NCP
SECURE COMMUNICATIONS

Secure Linux Client

NCP
SECURE COMMUNICATIONS

Secure Linux Client

Version 2.1
Mai 2004

Copyright

Alle Programme und das Handbuch wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit den Programmen stehen, sind ausdrücklich ausgeschlossen.

Die in diesem Handbuch enthaltene Information kann ohne Vorankündigung geändert werden und stellt keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Ohne ausdrückliche schriftliche Erlaubnis von NCP engineering GmbH darf kein Teil dieses Handbuchs für irgendwelche Zwecke oder in irgendeiner Form mit irgendwelchen Mitteln, elektronisch oder mechanisch, mittels Fotokopie, durch Aufzeichnung oder mit Informationsspeicherungs- und Informationswiedergewinnungssystemen reproduziert oder übertragen werden.

MS-DOS®, Windows®, Windows NT®, Microsoft Accelerator Pack®, Microsoft Internet Explorer® und Microsoft® sind entweder eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation in den USA und/oder anderen Ländern. Alle anderen genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber. © 2005 NCP engineering

Gesamtherstellung dieses Handbuchs:
Michael Lösel
Dokumentation + Publikation
ml-service@t-online.de
Pirckheimerstraße 47
90408 Nürnberg
0172 / 82 58 238

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp.de

NCP Hotline

Die NCP Hotline begleitet Sie mit technischem Sachverstand von der Beratung und Projektierung zur Installation, zum firmenspezifischen Training, bis zum Support in Ihrem Anwendungsumfeld.

Für eine umfassende Betreuung der NCP-Produkte im täglichen Einsatz bietet NCP Support von Montag bis Freitag, von 8:00 bis 17:00, der per Fax oder E-Mail kostenlos erreichbar ist, via Telefon per Dienstleistungsauftrag (siehe unten).

Service-Verträge werden nach Produkt-Gruppen abgeschlossen und umfassen alle dazugehörigen Produkte. Detaillierte Auskünfte zu Service-Verträgen erteilen NCP-Mitarbeiter unter: 09 11 / 99 68-0

Dienstleistungsauftrag nach Aufwand

Auch ohne Service-Vertrag können Sie Dienstleistungen von NCP in Anspruch nehmen. Allerdings nur in beschränktem Umfang und nach einer schriftlichen Auftragserteilung Ihrerseits. In diesem Falle werden die von NCP erbrachten Leistungen nach Aufwand in Rechnung gestellt.

Software Downloads und Auskünfte

Software Downloads und Informationen sind unter der Homepage von NCP erhältlich:
http://www.ncp.de
FTP-Server: ftp://ftp.ncp.de

Inhalt

1. Produktübersicht 13
1.1 NCP Secure Communications – Produktpalette 14
Die Leistungen im Überblick 15
1.2 Security Management 16
Zentrale Anforderungen an eine Security-Architektur 16
1.2.1 Standard Security 17
Personal Firewall 17
1.2.2 Advanced Security 18
Virtual Private Network 18
1.2.3 Strong Security 19
Public Key Infrastruktur 19
Smart Card 19
1.3 NCP Secure Communications – Einzelne Komponenten 21
1.3.1 NCP Secure Access-Komponenten 22
Access Server (Standard Security) 22
Access Client (Standard Security) 22
1.3.2 NCP Secure VPN-Komponenten 23
VPN Gateway (Advanced Security) 23
VPN Client (Advanced Security) 23
1.3.3 NCP Secure VPN/PKI-Komponenten 24
VPN/PKI Gateway (Strong Security) 24
VPN/PKI Client (Strong Security) 24
1.3.4 NCP Secure High Availability Services 25
NCP Failsafe Server (FS Server) 25
NCP Load Balancing Server (LB Server) 25
1.3.5 NCP Secure Administration Tools 26
NCP Secure Server Manager 26
NCP Secure Client Manager 26
NCP High Availability Manager (HA Manager) 27
NCP Secure Update Server 27
NCP Secure PKI Manager 27
1.3.6 Line Management 28
Gebührenmanagement 28

