verwenden, also z.B. `intra.net.lan` anstatt nur `intra`, denn im VPN-Client ist keine Domain hinterlegt die automatisch angehängt werden könnte.

Prüfen Sie im Fall von DNS-Problemen, ob das Intra2net System korrekt in die Domain im Firmennetz eingebunden ist. Siehe hierzu Abschnitt 9.4, „Domain und DNS“.

63.4. Besonderheiten des Clients für Windows

63.4.1. Schutz der privaten Schlüssel

Der WireGuard Client für Windows verwendet die Microsoft Data Protection API (DPAPI) zum Schutz der Konfiguration und Schlüssel. Diese werden immer mit der DPAPI verschlüsselt auf der Festplatte gespeichert, normalerweise in `C:\Program Files\WireGuard\Data\Configuration`. Zur Verschlüsselung per DPAPI wird das Passwort des Benutzers oder ein im Microsoft-Konto hinterlegter Zufallswert verwendet. Bei Verwendung von Active Directory ist dort noch ein Nachschlüssel hinterlegt.

Der Schutz der VPN-Konfiguration ist also eng an das Windows-Login gekoppelt. Maßnahmen zur Verbesserung der Sicherheit sollten daher am Windows-Login ansetzen. Andere Programme, die mit den Rechten des jeweiligen Benutzers laufen, können Zugriff auf die VPN-Konfiguration erlangen. Ohne gültiges Login des Benutzers ist ein Zugriff aber nicht möglich.

63.4.2. Nutzung ohne Administratorrechte

Für die volle Nutzung des WireGuard Clients werden unter Windows die Rechte der Administratorengruppe benötigt. Es ist aber möglich das WireGuard-VPN einmalig als Administrator einzurichten und dann für andere Nutzer ohne Administratorrechte vorzubereiten. Diese anderen Nutzer benötigen aber die Mitgliedschaft in der Windows-Benutzergruppe `Netzwerkkonfigurations-Operatoren` (S-1-5-32-556), um WireGuard nutzen zu können.

Gehen Sie wie folgt und in dieser Reihenfolge vor, um den Zugriff einzurichten:

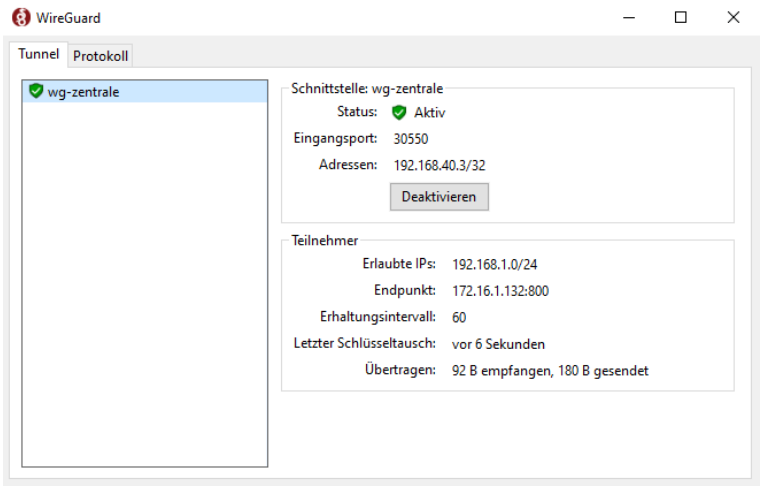
1. Öffnen Sie die Windows-Benutzerverwaltung und fügen den/die gewünschten Benutzer zur Gruppe `Netzwerkkonfigurations-Operatoren` (S-1-5-32-556) hinzu.

2. Öffnen Sie eine Eingabeaufforderung (cmd.exe) als Administrator und führen folgenden Befehl aus um den Zugriff im WireGuard Client freizugeben:

   ```
   reg add HKLM\Software\WireGuard /v LimitedOperatorUI /t REG_DWORD /d 1
   /f
   ```

3. Konfigurieren Sie die gewünschte VPN-Verbindung im WireGuard Client einmalig als Benutzer mit Administratorrechten.

Nutzer ohne Administratorrechte bekommen jetzt eine Variante des WireGuard Clients mit reduzierten Möglichkeiten zu sehen und können darüber die vorher vom Administrator hinterlegten Verbindungen aufbauen und trennen. Die Menüpunkte zum Importieren oder Bearbeiten von Verbindungen sind nicht verfügbar.



63.4.3. Routing für das Netz Alles (0.0.0.0/0.0.0.0)

Der WireGuard Client für Windows erlaubt das Standardgateway in den VPN-Tunnel zu legen. Dies wird bei der Konfiguration des Tunnels auf dem Intra2net System über die Option "Alles (0.0.0.0/0.0.0.0)" beim Punkt "Lokale Netze" umgesetzt.

Dann fließt aller Datenverkehr, auch der für das Internet bestimmte, zuerst durch den VPN-Tunnel zum Intra2net System. Dies ist empfehlenswert wenn der Client nicht über eine vertrauenswürdige Internetanbindung verfügt, z.B. einen öffentlichen WLAN-Hotspot. Allerdings wird die Internetleitung des Intra2net Systems stärker belastet, da der Datenverkehr vom Client ins Internet hier jetzt zweimal übertragen werden muss.

Der WireGuard Client für Windows verfügt in diesem Zusammenhang noch über eine weitere Funktion, das Blockieren des Datenverkehrs außerhalb des VPN-Tunnels. Mit dieser Funktion werden mit wenigen Ausnahmen alle Pakete blockiert, die nicht in den VPN-Tunnel laufen. Dies betrifft insbesondere auch den Datenverkehr in das lokale Netz am Standort des Clients. Also z.B. den Zugriff auf Netzwerkdrucker, NAS-Laufwerke und ähnliches am Standort des Clients.

Ob diese Pakete erlaubt oder blockiert werden sollen, können Sie beim Anlegen der Verbindung auf dem Intra2net System festlegen. Ebenso kann es nachträglich beim Bearbeiten des VPN-Tunnels auf dem Windows Client geändert werden.

Für das Blockieren wird die Windows Filtering Platform (WFP) verwendet. Diese ist nicht zu verwechseln mit der Windows Firewall und ist unabhängig von dieser eine Ebene tiefer im System angesiedelt. Daher sind diese Filter auch nicht in der Windows Firewall sichtbar oder mit ihr beeinflussbar.

64. Kapitel - Verbindung mit anderen Intra2net Systemen

Gehen Sie wie folgt vor um eine VPN-Verbindung zwischen 2 Intra2net Systemen aufzubauen:

1. Stellen Sie sicher dass die vorbereitenden Schritte alle wie im 61. Kapitel, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben auf *beiden Systemen* durchgeführt wurden.

2. Öffnen Sie auf dem zweiten Intra2net-System das Menü "System > Schlüssel > Eigene Schlüssel" und übernehmen Sie den öffentlichen Teil des WireGuard-Schlüssels in die Zwischenablage. Gehen Sie auf dem ersten Intra2net-System in das Menü "System > Schlüssel > Fremde Schlüssel", klicken Sie auf "Neu", fügen Sie den Schlüssel aus der Zwischenablage ein und speichern Sie.

3. Öffnen Sie auf dem ersten System das Menü "Dienste > VPN > Verbindungen" und legen eine neue Verbindung an. Wählen Sie den Typ "WireGuard: Site-to-Site oder eigene Konfiguration" und im nächsten Schritt "Intra2net System".

4. Geben Sie den externen DNS-Hostnamen der Gegenstelle sowie die UDP-Portnummer des dortigen WireGuard-Interface ein. Wählen Sie den vorher importierten öffentlichen Schlüssel der Gegenstelle aus.

5. Wählen Sie als nächstes die miteinander zu verbindenden Netze der beiden Seiten aus.

6. Konfigurieren Sie die Rechte für von der Gegenseite eingehende Verbindungen. Achten Sie insbesondere darauf, keine zu freizügige Firewall-Regelliste zu wählen und nur die Verbindungen zuzulassen, die tatsächlich benötigt werden. Legen Sie im Zweifelsfall eine dedizierte Firewall-Regelliste für diese VPN-Verbindung an.

7. Als letztes haben Sie die Möglichkeit, die Aktivierung zu konfigurieren. Eine passiv/manuell gestartete Verbindung bleibt erst mal offline und wird dann bei Bedarf gestartet. Dies geht zum einen über die Hauptseite, durch ein von dieser Seite aus zu sendendes IP-Paket oder durch ein Handshake der Gegenseite.

   Bei einer immer gestarteten Verbindung versucht das Intra2net System ständig die Verbindung aufzubauen und offen zu halten. Gerade bei letzterem sollte auch ein Keepalive konfiguriert werden, welches eine einmal geöffnete Verbindung ständig online hält.

8. Exportieren Sie die Verbindungkonfiguration über einen Klick auf "Download" und transferieren sie zur Gegenseite. Die Konfiguration enthält den Pre-Shared Key und sollte daher nur verschlüsselt übertragen werden.

9. Öffnen Sie auf dem zweiten System das Menü "Dienste > VPN > Verbindungen" und legen eine neue Verbindung an. Wählen Sie den Typ "WireGuard: Site-to-Site Import".

10. Fügen Sie die vorher exportierte Konfigurationsdatei ein und speichern.

Soll die VPN-Verbindung ständig online sein, so wird empfohlen, die Verbindung so zu konfigurieren, dass sie von beiden Seiten aus aufgebaut werden kann. Dies erhöht die Stabilität und sorgt im Fall einer Unterbrechung für einen schnelleren Wiederaufbau der Verbindung.