2. Installation 29
2.1 Installationsvoraussetzungen 30
Betriebssystem 30
Zielsystem 30
Lokales System 30
Voraussetzungen für die Strong Security-Version 32
2.2 Script-gesteuerte Installation 35
Installation vorbereiten 35
Install-Script aufrufen 35
Install-Script abarbeiten 35

Installationsroutine 36
2.2.1 Neuinstallation 37
2.2.2 Update 37
2.2.3 Unbeaufsichtigte Installation 37
2.2.4 Installation abschließen 37
2.3 Die installierten Dateien 38
2.4 Grundkonfiguration 39
2.5 Freischalten einer Vollversion 40
Lizenzierung mit ncplic 40
2.6 Deinstallation 41
2.7 Assistent für erste Konfiguration 42
2.8 Start des Linux Clients 43
2.9 Tests des Clients 44
2.9.1 Test Verbindung (testet ISDN, Modem, GSM) 45
2.9.2 Test Verbindung L2TP (testet L2TP-Protokoll) 45
2.9.3 Test Verbindung SSL (testet SSL-Verschlüsselung und Zertifikat) . 45
2.9.4 Test Verbindung IPSec (testet IPSec over L2TP mit Preshared Key) 46
2.9.5 Testen mit Ping 46
2.9.6 Testen mit FTP 47
2.9.7 Testen der Web-Funktionalität 47
2.8 Verzeichnisstruktur NCP Secure Linux Client 48

3. Client Monitor 53
3.1 Die Oberfläche des Client Monitors 54
3.1.1 Bedien- und Anzeigefelder 54
3.1.2 Das Erscheinungsbild des Monitors 54
3.1.3 Statusanzeigen 55
3.1.4 Anwahl und Auswahl des Zielsystems 56

4. Das Monitor-Menü 57
4.1 Verbindung 58
4.1.1 Verbinden 59
4.1.2 Trennen 59
4.1.3 HotSpot-Anmeldung 59
4.1.4 Verbindungs-Informationen 60
Verbindungszeit 60
Timeout 60
Richtung 60
Durchsatz 60
Verbindungsart 61
Multilink 61
Kompression 61
Verschlüsselung 61
Schlüsselaustausch 61
Rx und Tx Bytes 61
1.4.5 Zertifikate |Verbindung 62
Aussteller-Zertifikat anzeigen 63
Benutzer-Zertifikat anzeigen 63
Eingehendes Zertifikat anzeigen 64

CA-Zertifikate anzeigen . . . 64
Anzeige und Auswertung von Erweiterungen . . . 64
Anzeige der Erweiterungen (Extensions) . . . 65
Auswertung der Erweiterungen (Extensions) . . . 66
HTTP Proxy für CRL Download . . . 67
Auswertung von CRLs und ARLs . . . 67
Hardware-Zertifikat . . . 67
4.1.6 PIN eingeben . . . 68
4.1.7 PIN zurücksetzen . . . 69
PIN-Status im Client Monitor . . . 69
PIN-Eingabezwang nach Abmeldung oder Sleep-Mode . . . 69
Anzeige der Meldungen des ACE-Servers für RSA-Token . . . 69
4.1.8 PIN ändern (für Smart Cards und Soft-Zertifikate) . . . 70
4.1.9 Parametersperre aufheben . . . 71
4.1.10 Beenden (des Monitors) . . . 71
4.2 Konfiguration . . . 72
4.2.1 Telefonbuch . . . 73
4.2.2 IPSec . . . 78
4.2.3 Firewall-Einstellungen . . . 80
Eigenschaften der Firewall . . . 81
Konfiguration der Firewall-Einstellungen . . . 81
Konfigurationsfeld Grundeinstellungen . . . 82
Firewall deaktiviert . . . 83
Gesperrte Grundeinstellung (empfohlen) . . . 83
Offene Grundeinstellung . . . 83
Konfigurationsfeld Firewall-Regeln . . . 84
Erstellen einer Firewall-Regel . . . 84
Firewall-Regel / Allgemein . . . 85
Firewall-Regel / Lokal . . . 87
Firewall-Regel / Remote . . . 88
Konfigurationsfeld Bekannte Netze . . . 90
Konfigurationsfeld Optionen . . . 91
Konfigurationsfeld Protokollierung . . . 92
4.2.3 Amtsholung . . . 94
4.2.4 Zertifikate |Konfiguration . . . 95
Benutzer-Zertifikat . . . 96
Zertifikat . . . 96
Chipkartenleser . . . 97
Port . . . 98
Auswahl Zertifikat . . . 98
PKCS#12-Dateiname . . . 98
PKCS#11-Modul . . . 99
Verbindungsabbau bei gezogener Chipkarte . . . 100
PIN-Abfrage bei jedem Verbindungsaufbau . . . 100
Softzertifikatsauswahl aktivieren . . . 100
Zertifikatspfad . . . 100
PIN-Richtlinie . . . 101
Zertifikatsverlängerung . . . 101
Gültigkeitsverlängerung über Update Server . . . 101

Hardware-Zertifikat . . . 102
4.2.5 EAP-Optionen . . . 103
4.2.6 Letzte Konfiguration laden . . . 104
4.2.7 Telefonbuch-Sicherung . . . 105
4.3 Log . . . 106
4.4 Fenster . . . 108
4.4.1 Zielauswahl anzeigen . . . 108
4.4.2 Button-Leiste anzeigen . . . 109
4.4.3 Statistik anzeigen . . . 109
4.4.4 Beim Schließen minimieren und Beenden des Monitors . . . 110
4.4.5 Nach Verbindungsaufbau minimieren . . . 110
4.4.6 Sprache . . . 110
4.5 Hilfe . . . 110

5. Konfigurationsparameter . . . 111
Ordnungsprinzip der Parameter . . . 112
5.1 Telefonbuch . . . 113
5.1.1 Zielsystem . . . 114
Name des Zielsystems . . . 115
Verbindungsart . . . 115
ISDN . . . 115
Modem . . . 115
LAN (over IP) . . . *115*
PPP over Ethernet . . . 115
xDSL (AVM - PPP over CAPI) . . . 115
GPRS / UMTS . . . 116
PPTP . . . 116
Diesen Telefonbucheintrag nach jedem Neustart des Systems verwenden116
5.1.2 Netzeinwahl . . . 117
Benutzername . . . 118
Passwort . . . 118
Passwort speichern . . . 118
Rufnummer (Ziel) . . . 118
Alternative Rufnummern . . . 119
5.1.3 Modem . . . 120
Anschluss . . . 121
Baudrate . . . 121
Com Port freigeben . . . 121
Modem . . . 121
Modem Init. String . . . 122
Dial Prefix . . . 122
APN . . . 122
SIM PIN AT-Befehl . . . 122
SIM PIN . . . 122
5.1.4 Verbindungssteuerung . . . 123
Verbindungsaufbau . . . 124
IP-Adr. halten bei manuellem Verbindungsaufbau . . . 124
Bei Booten verbinden . . . 125
Timeout . . . 125