65. Kapitel - Verbindung mit anderen Routern und Firewalls

Gehen Sie wie folgt vor, um eine Netz-zu-Netz Verbindung mit anderen Routern aufzubauen.

1. Stellen Sie sicher, dass die vorbereitenden Schritte alle wie im 61. Kapitel, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben durchgeführt wurden.

2. Prüfen Sie, ob der andere Router oder Firewall bereits über irgendeine andere WireGuard VPN-Verbindung, oder zumindest einen eigenen WireGuard-Schlüssel verfügt.

Fahren Sie abhängig vom Ergebnis mit einem der beiden folgenden Abschnitte fort.

65.1. Gegenseite ohne eigenen Schlüssel

Mit den folgenden Schritten wird die Verbindungskonfiguration und ein passendes Schlüsselpaar für die Gegenseite auf dem Intra2net System erzeugt:

1. Öffnen Sie auf dem Intra2net System das Menü "Dienste > VPN > Verbindungen" und legen eine neue Verbindung an. Wählen Sie den Typ "WireGuard: Site-to-Site oder eigene Konfiguration" und im nächsten Schritt "Anderes Gerät ohne vorhandene WireGuard VPN-Verbindungen".

2. Geben Sie den externen DNS-Hostnamen der Gegenstelle sowie die UDP-Portnummer des dortigen WireGuard-Interface ein.

3. Wählen Sie als nächstes die miteinander zu verbindenden Netze der beiden Seiten aus.

4. Konfigurieren Sie die Rechte für von der Gegenseite eingehende Verbindungen. Achten Sie insbesondere darauf keine zu freizügige Firewall-Regelliste zu wählen und nur die Verbindungen zuzulassen, die tatsächlich benötigt werden. Legen Sie im Zweifelsfall eine dedizierte Firewall-Regelliste für diese VPN-Verbindung an.

5. Als letztes haben Sie die Möglichkeit, die Aktivierung zu konfigurieren. Eine passiv/manuell gestartete Verbindung bleibt erst mal offline und wird dann bei Bedarf gestartet. Dies geht zum einen über die Hauptseite, durch ein von dieser Seite aus zu sendendes IP-Paket oder durch ein Handshake der Gegenseite.

   Bei einer immer gestarteten Verbindung versucht das Intra2net System ständig die Verbindung aufzubauen und offen zu halten. Gerade bei letzterem sollte auch ein Keepalive konfiguriert werden, welches eine einmal geöffnete Verbindung ständig online hält.

6. Exportieren Sie die Verbindungkonfiguration über einen Klick auf "Download". Es handelt sich um eine vollständige Konfiguration für ein WireGuard-Interface inkl. privatem Schlüssel. Transferieren Sie diese zur Gegenseite.

   Die Konfiguration enthält den Privaten Schlüssel und Pre-Shared Key und sollte daher nur verschlüsselt übertragen werden.

7. Importieren Sie die Konfigurationsdatei auf dem anderen Routers oder Firewall.

   Unter Linux wird die Datei normalerweise als `/etc/wireguard/wg0.conf` abgelegt.

Abhängig vom jeweiligen Produkt kann es auch sein, dass Sie die Daten aus der Konfigurationsdatei über einzelne Punkte in einer Oberfläche konfigurieren müssen. Konsultieren im Zweifelsfall die Dokumentation des Produkts.

Soll die VPN-Verbindung ständig online sein, so wird empfohlen die Verbindung so zu konfigurieren, dass sie von beiden Seiten aus aufgebaut werden kann. Dies erhöht die Stabilität und sorgt im Fall einer Unterbrechung für einen schnelleren Wiederaufbau der Verbindung.

65.2. Gegenseite mit vorhandenem eigenen Schlüssel

1. Lassen Sie sich auf dem anderen Router oder Firewall den öffentlichen Schlüssel eines WireGuard-Interfaces anzeigen. Dies ist oft in einem Menü für die WireGuard-Interfaces oder dem WireGuard-Status einsehbar. Auf der Linux Kommandozeile kann der Befehl `wg` verwendet werden. Achten Sie darauf, dass Sie den öffentlichen Schlüssel und nicht den privaten exportieren. Konsultieren im Zweifelsfall die Dokumentation des Produkts.

   Übernehmen Sie den öffentlichen Schlüssel in die Zwischenablage.

2. Öffnen Sie auf dem Intra2net System das Menü "System > Schlüssel > Fremde Schlüssel", Klick auf "Neu", fügen den Schlüssel aus der Zwischenablage ein und speichern.

3. Öffnen Sie auf dem Intra2net System das Menü "Dienste > VPN > Verbindungen" und legen eine neue Verbindung an. Wählen Sie den Typ "WireGuard: Site-to-Site oder eigene Konfiguration" und im nächsten Schritt "Anderes Gerät mit vorhandenen WireGuard-Verbindungen".

4. Geben Sie den externen DNS-Hostnamen der Gegenstelle sowie die UDP-Portnummer des dortigen WireGuard-Interface ein. Wählen Sie den vorher importierten öffentlichen Schlüssel der Gegenstelle aus.

5. Wählen Sie als nächstes die miteinander zu verbindenden Netze der beiden Seiten aus.

6. Konfigurieren Sie die Rechte für von der Gegenseite eingehende Verbindungen. Achten Sie insbesondere darauf keine zu freizügige Firewall-Regelliste zu wählen und nur die Verbindungen zuzulassen, die tatsächlich benötigt werden. Legen Sie im Zweifelsfall eine dedizierte Firewall-Regelliste für diese VPN-Verbindung an.

7. Als letztes haben Sie die Möglichkeit die Aktivierung zu konfigurieren. Eine passiv/manuell gestartete Verbindung bleibt erst mal offline und wird dann bei Bedarf gestartet. Dies geht zum einen über die Hauptseite, durch ein von dieser Seite aus zu sendendes IP-Paket oder durch ein Handshake der Gegenseite.

   Bei einer immer gestarteten Verbindung versucht das Intra2net System ständig die Verbindung aufzubauen und offen zu halten. Gerade bei letzterem sollte auch ein Keepalive konfiguriert werden, welches eine einmal geöffnete Verbindung ständig online hält.

8. Exportieren Sie die Verbindungkonfiguration über einen Klick auf "Download" und transferieren sie zur Gegenseite. Die Konfiguration enthält den Pre-Shared Key und sollte daher nur verschlüsselt übertragen werden.

9. Fügen Sie die vorher exportierte Konfigurationsdatei zu der bestehenden Konfiguration des anderen Routers oder Firewall hinzu.

   Wenn das Gerät die Möglichkeit zur Bearbeitung der Konfiguration im wg-quick-Format bietet, dann fügen Sie die neue Verbindung als eine weitere "[Peer]"-Sektion am Ende der bestehenden Datei hinzu. Unter Linux finden Sie die Dateien normalerweise im Verzeichnis `/etc/wireguard/`. Sollte es Dateien für mehrere Interfaces geben, so achten Sie darauf die zu bearbeiten, von der Sie vorher den öffentlichen Schlüssel exportiert haben.

   Abhängig vom jeweiligen Produkt kann es auch sein, dass Sie die Daten aus der Konfigurationsdatei über einzelne Punkte in einer Oberfläche konfigurieren müssen. Konsultieren im Zweifelsfall die Dokumentation des Produkts.

Soll die VPN-Verbindung ständig online sein, so wird empfohlen, die Verbindung so zu konfigurieren, dass sie von beiden Seiten aus aufgebaut werden kann. Dies erhöht die Stabilität und sorgt im Fall einer Unterbrechung für einen schnelleren Wiederaufbau der Verbindung.

66. Kapitel - Verbindung mit AVM FRITZ!Boxen

Gehen Sie wie folgt vor, um eine Netz-zu-Netz Verbindung mit einer AVM FRITZ!Box aufzubauen.

1. Stellen Sie sicher, dass die vorbereitenden Schritte alle wie im 61. Kapitel, „Vorbereiten der Konfiguration auf dem Intra2net System“ beschrieben durchgeführt wurden.

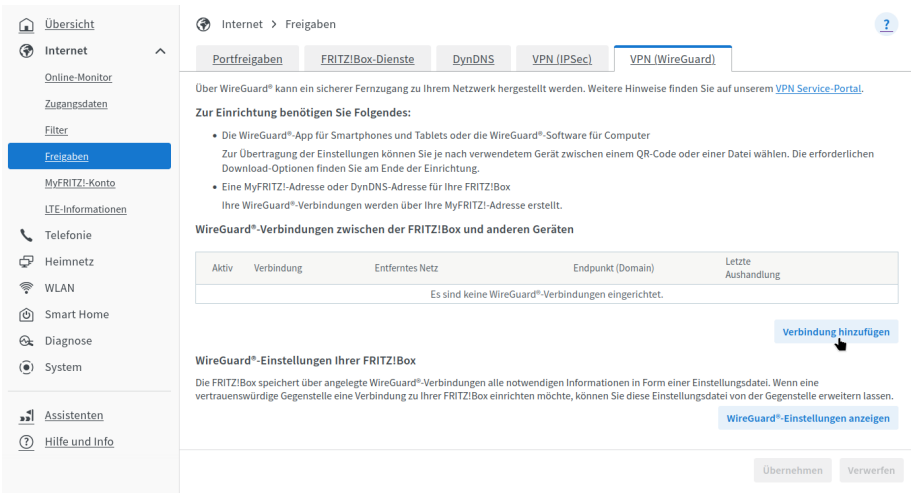
2. Prüfen Sie, ob die AVM FRITZ!Box bereits über irgendeine andere WireGuard VPN-Verbindung verfügt. Öffnen Sie dafür das Menü "Internet > Freigaben > VPN (WireGuard)".