Timeout-Richtung . . . 125
Kompression . . . 126
Dynamische Linkzuschaltung (Nur für ISDN) . . . 126
Schwellwert für Linkzuschaltung (Nur für ISDN) . . . 126
OTP-Token . . . 127
5.1.5 Rückruf . . . 128
Rückruf für ausgehende Verbindungen (Zielsystem ruft zurück) 129
Rückrufnummer . . . 129
Verhandle PPP Callback . . . 130
Rückruf für eingehende Verbindungen . . . 130
Rückrufmodus . . . 130
5.1.6 Eingehende Rufe . . . 132
Richtung . . . 133
Benutzername der Gegenstelle . . . 133
Passwort der Gegenstelle . . . 133
Rufnummer lokal . . . 134
gegenseitige Authentisierung . . . 134
5.1.7 Security . . . 136
Security-Modus . . . 138
Verschlüsselung |Security . . . 138
Index |Security . . . 138
Statischer Schlüssel |Security . . . 139
Preshared Key |Security . . . 139
Dateiname |Security . . . 139
IKE-Richtlinie |Security . . . 139
IPSec-Richtlinie |Security . . . 140
Austausch-Modus |Security . . . 141
IKE ID-Typ |Security . . . 141
IKE ID |Security . . . 141
5.1.8 Link Einstellungen . . . 142
IP Network Address Translation . . . 143
Erlaube eingehende IP-Verbindungen . . . 143
IP Broadcast erlaubt . . . 143
SPX Spoofing . . . 144
Aktiviere IPX/SAP Spoofing . . . 144
Deaktiviere IPX-Protokoll . . . 144
Erlaube NetBios over IP . . . 144
MAC-Adresse . . . 145
5.1.9 Tunnel – Parameter . . . 146
VPN-Protokoll . . . 147
VPN-Benutzername . . . 148
VPN-Passwort . . . 148
Tunnel Secret . . . 148
Tunnel-Endpunkt (Ziel) . . . 148
Tunnel-Endpunkt (Lokal) . . . 149
Verwende VPN-Benutzername und -Passwort von . . . 149
5.1.10 VPN IP-Netze . . . 150
VPN IP-Netzwerke . . . 151
VPN IP-Netzmasken . . . 151

Auch lokale Netze im Tunnel weiterleiten . . . 151
5.1.11 IPSec-Optionen . . . 152
Private IP-Adresse . . . 153
Destination IPSec Gateway . . . 153
5.1.12 HA-Unterstützung . . . 154
Aktivierung . . . 155
Erster / Zweiter HA-Server . . . 155
DVE Secret . . . 155
Zuletzt zugewiesenes Gateway benutzen . . . 155
5.1.13 DNS / WINS . . . 156
DNS-Server . . . 157
WINS-Server . . . 157
Management Server . . . 157
Domain Name . . . 157
5.1.14 X.31 . . . 158
Übertragungskanal . . . 159
Präferenz . . . 159
X.25 Link-Protokoll . . . 160
X.25 Window Size . . . 160
TEI-Wert . . . 160
5.1.15 Zertifikats-Überprüfung . . . 161
Benutzer des eingehenden Zertifikats . . . 162
Aussteller des eingehenden Zertifikats . . . 162
Fingerprint des Aussteller-Zertifikats . . . 163
Benutze SHA1 Fingerprint statt MD5 . . . 163
5.1.16 Link Firewall . . . 164
Aktivierung (der Firewall) . . . 165
Ausschließlich Kommunikation im Tunnel zulassen . . . 165
5.2 IPSec . . . 167
5.2.1 IKE-Richtlinie (Allgemein / Vorschläge) . . . 168
Name | IKE-Richtlinie . . . 170
Art der Gültigkeit | IKE-Richtlinie . . . 170
Dauer | IKE-Richtlinie . . . 170
kBytes | IKE-Richtlinie . . . 170
Authentisierung | IKE-Richtlinie . . . 170
Verschlüsselung | IKE-Richtlinie . . . 171
Hash | IKE-Richtlinie . . . 171
DH-Gruppe | IKE-Richtlinie . . . 171
5.2.2 IPSec-Richtlinie (Allgemein / Vorschläge) . . . 172
Name | IPSec-Richtlinie . . . 174
Art der Gültigkeit | IPSec-Richtlinie . . . 174
Dauer | IPSec-Richtlinie . . . 174
kBytes | IPSec-Richtlinie . . . 174
Protokoll | IPSec-Richtlinie . . . 174
Transformation (ESP) | IPSec-Richtlinie . . . 174
Transformation (Comp) | IPSec-Richtlinie . . . 174
Authentisierung (nur ESP) | IPSec-Richtlinie . . . 175
DH-Gruppe | IPSec-Richtlinie . . . 175
Secure Policy Database | IPSec . . . 176