Fahren Sie abhängig vom Ergebnis mit einem der beiden folgenden Abschnitte fort.

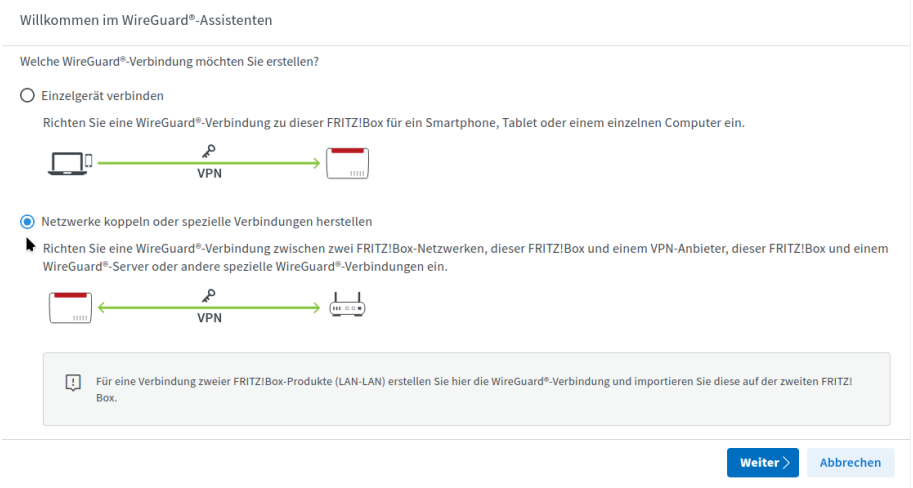
66.1. AVM FRITZ!Box ohne bisherige Verbindung

1. Führen Sie die in Abschnitt 65.1, „Gegenseite ohne eigenen Schlüssel“ beschriebenen Schritte auf dem Intra2net System durch.

2. Öffnen Sie auf der AVM FRITZ!Box das Menü "Internet > Freigaben > VPN (WireGuard)" und klicken auf "Verbindung hinzufügen".



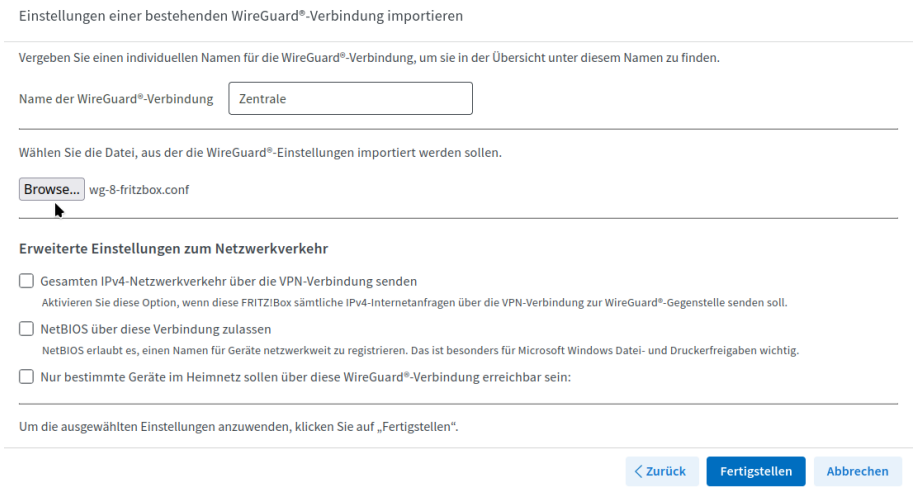
3. Wählen Sie "Netzwerke koppeln oder spezielle Verbindungen herstellen"



4. Wählen Sie "Ja" bei der Frage ob die Verbindung bereits auf der Gegenstelle erstellt wurde.



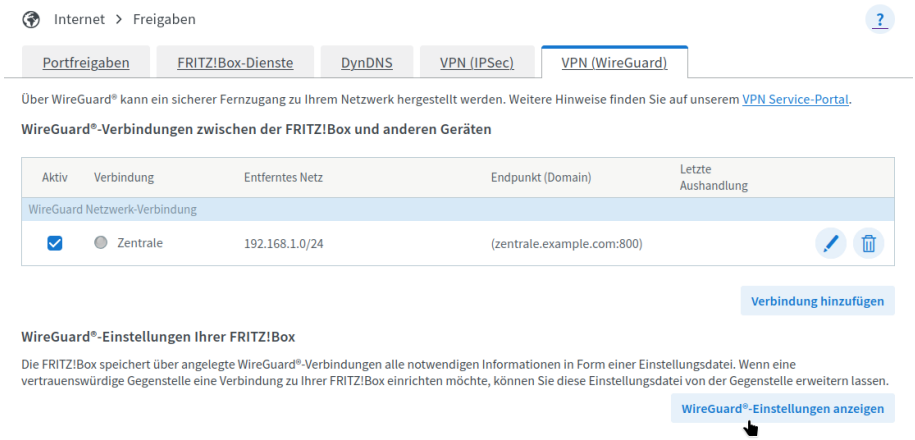
5. Geben Sie der Verbindung einen Namen und wählen die vorher vom Intra2net System exportierte Konfigurationsdatei. Klicken Sie auf "Fertigstellen".



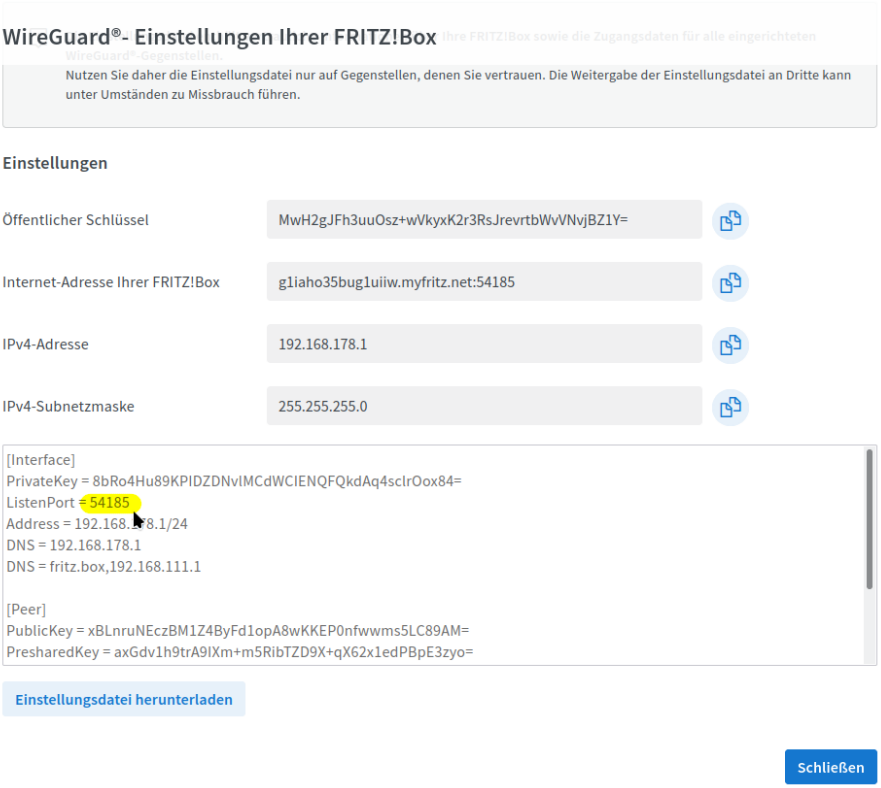
6. Die Verbindung wird importiert.

   Es wurde beobachtet, dass es hierbei manchmal zu internen Fehlern auf der FRITZ!Box kommen kann. Wiederholen Sie den Import in diesem Fall. Sollte es nach 2 Versuchen immer noch nicht funktionieren, so starten Sie die FRITZ!Box neu (Menü "System > Sicherung > Neustart").

7. Lassen Sie sich die WireGuard-Einstellungen der FRITZ!Box anzeigen.



8. Die FRITZ!Box wählt beim Anlegen der ersten Verbindung immer eigenständig eine zufällige UDP-Portnummer für WireGuard aus. Lesen Sie diese unter dem Punkt "ListenPort" aus.



9. Gehen Sie auf dem Intra2net System in das Menü "Dienste > VPN > Verbindungen", wählen die Verbindung zur FRITZ!Box und tragen Sie die ausgelesene Portnummer der FRITZ!Box beim Punkt "Port auf Gegenseite (UDP)" ein.

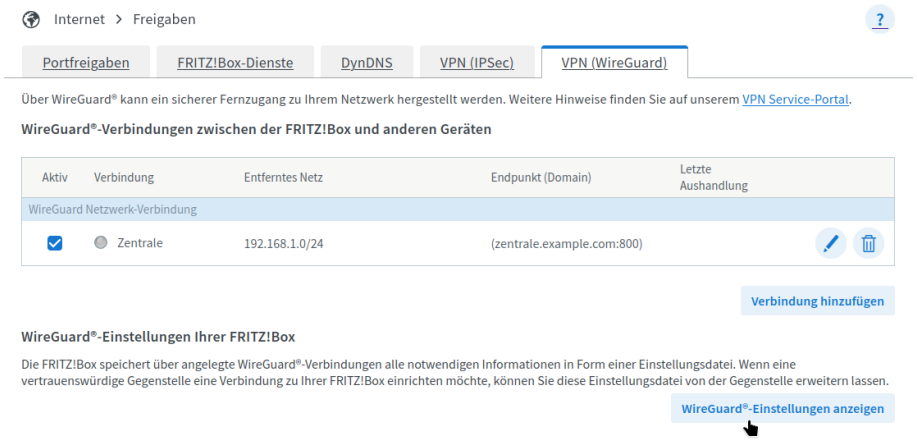
In einzelnen Fällen wurde beobachtet, dass die FRITZ!Box eine neu eingerichtete WireGuard Verbindung erst nach einem Neustart aktiviert hat, obwohl sie in der Verbindungsliste angezeigt wurde. Im Fall von Verbindungsproblemen empfehlen wir daher die FRITZ!Box neu zu starten (Menü "System > Sicherung > Neustart").

Soll die VPN-Verbindung ständig online sein, so wird empfohlen die Verbindung so zu konfigurieren, dass sie von beiden Seiten aus aufgebaut werden kann. Dies erhöht die Stabilität und sorgt im Fall einer Unterbrechung für einen schnelleren Wiederaufbau der Verbindung.

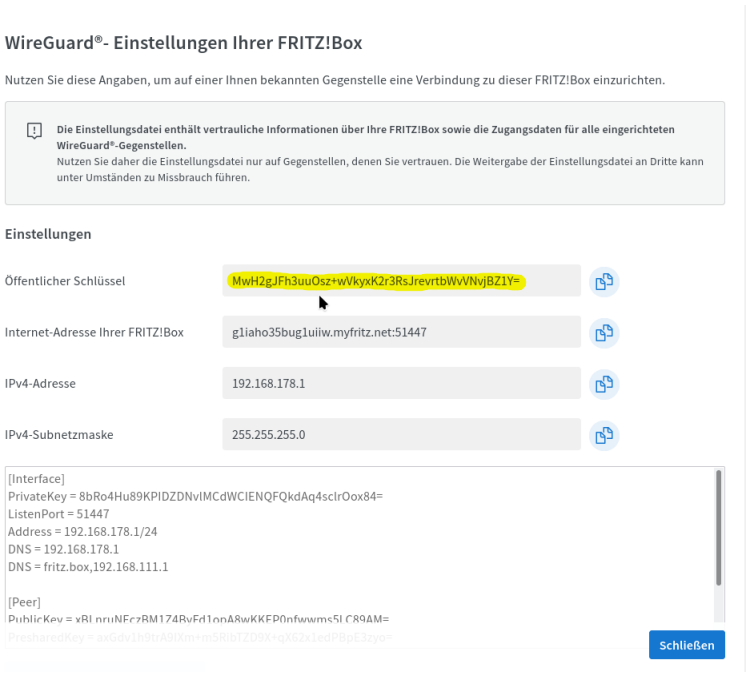
66.2. AVM FRITZ!Box mit anderer VPN-Verbindung

Gehen Sie auf einer AVM FRITZ!Box mit einer bereits bestehenden VPN-Verbindung zu einer anderen Gegenstelle wie folgt vor:

1. Öffnen Sie auf der AVM FRITZ!Box das Menü "Internet > Freigaben > VPN (WireGuard)" und klicken auf "WireGuard-Einstellungen anzeigen".



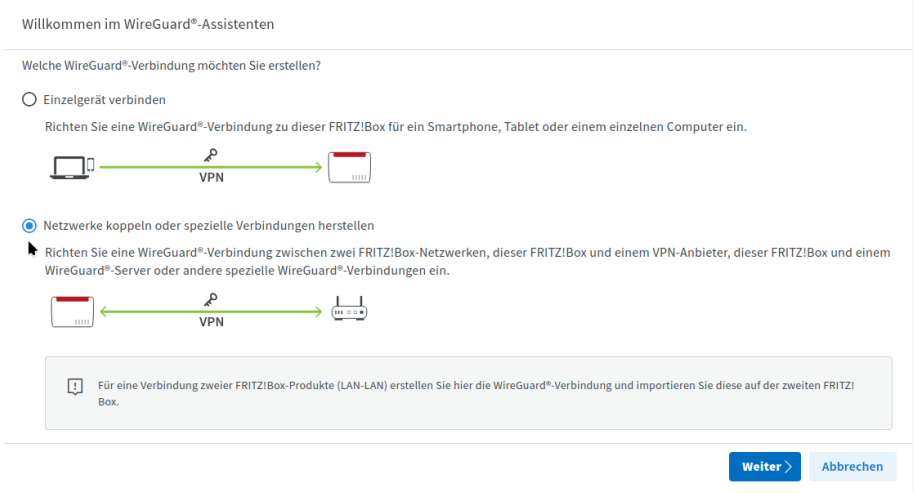
2. Der bestehende öffentliche Schlüssel der FRITZ!Box wird angezeigt. Übernehmen Sie diesen in die Zwischenablage.



3. Führen Sie die in Abschnitt 65.2, „Gegenseite mit vorhandenem eigenen Schlüssel“ beschriebenen Schritte auf dem Intra2net System durch.

4. Öffnen Sie auf der AVM FRITZ!Box das Menü "Internet > Freigaben > VPN (WireGuard)" und klicken auf "Verbindung hinzufügen".

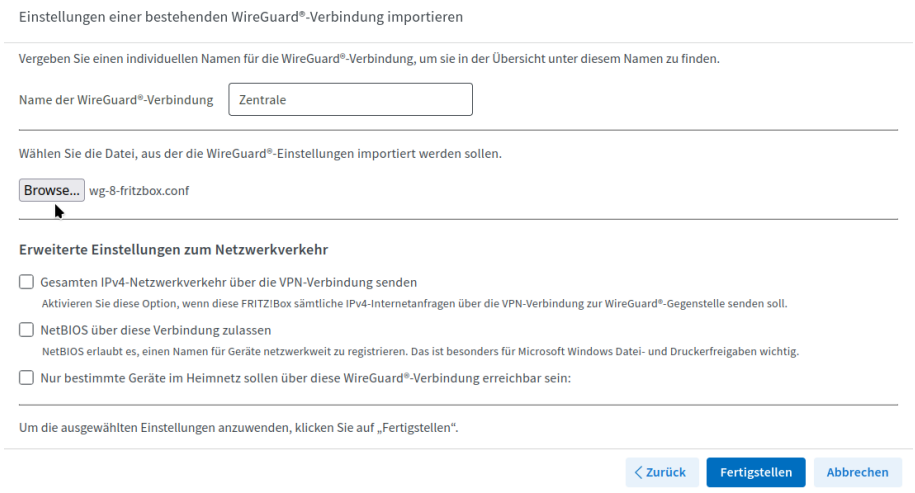
5. Wählen Sie "Netzwerke koppeln oder spezielle Verbindungen herstellen"



6. Wählen Sie "Ja" bei der Frage ob die Verbindung bereits auf der Gegenstelle erstellt wurde.



7. Geben Sie der Verbindung einen Namen und wählen die vorher vom Intra2net System exportierte Konfigurationsdatei. Klicken Sie auf "Fertigstellen".



8. Die Verbindung wird importiert.

   Es wurde beobachtet, dass es hierbei manchmal zu internen Fehlern auf der FRITZ!Box kommen kann. Wiederholen Sie den Import in diesem Fall. Sollte es nach 2 Versuchen immer noch nicht funktionieren, so starten Sie die FRITZ!Box neu (Menü "System > Sicherung > Neustart").

In einzelnen Fällen wurde beobachtet, dass die FRITZ!Box eine neu eingerichtete WireGuard Verbindung erst nach einem Neustart aktiviert hat, obwohl sie in der Verbindungsliste angezeigt wird. Im Fall von Verbindungsproblemen empfehlen wir daher die FRITZ!Box neu zu starten (Menü "System > Sicherung > Neustart").

Soll die VPN-Verbindung ständig online sein, so wird empfohlen die Verbindung so zu konfigurieren, dass sie von beiden Seiten aus aufgebaut werden kann. Dies erhöht die Stabilität und sorgt im Fall einer Unterbrechung für einen schnelleren Wiederaufbau der Verbindung.

67. Kapitel - Zustands- und Fehlerdiagnose

67.1. Hauptseite

Auf der Hauptseite werden im Statusbereich alle VPN-Verbindungen angezeigt, die momentan online sind. Verbindungen, die immer online sein sollten (Aktivierung "Immer"), jedoch nicht hergestellt werden können, werden explizit als `Offline` aufgeführt. Dies gilt sowohl für WireGuard- als auch für IPSec-Verbindungen.

Über die Schaltflächen "VPN verbinden" und "VPN trennen" lassen sich die VPNs direkt steuern.