Allgemein | SPD (5.2.3) . . . 176
Selektoren | SPD (5.2.4) . . . 176
Authentisierung | SPD (5.2.5) . . . 176
Security | SPD (5.2.6) . . . 176
Tunnel | SPD (5.2.7) . . . 176
5.2.3 Allgemein | SPD . . . 177
Name | SPD . . . 178
Ausführung | SPD . . . 178
Richtung | SPD . . . 178
5.2.4 Selektoren | SPD . . . 179
IP-Protokoll | SPD . . . 180
IP-Adresse (Quelle) | SPD . . . 180
IP-Adresse (Ziel) | SPD . . . 180
Port (Quelle) | SPD . . . 180
Port (Ziel) | SPD . . . 180
5.2.5 Authentisierung | SPD . . . 181
Art der ID (Ausgehende / Eingehende Verbindung) | SPD . . . 182
ID String (Ausgehende / Eingehende Verbindung) | SPD . . . 182
5.2.6 Security | SPD . . . 183
IKE-Richtlinie | SPD . . . 184
IPSec-Richtlinie | SPD . . . 184
Statischer Schlüssel | SPD . . . 184
Austausch-Modus | SPD . . . 185
5.2.7 Tunnel | SPD . . . 186
Modus | SPD . . . 187
IPSec-Endpunkt (Ziel) | SPD . . . 187
IPSec-Endpunkt (lokal) | SPD . . . 187

6. Eine Verbindung herstellen . . . 189
Verbindungsaufbau zum Zielsystem . . . 189
Verbinden . . . 189
Passwörter und Benutzernamen . . . 192
Benutzername für NAS-Einwahl . . . 192
Benutzername und Passwort für VPN-Einwahl . . . 193
Passwort für OTP-Token . . . 193
Verbindungsabruch und Fehler . . . 194
Trennen . . . 194

7. Beispiele und Erklärungen . . . 195
7.1 IP-Funktionen . . . 196
7.1.1 Geräte eines IP-Netzwerks . . . 196
7.1.2 IP-Adress-Struktur . . . 196
7.1.3 Netzmasken (Subnet Masks) . . . 198
7.1.4 Zum Umgang mit IP-Adressen . . . 200
7.2 Security . . . 201
7.2.1 Verschlüsselungsart L2Sec nach RFC 2716 . . . 202
L2Sec – Funktionsbeschreibung . . . 203
7.2.2 IPSec – Übersicht . . . 205
IPSec – Funktionsbeschreibung . . . 206

IPSec-Dienste . . . 208
IPSec-Richtlinien / IPSec Policy . . . 208
AH und ESP im Transport- und Tunnelmodus . . . 209
7.2.3 Anwendungen . . . 211
7.2.4 Secure Policy Database – Datenbank der Sicherheits-Richtlinien . 212
Sicherheits-Verknüpfung (Security Association / SA) . . . 213
Selektoren (der statischen SPD) . . . 215
7.2.5 SA-Verhandlung und Richtlinien / Policies . . . 216
Phase 1 (Parameter der IKE-Richtlinie / IKE Policy): . . . 216
Phase 2 (Parameter der IPSec-Richtlinie / IPSec Policy): . . . 216
IKE-Modi . . . 218
7.3 IPSec für Remote Access – IPSec over L2TP . . . 220
7.4 Verbindungen über das Tunnelprotokoll “IPSec Tunneling” . . . 222
Implementierte Algorithmen für Phase 1 und 2: . . . 222
Standard IKE-Vorschläge: . . . 224
Zur Konfiguration des VPN-Protokolls “IPSec Tunneling” . . . 226
7.5 Sichere End-to-End-Kommunikation auch ohne feste offizielle IP-Adresse 228
7.5.1 Lockruf . . . 229
Zur Konfiguration . . . 229
7.5.2 Dynamic DNS . . . 230
Zur Konfiguration . . . 230
7.5.3 Managed VPNs . . . 233
Zur Konfiguration . . . 233
7.5.4 Szenarien in Internet-VPNs . . . 234
7.5 Rückruf . . . 235
7.5.1 Rückruf des Zielsystems an den Secure Client . . . 235
7.5.2 Rückruf des Secure Client an das Zielsystem . . . 236
7.6 Parallele Verbindungen ins Internet und zu einem VPN IP-Netz . . . 238
Parameterfeld Tunnel-Parameter . . . 238
Parameterfeld VPN IP-Netze . . . 238
Parallele Verbindungen ins Internet und zu einem VPN IP-Netz 239
7.8 Zertifikats-Überprüfungen . . . 240
7.8.1. Auswahl der CA-Zertifikate . . . 240
7.8.2. Überprüfung der Zertifikats-Erweiterung . . . 240
KeyUsage . . . 241
extendedKeyUsage . . . 241
subjectKeyIdentifier / authorityKeyIdentifier . . . 241
CDP (Certificate Distribution Point) . . . 241
7.8.3. Überprüfung von Sperrlisten . . . 242
7.9 Stateful Inspection-Technologie für die Firewall-Einstellungen . . . 243