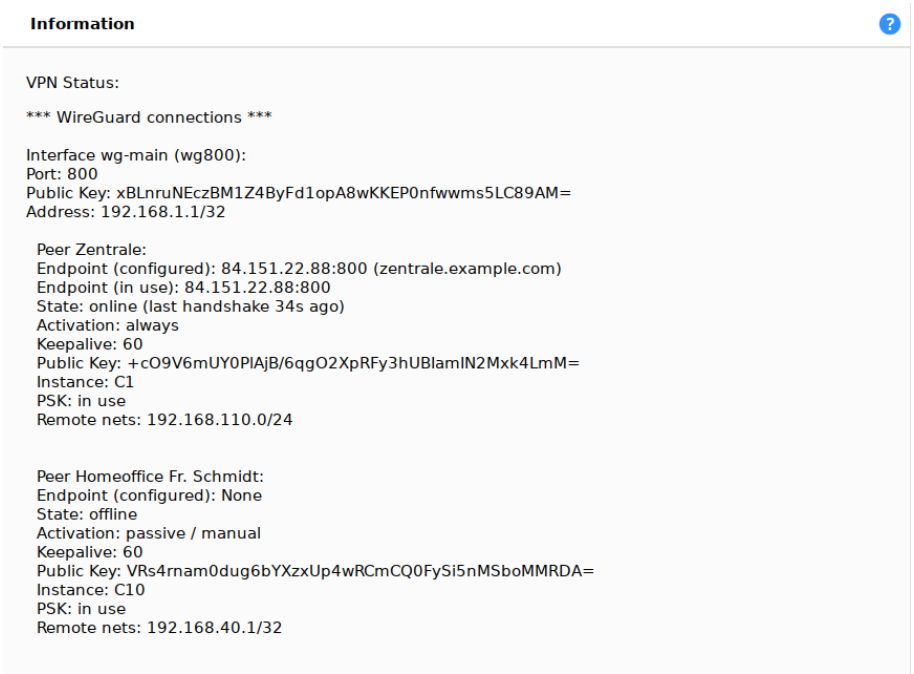
Beachten Sie dabei, dass durch "VPN trennen" die Verbindung nur auf der lokalen Seite getrennt wird, denn das WireGuard-Protokoll sieht keine Möglichkeit vor, der Gegenseite eine Trennung mitzuteilen. Die Gegenseite kann auch von sich aus weiterhin die Verbindung neu aufbauen. Möchten Sie dies verhindern, so muss die Verbindung im Menü "Dienste > VPN > Verbindungen" deaktiviert werden.

67.2. VPN-Status

Einen detaillierteren Überblick über den aktuellen Status aller VPN-Verbindungen erhält man über das Menü "Information > System > VPN".

Hier werden alle konfigurierten WireGuard-Verbindungen unterhalb des jeweiligen WireGuard-Interfaces aufgeführt. Punkte wie u.a. der aktuelle Verbindungsstatus, die IP der Gegenstelle und der letzte erfolgreiche Handshake werden angezeigt.

Im Gegensatz zu den VPN-Clients zeigt das Intra2net System nur dann den Status "Online" an, wenn tatsächlich innerhalb der letzten 3 Minuten (evtl. zzgl. Keepalive-Zeit) ein erfolgreicher Handshake stattgefunden hat.



67.3. Logs

Alle Protokolle bezügl. WireGuard-VPN werden in den Systemmeldungen (messages) protokolliert und können über das Menü "Information > System > Logdateien" abgerufen werden. Für WireGuard sind Meldungen mit den Dienstekennungen `i2n-wg` und `kernel: wireguard:` relevant.

Bei jeder Meldung wird der öffentliche Schlüssel der Gegenseite mit angegeben. Über diesen lassen sich alle Meldungen einer Verbindung zuordnen. Eine Übersicht über alle öffentlichen Schlüssel finden Sie unter "Information > System > VPN".

Wurde eine Verbindung erfolgreich aufgebaut, so wird dies wie in diesem Beispiel protokolliert:

```
i2n-wg[2732]: Connection "Zentrale" (C1) is now online with peer
84.151.22.88:800; [wg800: +cO9V6mUY0PlAjB/6qgO2XpRFy3hUBIamIN2Mxk4LmM=]
```

Wechselt eine Verbindung in den Status Offline sieht das Protokoll so aus:

```
i2n-wg[2732]: Connection "Zentrale" (C1) is now offline; [wg800:
+cO9V6mUY0PlAjB/6qgO2XpRFy3hUBIamIN2Mxk4LmM=]
```

Teil 8. Anhang

Anhang A. Lizenzen

A.1. Intra2net Software Lizenzvertrag

Version 2.2 vom 12. April 2022

Intra2net AG, Mömpelgarder Weg 8, 72072 Tübingen, Deutschland

Dieser Lizenzvertrag räumt Ihnen als Lizenznehmer ein nicht ausschließliches unbefristetes Nutzungsrecht an dem von der Intra2net AG entwickelten Computerprogramm "Intra2net System Manager" unter den nachfolgenden Lizenzbedingungen und in dem nachfolgend beschriebenen Umfang ein. Mit der Installation der Software erklären Sie sich mit folgenden Lizenzbedingungen einverstanden:

§ 1 Vertragsgegenstand

1) Die Software Produkte Intra2net Business Server, Intra2net Security Gateway und Intra2net Network Security (nachfolgend als "Intra2net Software" bezeichnet) bestehen aus dem "Intra2net System Manager" sowie der "Linux Open-Source Distribution". Gegenstand dieses Lizenzvertrages ist - vorbehaltlich der Regelung in § 2 dieses Vertrags - nur der "Intra2net System Manager". Die "Linux Open-Source Distribution" unterliegt eigenen Lizenzbedingungen, die den entsprechenden RPM-Paketen beigefügt sind.

2) Der "Intra2net System Manager" besteht aus komprimierten Dateien zzgl. Installationsprogramm (RPM-Paket), die den lauffähigen Code der von der Intra2net AG programmierten Software enthalten. Der "Intra2net System Manager" wird nicht als Open-Source Software vertrieben. Alle urheberrechtlichen Nutzungsrechte und sonstigen gewerblichen Schutzrechte an dem "Intra2net System Manager" liegen bei der Intra2net AG oder wurden der Intra2net AG zur vertragsgemäßen Nutzung von Dritten eingeräumt. Die Bestandteile des "Intra2net System Manager" sind in den RPM-Paketen entsprechend gekennzeichnet.

§ 2 Andere Lizenzen

1) Zusammen mit dem "Intra2net System Manager" erhalten Sie auch eine Programmkopie einer "Linux Open-Source Distribution". Die Intra2net AG überlässt Ihnen die Programmkopie der "Linux Open-Source Distribution" unentgeltlich, so dass die Haftung sich insoweit 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, räumt Ihnen nicht die Intra2net AG ein, sondern die jeweiligen Autoren der entsprechenden Programmteile übertragen die Nutzungsrechte unmittelbar. Der Umfang Ihrer Nutzungsrechte bezogen auf die "Linux Open-Source Distribution" bestimmt sich folglich ausschließlich nach den der "Linux Open-Source Distribution" beigefügten 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 "Intra2net Software", neben den Vorschriften dieses Lizenzvertrages, im Rahmen eines direkten Nutzungsvertrages mit den jeweiligen Softwareherstellers ohne Zwischenschaltung der Intra2net AG zu beachten. Die entsprechenden Lizenzbedingungen sind in elektronischer Form der zugehörigen Software beigefügt.

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, können die Quelltexte auf der Website www.intra2net.com frei heruntergeladen werden.

5) Soweit innerhalb der überlassenen Programme Libraries genutzt werden, die unter der LGPL lizenziert sind, werden diese entweder als gemeinsam genutzte Programmbibliothek 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 "Intra2net Software" läuft nicht parallel mit anderen Betriebssystemen auf einem System. Insbesondere formatiert die "Intra2net Software" bei Installation die gesamte Festplatte und löscht alle bestehenden Daten. Sofern auf dem System bereits Daten vorhanden sind, sind vor der Installation die zwingend erforderlichen Sicherungskopien anzufertigen und im Anschluss daran in einer Weise sicher aufzubewahren, dass sie jederzeit reproduziert werden können.

2) Die "Intra2net Software" arbeitet nur mit dafür von Intra2net freigegebenen Hardwarekomponenten zusammen. Diese sind in der Dokumentation sowie auf der Webseite www.intra2net.com aufgeführt und werden regelmäßig aktualisiert. Diese Hinweise hat der Lizenznehmer zu beachten. Die Intra2net AG 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 bei Intra2net registrierten Kunden werden per E-Mail mindestens 3 Monate vorher darüber in Kenntnis gesetzt (Abkündigung).

§ 4 Vervielfältigungsrechte und Zugriffsschutz

1) Eine Vervielfältigung des "Intra2net System Manager" 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 oder im Wege des Downloads auf den Massenspeicher der eingesetzten Hardware sowie das Laden des Programms in den Arbeitsspeicher.

2) 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.

3) 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.

4) Die Mitarbeiter des Lizenznehmers sind nachdrücklich auf die Einhaltung der vorliegenden Vertragsbedingungen sowie der Bestimmungen des Urheberrechts hinzuweisen.

5) Der Lizenzgeber ist berechtigt, Lizenzcodes zu sperren, wenn nachweislich Hinweise auf einen Verstoß gegen den Lizenzvertrag vorliegen. Der Lizenznehmer wird, sofern gültige Kontaktdaten vorliegen, unter Setzung einer Nachfrist von 14 Tagen zur Nachli-

zensierung aufgefordert. Der rechtmäßige Eigentümer einer Lizenz kann bei Sperrung eines Lizenzcodes gegen Vorlage des Kaufbelegs kostenfrei einen neuen Lizenzcode erhalten. Es wird darauf hingewiesen, dass Kontaktdaten von Lizenznehmern nach Beendigung eines Support- und Wartungsvertrages aus datenschutzrechtlichen Gründen innerhalb der erforderlichen Fristen gelöscht werden.

6) Der Quellcode des "Intra2net System Manager" ist nicht geschuldet.

§ 5 Nutzungsbeschränkungen

1) Der Lizenznehmer darf den "Intra2net System Manager" auf einer ihm zur Verfügung stehenden Hardware einsetzen. Wechselt der Lizenznehmer jedoch die Hardware, muss er den "Intra2net System Manager" von der bisher verwendeten Hardware löschen.

2) Ein zeitgleiches Einspeichern, Vorrätighalten oder Benutzen ist nur in einer Instanz zulässig. Möchte der Lizenznehmer die Software in mehreren Instanzen einsetzen, muss er eine entsprechende Anzahl von weiteren Lizenzen erwerben.

3) Der Lizenznehmer muss eine zeitgleiche Mehrfachnutzung über die Anzahl der erworbenen Lizenzen 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 im Menüpunkt "Benutzermanager" angelegten Benutzer, der Benutzerkonten auf Zielservern, die für durch das System weitergeleitete E-Mails genutzt werden, sowie der Benutzer, die nicht im Benutzermanager angelegt sind, aber die Möglichkeit haben, den Proxy-Server des Systems zu nutzen.

6) Der Lizenznehmer ist nicht berechtigt, den "Intra2net System Manager" oder einzelne Komponenten hiervon in Gefahrenbereichen, die einen fehlerfreien Dauerbetrieb entsprechender Systeme voraussetzen, einzusetzen. Zu den Gefahrenbereichen zählen insbesondere Hoch-Risiko-Aktivitäten und Hoch-Verfügbarkeits-Aktivitäten, wie zum Beispiel der Betrieb von Kernkraft-Einrichtungen, Waffensystemen, Luftfahrtnavigations- oder Kommunikationssystemen, Verkehrssystemen sowie von Geräten und Maschinen im Klinik- und Gesundheitsbereich oder andere Anwendungen, die für Leben und Gesundheit von Personen von Relevanz sind.

§ 6 Begleitende Dienstleistungen

1) Wurde mit der Lizenz das Recht auf zeitlich beschränkte Dienstleistungen, wie Software-Wartung oder Support, 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 befristete Evaluationslizenz, d.h. für 30 Tage das Recht, den "Intra2net System Manager" auf einer Hardware zu installieren und zu Testzwecken unter diesen Lizenzbedingungen zu nutzen. Mit der Eingabe eines nicht selbst erworbenen Lizenzschlüssels 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 Unternehmern 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 von dem Vertrag zurücktreten oder die vereinbarte Vergütung mindern und Schadensersatz verlangen. Es gelten - vorbehaltlich § 11 - die gesetzlichen Regelungen.

§ 11 Haftung

1) Die nachstehenden Regelungen beziehen sich auf sämtliche Schadensersatzansprüche des Lizenznehmers, egal aus welchem Rechtsgrund, sei es auf Grund von Verschulden bei Vertragsschluss, sei es auf Grund sonstiger Pflichtverletzungen, deliktischer Handlungen oder sonstiger Tatbestände.

2) Die Intra2net AG haftet in voller Höhe für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer vorsätzlichen oder fahrlässigen Pflichtverletzung der gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

3) Die Intra2net AG haftet in voller Höhe für sonstige Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung ihrer gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

4) Die Intra2net AG haftet in voller Höhe für das Fehlen einer garantierten Beschaffenheit der zugesagten Leistung und für das arglistige Verschweigen eines Mangels.

5) Für die verbleibenden Schäden haftet die Intra2net AG dem Grunde nach bei jeder schuldhaften Verletzung von Kardinalpflichten. Kardinalpflichten sind solche Vertragspflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung Vertragspartner regelmäßig vertrauen dürfen. Der Höhe nach haftet die Intra2net AG in diesen Fällen begrenzt auf den Ersatz der Schäden, die bei Vertragsschluss typisch und vorhersehbar waren.

6) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

7) Im Übrigen ist die Haftung der Intra2net AG ausgeschlossen.

8) Ein Mitverschulden des Lizenznehmers infolge der unzureichenden Erbringung von Mitwirkungsleistungen, der verspäteten Anzeige von Schäden, des Einsatzes nicht freigegebener Hardware oder aus sonstigen Gründen ist dem Lizenznehmer anzurechnen.

9) Für den Verlust von Daten und/oder Programmen haftet die Intra2net AG insoweit nicht, als der Schaden darauf beruht, dass es der Lizenznehmer unterlassen hat, die erforderlichen Datensicherungen durchzuführen oder regelmäßig die Vollständigkeit der Datensicherungen zu kontrollieren und dadurch sicherzustellen, dass verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

10) Für durch zusätzlich installierte Software verursachte Schäden wird eine Haftung nur bei Lieferung und Installation durch die Intra2net AG übernommen.

§ 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 Programmfunktionen. Mängel, die hierbei festgestellt werden oder feststellbar sind, müssen dem Lizenzgeber innerhalb weiterer 8 Werktage 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 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.

§ 14 Rechtswahl

Die Parteien vereinbaren im Hinblick auf sämtliche Rechtsbeziehungen aus und im Zusammenhang mit diesem Vertragsverhältnis die Anwendung des Rechts der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

§ 15 Gerichtsstand

Sofern der Lizenznehmer Kaufmann im Sinne des Handelsgesetzbuchs, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder keinen Gerichtsstand im Inland hat wird für sämtliche Streitigkeiten, die im Zusammenhang mit der Begründung, Durchführung und Beendigung dieses Vertragsverhältnisses entstehen, Stuttgart als Gerichtsstand vereinbart.

§ 16 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 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.

A.3. Hinweise zur Rücknahme und Entsorgung

Das Elektro- und Elektronikgerätegesetz (ElektroG) sowie das Batteriegesetz (BattG) enthalten eine Vielzahl von Anforderungen an den Umgang mit Elektro- und Elektronikgeräten. Die wichtigsten Hinweise zur Rücknahme und Entsorgung für B2B-Elektroaltgeräte und Altbatterien sind hier zusammengestellt.

A.3.1. Getrennte Erfassung von Altgeräten

Elektro- und Elektronikgeräte, die zu Abfall geworden sind, werden als Altgeräte bezeichnet. Besitzer von Altgeräten haben diese einer vom unsortierten Siedlungsabfall getrennten Erfassung zuzuführen. Altgeräte gehören insbesondere nicht in den Hausmüll, sondern in spezielle Sammel- und Rückgabesysteme.

A.3.2. Batterien und Akkus sowie Lampen

Besitzer von Altgeräten haben Altbatterien und Altakkumulatoren, die nicht vom Altgerät umschlossen sind, sowie Lampen, die zerstörungsfrei aus dem Altgerät entnommen werden können, im Regelfall vor der Abgabe an einer Erfassungsstelle vom Altgerät zu trennen. Dies gilt nicht, soweit Altgeräte einer Vorbereitung zur Wiederverwendung unter Beteiligung eines öffentlich-rechtlichen Entsorgungsträgers zugeführt werden.

A.3.3. Möglichkeiten der Rückgabe von Altgeräten

Um Möglichkeiten der Rückgabe von Altgeräten zu schaffen, arbeiten wir mit mehreren qualifizierten Recyclingunternehmen zusammen. Wenn ein von uns hergestelltes Gerät zu einem Altgerät geworden ist und Sie es zurückgeben möchten, wenden Sie sich bitte an uns und füllen Sie den Fragebogen aus: https://www.intra2net.com/de/recycling/

A.3.4. Datenschutzhinweis

Altgeräte enthalten häufig sensible personenbezogene Daten. Dies gilt insbesondere für Geräte der Informations- und Telekommunikationstechnik wie Computer und Smartphones. Bitte beachten Sie in Ihrem eigenen Interesse, dass für die Löschung der Daten auf den zu entsorgenden Altgeräten jeder Endnutzer selbst verantwortlich ist.

A.3.5. Bedeutung des Symbols der durchgestrichenen Mülltonne

Das auf den Elektro- und Elektronikgeräten regelmäßig abgebildete Symbol einer durchgestrichenen Mülltonne weist darauf hin, dass das jeweilige Gerät am Ende seiner Lebensdauer getrennt vom unsortierten Siedlungsabfall zu erfassen ist.



A.3.6. Unentgeltliche Rücknahme von Altbatterien

Batterien dürfen nicht über den Hausmüll entsorgt werden. Sie sind zur Rückgabe von Altbatterien gesetzlich verpflichtet, damit eine fachgerechte Entsorgung gewährleistet werden kann. Sie können Altbatterien an einer kommunalen Sammelstelle oder im Handel vor Ort abgeben.

A.3.7. Bedeutung der Batteriesymbole

Batterien sind mit dem Symbol einer durchgekreuzten Mülltonne gekennzeichnet. Dieses Symbol weist darauf hin, dass Batterien nicht in den Hausmüll gegeben werden dürfen. Bei Batterien, die mehr als 0,0005 Masseprozent Quecksilber, mehr als 0,002 Masseprozent Cadmium oder mehr als 0,004 Masseprozent Blei enthalten, befindet sich unter dem Mülltonnen-Symbol die chemische Bezeichnung des jeweils eingesetzten Schadstoffes – dabei steht "Cd" für Cadmium, "Pb" steht für Blei, und "Hg" für Quecksilber.

Anhang B. Lizenz

B.1. Intra2net Groupware Client Lizenzvertrag (EULA)

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 Erlaubte Nutzung

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", ist an diese gebunden und gilt für die dort ausgewiesene Benutzeranzahl.

2) Ein zeitgleiches Einspeichern, Vorrätighalten oder Benutzen ist nur in der Zahl der lizenzierten Benutzer zulässig.

§ 3 Nutzungsbeschränkungen

1) 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.