8. Abkürzungen und Begriffe . . . 247

9. Fehler- und ISDN-Meldungen . . . 261

10. Index . . . 269

1. Produktübersicht

Dieses Handbuch beschreibt Installation, Konfiguration, Leistungsumfang und Benutzeroberfläche der Secure Communications-Komponenten:

- **NCP Secure Linux Client**
- **NCP Secure Linux Client Monitor**

Der NCP Secure Client ist je nach Security-Stufe in folgenden Varianten erhältlich:

- ☐ Standard Security: NCP Access Client
- ☐ Advanced Security: NCP VPN Client
- ☐ Strong Security: NCP VPN/PKI Client

Die NCP Secure Client Software arbeitet nach einer LAN Emulation für Ethernet und unterstützt die routbaren Protokolle TCP/IP und IPX/SPX.

Die Client Software (für ISDN) wurde für den Einsatz mit den D-Kanal-Protokollen DSS1 und 1TR6 getestet. Darüber hinaus unterstützt sie jedoch auch andere D-Kanal-Protokolle, wie VN3/4, NT1, CT1, 5ESS, Austel, usw.

Weitere Informationen zu Ausbaustufen und Produktvarianten erhalten Sie auf der NCP Website: http://www.ncp.de

1.1 NCP Secure Communications – Produktpalette

Mit NCP Secure Communications verfügen Sie über ein vollständiges Portfolio an Produkten für die Implementierung hochsicherer Remote Access-Komplettlösungen. NCP Secure Communications Software entspricht den aktuellsten, von IETF (Internet Engineering Task Force) und ITU (International Telecommunication Union) verabschiedeten Standards für Kommunikations- und Verschlüsselungstechnologien. Alle Produkte fügen sich damit vollständig in bestehende Hard- und Softwarearchitekturen ein. Das Internetworking-Umfeld, in dem sich bereits Security- und Access-Komponenten von Drittanbietern in Betrieb befinden, kann unverändert weiter genutzt werden – es fallen keine administrativen Kosten an.

NCP Secure Communications setzt konsequent auf eigenentwickelte Software. Alle Client- und Server-seitigen Produkte sind für Rechner mit Standardbetriebsystem verfügbar. Anwender und Netzwerkadministratoren bewegen sich mit NCP Secure Communications somit in einem vertrauten Umfeld – entsprechend einfach und übersichtlich gestalten sich Installation, Administration und Bedienung der Komponenten.