2) Der Lizenznehmer ist nicht berechtigt, den „Intra2net Groupware Client" oder einzelne Komponenten hiervon in Gefahrenbereichen, die einen fehlerfreien Dauerbetrieb entsprechender Systeme voraussetzen, einzusetzen. Zu den Gefahrenbereichen zählen insbesondere Hoch-Risiko-Aktivitäten und Hoch-Verfügbarkeits-Aktivitäten, wie zum Beispiel der Betrieb von Kernkraft-Einrichtungen, Waffensystemen, Luftfahrtnavigations- oder Kommunikationssystemen, Verkehrssystemen sowie von Geräten und Maschinen im Klinik- und Gesundheitsbereich oder andere Anwendungen, die für Leben und Gesundheit von Personen von Relevanz sind.

3) Der Lizenznehmer hat die Hinweise des Lizenzgebers zu der Einsatzumgebung des „Intra2net Groupware Clients", zu den freigegebenen Versionen des Betriebssystems, zu Microsoft Outlook und zu von der Grundversion abweichenden Konfigurationen von Microsoft Outlook zu beachten. Dies gilt insbesondere für die Verwendung weiterer Outlook-Plugins und Addins.

§ 4 Begleitende Dienstleistungen

Wurde mit der Lizenz das Recht auf zeitlich beschränkte Dienstleistungen (z.B. Update-Service) erworben, so ist deren Laufzeit an die Lizenz des „Intra2net Business Server" gebunden.

§ 5 Evaluationslizenz

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 den Lizenzgeber Vorsatz oder grobe Fahrlässigkeit zu vertreten ist.

§ 6 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.

§ 7 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.

§ 8 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 Unternehmern 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 von dem Vertrag zurücktreten oder die vereinbarte Vergütung mindern und Schadensersatz verlangen. Es gelten - vorbehaltlich § 9 - die gesetzlichen Regelungen.

§ 9 Haftung

1) Die nachstehenden Regelungen beziehen sich auf sämtliche Schadensersatzansprüche des Lizenznehmers, egal aus welchem Rechtsgrund, sei es auf Grund von Verschulden bei Vertragsschluss, sei es auf Grund sonstiger Pflichtverletzungen, deliktischer Handlungen oder sonstiger Tatbestände.

2) Die Intra2net AG haftet in voller Höhe für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer vorsätzlichen oder fahrlässigen Pflichtverletzung der gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

3) Die Intra2net AG haftet in voller Höhe für sonstige Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung ihrer gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

4) Die Intra2net AG haftet in voller Höhe für das Fehlen einer garantierten Beschaffenheit der zugesagten Leistung und für das arglistige Verschweigen eines Mangels.

5) Für die verbleibenden Schäden haftet die Intra2net AG dem Grunde nach bei jeder schuldhaften Verletzung von Kardinalpflichten. Kardinalpflichten sind solche Vertragspflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung Vertragspartner regelmäßig vertrauen dürfen. Der Höhe nach haftet die Intra2net AG in diesen Fällen begrenzt auf den Ersatz der Schäden, die bei Vertragsschluss typisch und vorhersehbar waren.

6) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

7) Im Übrigen ist die Haftung der Intra2net AG ausgeschlossen.

8) Ein Mitverschulden des Lizenznehmers infolge der unzureichenden Erbringung von Mitwirkungsleistungen, der verspäteten Anzeige von Schäden, des Einsatzes nicht freigegebener Software oder aus sonstigen Gründen ist dem Lizenznehmer anzurechnen.

9) Für den Verlust von Daten und/oder Programmen haftet die Intra2net AG insoweit nicht, als der Schaden darauf beruht, dass es der Lizenznehmer unterlassen hat, die erforderlichen Datensicherungen durchzuführen oder regelmäßig die Vollständigkeit der Datensicherungen zu kontrollieren und dadurch sicherzustellen, dass verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

10) Für durch zusätzlich installierte Software verursachte Schäden wird eine Haftung nur bei Lieferung und Installation durch die Intra2net AG übernommen.

11) 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 übernommen. Dies gilt insbesondere bei der Verwendung weiterer Outlook-Plugins und -Addins.

§ 10 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 Programmfunktionen. Mängel, die hierbei festgestellt werden oder feststellbar sind, müssen dem Lizenzgeber innerhalb weiterer acht Werktage 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.

§ 11 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 Lizenz-

gebers erklärt, sind sie nur dann verbindlich, wenn der Lizenzgeber hierfür seine schriftliche Zustimmung erteilt.

§ 12 Rechtswahl

Die Parteien vereinbaren im Hinblick auf sämtliche Rechtsbeziehungen aus diesem Vertragsverhältnis die Anwendung des Rechts der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

§ 13 Gerichtsstand

Sofern der Lizenznehmer Kaufmann im Sinne des Handelsgesetzbuchs, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder keinen Gerichtsstand im Inland hat wird für sämtliche Streitigkeiten, die im Zusammenhang mit der Begründung, Durchführung und Beendigung dieses Vertragsverhältnisses entstehen, Stuttgart als Gerichtsstand vereinbart.

§ 14 Salvatorische Klausel

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.

EULA Version 2.2 vom 30. November 2022

B.2. Lizenzierte Software

Teile des Intra2net Groupware Clients unterliegen anderen Lizenzen. Fordern diese Lizenzen eine Nennung in der Dokumentation, finden Sie diese im folgenden Abschnitt.

B.2.1. Info-ZIP

Copyright © 1990-1999 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution.

3. Altered versions -- including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions -- must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases -- including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip", "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "WiZ", "Pocket UnZip", "Pocket Zip" and "MacZip" for its own source and binary releases.

Der Intra2net Groupware Client enthält angepasste (*"altered"*) Teile des Programmcodes von Info-ZIP.

B.2.2. JsonCpp

The JsonCpp library's source code, including accompanying documentation, tests and demonstration applications, are licensed under the following conditions:

Baptiste Lepilleur and The JsonCpp Authors explicitly disclaim copyright in all jurisdictions which recognize such a disclaimer. In such jurisdictions, this software is released into the Public Domain.

In jurisdictions which do not recognize Public Domain property (e.g. Germany as of 2010), this software is Copyright © 2007-2010 by Baptiste Lepilleur and The JsonCpp Authors, and is released under the terms of the MIT License (see below).

In jurisdictions which recognize Public Domain property, the user of this software may choose to accept it either as 1) Public Domain, 2) under the conditions of the MIT License (see below), or 3) under the terms of dual Public Domain/MIT License conditions described here, as they choose.

The full text of the MIT License follows:

Copyright © 2007-2010 Baptiste Lepilleur and The JsonCpp Authors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR

OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Index

A

ACME-Protokoll, 59-60
Active Directory
  Empfängeradressprüfung, 96-98
  Softwareverteilung, 148-149
  Zertifikate verteilen, 58
ADSL, 63
Android
  VPN Client, 310-317
Anti-Virus
  E-Mail, 106
  Proxy, 78
Appliance
  Eco, 8
  Micro, 8
  Pro, 8-9
ARP
  Proxy, 68-69
Auslieferungszustand
  Zurücksetzen in, 38
Ausschalten, 42
  zeitgesteuert, 140
Ausweichen
  auf anderen Provider, 70

B

Backup
  Auslagern, 134
  Erstellen, 132-133
  Rücksichern, 134, 196
  von anderer Version, 134
BADMAC, 270
Bandbreitenmanagement, 70-72
Benutzer
  Gruppe, 85
  Import und Export, 87
  Rechte, 85-86
Benutzerkonto
  gemeinsam genutzt, 207-208
Bereich, 51
BIOS
  Einstellungen, 3-5
  zeitgesteuertes Einschalten, 140

C

Catch-All-Konto, 92-95
Certificate Authority (CA), 59-61, 280-281
Cold-Standby-System, 137

D

Daten, bestehende importieren, 156-160
Datenschutz
  Statistik, 84
De-Militarized Zone (DMZ), 66-69
Demomodus, 40
DHCP, 50
  Pool, 51
DiffServ, 72
DKIM, 108-115
  Header, 109
  Konfiguration, 110-112
  Wege zur Signatur, 109-110
DMARC, 109
DNS, 45-49
  Firewall, 265
  Rebind, 47-49
  Weiterleitung, 46-49
Domain, 45-49
DSL-Modem, 63
DynDNS, 73-74

E

E-Mail
  Abwesenheitsschaltung, 100
  Adressen, 99
  Alias, 99
  Anhangfilter, 106-108
  Antivirus, 106
  Archivierung
    MailStore Server, 117-124
    Schnittstelle, 116-117
  Automatischer Transfer, 124
  DKIM, 108-115
  DMARC, 109
  Empfängeradressprüfung, 95-98
    Active Directory / LDAP, 96-98
    SMTP, 96
  Externer Servername (EHLO), 89
  Flags, 133
  Gelesen-Status, 176-177
  Größe, 125
  IMAP
    auf dem Intra2net System, 90-91
    Flags, 133
  Kopfzeilen, 195
  Löschen, 101
  Mailinglisten, 124
  POP3
    Abruf und Weiterleiten, 98-99
    Abruf von Provider, 91, 93
    auf dem Intra2net System, 90-91

Postmaster
Adresse, 125
Quelltext, 195
SMTP
Authentifizierung, 86
Empfang, 92-93
Weiterleitung, 95-98
Sortierung, 100
Spamfilter
Benutzerabhängig, 104
Erkennung, 101-102
Glaubwürdige Server, 104-105
Global, 102-103
Punktwerte, 102
Quarantäne, 103
SMTP, 101
Spamverdacht, 102
SPF, 109
Versand
Client, 88
Direkt, 89
Relay-Berechtigung, 86
Relayserver, 88-89
SMTP-Submission, 88
Verteiler, 124
Warteschlange, 125
Weiterleitung
Domain, 95-98
E-Mails eines Benutzers, 99-100
POP-Konten, 98-99
E-Mail-Ordner (IMAP)
freigeben, 175-176
Synchronisationsfrequenz, 185-186
E-Mails
Nachverfolgen, 201
Erinnerungen, 194
Exchange
Migration von, 211-215
Export
Benutzer, 87
Rechner, 51

F

Fallback, 70
Farben zuweisen, 187-190
Fernwartung, 74
Fernzugriff
auf das Intra2net System, 74
Festplattenschaden, 134-136
Firewall
auf virtueller Maschine, 14-16
Automatische Antwortregel, 266
Bedingungen, 266
Blockieren nach Loginfehlern, 270
Dienste, 264
DNS, 265
in VMware vSphere Hypervisor, 22-25
IPs eintragen, 264
MACs überprüfen, 270
Netzgruppen, 264
Notmodus, 37, 270
Ports eintragen, 264
Regellisten
Auswahl, 259-261
Einfache Profile, 262-263
Internet, 259
LAN, 259
Vollständige, 264-269
Routing, 52
vor dem Intra2net System, 138-139
Free-/Busy, 191-193
Frei-/Gebucht, 191-193
Freigeben
von E-Mail-Ordnern (IMAP), 175-176
Fremde Ordner
Erinnerungen, 194

G

Groupware-Daten
bestehende importieren, 156-160

H

Haftung, 1
Hardware
kompatible, 3
Tausch oder Defekt, 134-136
Hauptseite, 40-42
übers Internet erreichen, 74
Herunterfahren, 42
zeitgesteuert, 140
Hot-Standby-System, 138

I

ibx_sub, 185
IKE, 278
IMAP
auf dem Intra2net System, 90-91
IMAP-Ordner
freigeben, 175-176
Synchronisationsfrequenz, 185-186
Import
Benutzer, 87
bestehender Groupwaredaten, 156-160
Rechner, 51

Installation
auf Microsoft Hyper-V, 27-35
auf VMware vSphere Hypervisor, 17-26
von DVD, 6
von USB-Stick, 5-6
Internet
Verbindungsaufbau, 69
Verbindungsüberwachung, 70
Internet-Tachometer, 41
iOS
VPN Client, 308-309
IP
Bereich, 51
Konfigurieren, 37, 44
offizielle, 66-69
private Netzbereiche, 37
IPSec, 277
Aggressive Mode, 278
Client
Android, 310-321
iOS, 308-309
macOS, 305-307
MacOS X, 298-304
Windows, 291-297
Client anbinden, 282-290
dynamische IP, 322
Logs, 354-356
Main Mode, 278
Mode Config, 289
NAT, 349-353
Netz-zu-Netz, 322-324
Perfect Forward Secrecy (PFS), 278-279
Pre-Shared Key, 277
Quick Mode, 278
Verbindungsphasen, 278
Vergleich mit WireGuard, 360-362
Verschlüsselungsalgorithmen, 278-279
Virtuelle IP, 289
XAUTH, 288
Zertifikate, 280-281
IPSecuritas
VPN Client, 298-304
ISAKMP, 278

K

Kabelanschluss, 64
Kabelmodem, 64
Kategorien, 187-190
Kompatibilitätsliste, 3
Konfiguration
bei Auslieferung, 2
Konflikt, 42
Überprüfung, 42
Zurücksetzen, 38
Konsole, 36
serielle, 6-7, 36

L

Lancom
VPN-Verbindungen, 335-344
LDAP
Empfängeradressprüfung, 96-98
Let's Encrypt, 59-60
Linux
Shell, 38-39
VPN, 345-348
Lizenz
Ablauf, 130
Code Eingeben, 130
Demomodus, 130
Groupware Client, 393-397
Intra2net, 384-390
Open Source, 390-391
Lizenzcode, 40
Logdateien
Proxy, 79
System, 140
Loginfehler
IPs blockieren, 270

M

MAC
Firewall, 270
hinterlegen, 49
MailStore Server, 117-124
Microsoft Exchange
Migration von, 211-215
Migration
von Microsoft Exchange, 211-215
Mulitdrop, 92-95

N

Nachverfolgen-Funktion, 201
NAT
für VPNs, 349-353
Masquerading (N:1), 73
statisch (1:1), 67-68
VPN-Gegenseite, 289
NCP
Secure Android Client Premium, 318-321
Secure Entry macOS Client, 305-307
Secure Entry Windows Client, 291-294
Netzwerkkarte, 36-37, 44
Typ, 37, 44

NTP, 128

O

Openswan, 345-348
Ordner
  eigene verbinden, 170-171
  freigeben, 175-176
  gemeinsame verbinden, 173-174
  öffentliche, 207-208
  Synchronisationsfrequenz, 185-186
  von der Synchronisation ausschließen, 171-172
Ordnerliste
  aktualisieren, 172-173
Outlook konfigurieren, 150-152
Outlook-Profile, 150-152

P

Passwort
  Administrator, 2
  root, 38
Perfect Forward Secrecy (PFS)
  IPSec, 278-279
  SSL/TLS, 61-62
POP3
  Abruf und Weiterleiten, 98-99
  Abruf von Provider, 91, 93
  auf dem Intra2net System, 90-91
  Sammelkonten (Multidrop, Catch-All), 92-95
Postmaster
  Adresse, 125
PPPoE, 63
  Passthrough, 63
PPTP, 63
Pre-Shared Key, 277, 358
Privat-Kennzeichnung, 193-194
Proxy
  Antivirus, 78
  Port, 75
  Profile, 76
  Protokollierung, 79
  Statistik, 79-80
  Transparent, 75-76
  URL-Filter, 76-77
  Web-Content-Filter, 77-78
  Zeitsteuerung, 77
  Zielports, 76
  Zugriffslisten, 76-77
Proxy-ARP, 68-69

Q

Quality-of-Service (QoS), 70-72

R

RAID
  Hardware, 5
  Software, 5
Rechner
  eintragen, 49-50
  Import und Export, 51
Rechte
  Benutzer, 85-86
  Netzwerkobjekt, 45
Registry, 222-233
Rettungssystem, 132
root-Passwort, 38
Router, 63-65
Routing
  DMZ, 66-69
  Internet, 63-65
  LAN, 51-52

S

Searchindexer, 154-155
Serielle Konsole, 6-7
Shrew Soft
  VPN Client für Windows, 295-297
SMTP
  Authentifizierung, 86
  Empfang, 92-93
  Empfängeradressprüfung, 96
  Versand
    Direkt, 89
    Relayserver, 88-89
  Weiterleitung, 95-98
SNMP, 128-129
Spamfilter
  Benutzerabhängig, 104
  Erkennung, 101-102
  Glaubwürdige Server, 104-105
  Global, 102-103
  Punktwerte, 102
  Quarantäne, 103
  SMTP, 101
  Spamverdacht, 102
SPF, 109
SSL
  Perfect Forward Secrecy (PFS), 61-62
  Prinzip, 53
  Verschlüsselungsverfahren, 61-62
  Zertifikate, 53-54
Standardeinstellungen, 2
Standby-System, 136-138
  Cold-Standby, 137
  Hot-Standby, 138

Statistik
Datenschutz, 84
Internet, 80-81
Proxy, 79-80
Speicherverbrauch, 84
Tachometer, 81-83
strongSwan, 345-348
Synchronisationsfrequenz
Groupware-Ordner, 185-186

T

TLS
Prinzip, 53
Zertifikate, 53-54

U

Überwachung
SNMP, 128-129
Update
Antivirus, 131
Fernsteuerung über Partnerweb, 131
Neustart, 131
Rettungssystem, 132
Spamfilter, 131
System, 131
URL-Filter, 76-77

V

VDSL, 63
Verbindungsaufbau
ins Internet, 69
über Ersatzprovider, 70
Verbindungsüberwachung, 70
Version, 1
Virenscanner
E-Mail, 106
Proxy, 78
Virtuelle Maschine, 14-35
VLAN
Einwahl mit DSL (PPPoE), 63
VLAN-Tagging, 44-45
VMDirectPath, 22-25
Voice-over-IP (VoIP)
priorisieren, 72
VPN, 277
Adresskonflikt, 349-353
Client anbinden
IPSec, 282-290
WireGuard, 365-366
dynamische IP, 322
FRITZ!Box, 375-380
NAT, 349-353
Netz-zu-Netz, 322-324, 371-374
Vergleich IPSec mit WireGuard, 360-362
WireGuard, 358-360

W

Wake-On-LAN, 50
Web-Content-Filter, 77-78
Weboberfläche
übers Internet erreichen, 74
Werkseinstellungen, 2
WireGuard
Client anbinden, 365-366
Client Installation, 367
FRITZ!Box, 375-380
Grundlagen, 358-360
Interface, 363
Netz-zu-Netz, 371-374
Privater Schlüssel, 363
UDP-Portnummer, 363
Vergleich mit IPSec, 360-362

X

X.509
für IPSec, 280-281
für SSL/TLS, 53-54
XAUTH, 288

Z

Zeitabgleich, 128
Zertifikate
auf Client installieren, 54-58
für IPSec, 280-281
für SSL/TLS, 53-54
mit Active Directory verteilen, 58
Zertifizierungsstelle (CA), 59-61, 280-281
Zwangstrennung, 69
ZyWALL VPN-Router, 325-329