NCP SECURE COMMUNICATIONS

NCP Secure Client	NCP Secure Server	NCP Administration Tools	NCP High Availability Services
Secure Access Client	Secure Access Server	Secure Client Manager	Secure Failsafe Server
Secure VPN Client	Secure VPN Gateway	Secure Server Manager	Secure Load Balancing Server
Secure VPN/PKI Client	Secure VPN/PKI Gateway	Secure HA Manager	
		Secure Update Server	
		Secure PKI Manager	

Produktübersicht

© NCP engineering GmbH

Die Leistungen im Überblick

- ☐ Flexibler Zugriff auf zentrale Datenbestände und Ressourcen von beliebigen, globalen Standorten aus, über alle öffentlichen Netze
- ☐ Intelligentes Verbindungsmanagement zur schnellen, kostengünstigen Datenübertragung
- ☐ Leistungsfähige Encryption mit Schlüssellängen von bis 448 Bit (symmetrisch) und 2048 Bit (asymmetrisch)
- ☐ Interoperabilität mit allen Mitbewerberprodukten auf der Basis internationaler Standards
- ☐ Leistungsstarke Administrations-Tools für Fernwartung und Konfigurationsoptimierungen beim Roll-out
- ☐ Unterstützung der marktgängigen VPN-Tunneling-Verfahren L2TP und IPSec
- ☐ Unterstützung von Remote Access-optimierten VPN-Varianten: L2Sec, IPSec over L2TP
- ☐ PKI-Support in beliebigen Umgebungen: Unterstützung unterschiedlicher Smart Cards, Kartenleser und Trust Center.

1.2 Security Management

NCP Secure Communications bietet ein dreistufiges, modulares Security Management. Ändern sich die Security-Anforderungen Ihres Unternehmens, so ist per Software-Update eine einfache Migration auf die nächst höhere Security-Stufe möglich.

Zentrale Anforderungen an eine Security-Architektur

- ☐ Verifizieren der Identität aller Kommunikationsteilnehmer
- ☐ Sicherung der Vertraulichkeit der übertragenen Daten
- ☐ Sicherung der Integrität aller übermittelten Daten
- ☐ Zugriffskontrolle auf Clients und Server
- ☐ Sicherung der Clients gegen Angriffe aus dem Internet

Ergänzend zu den Sicherheitsmechanismen für Kommunikation bietet NCP mit der Ausfallsicherung der zentralen Gateways eine zusätzliche Security-Funktionalität. Mit den High Availability Services wird die permanente Verfügbarkeit aller zentralen Gateways durch gleichmäßige Auslastung und automatisches Back-Up im Servicefall sichergestellt.

1.2.1 Standard Security

Der Leistungsumfang der Standard Security ist im Lieferumfang aller NCP-Remote Access-Komponenten enthalten:

- ☐ Anruferidentifikation im ISDN – Calling Line Identification (CLI)
- ☐ Callback
- ☐ Authentifizierung nach CHAP oder PAP (UserID und Passwort)
- ☐ Authentifizierung und Verschlüsselung nach SSL/TLS (RFC 2716) und RFC 2888
- ☐ IP-NAT (Network Address Translation), Personal Firewall
- ☐ Protokollfilter
- ☐ Datenverschlüsselung (Triple-DES, Blowfish, AES, RSA)

■ **Personal Firewall**

Damit jeder Telearbeitsplatz gegenüber Angriffen aus dem Internet geschützt ist, beinhaltet das Security Management eine Personal Firewall-Software. Die wesentlichen Security-Mechanismen sind IP-NAT und Protokollfilter. NAT (Network Address Translation) ist ein Security-Standard zum Verbergen der individuellen IP-Adressen gegenüber dem Internet. NAT bewirkt eine Übersetzung der von außen sichtbaren Adresse in entsprechende Client-Adressen und umgekehrt. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filterings nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.

1.2.2 Advanced Security

Die Advanced Security enthält alle Komponenten der Standard Security. Darüber hinaus umfasst die Advanced Security Mechanismen für eine sichere Datenkommunikation über IP-Netze und bahnt so auch den sicheren Weg durch das Internet. VPN-Tunneling schützt den kompletten Übertragungsweg. Zusätzliche Features:

- ☐ Layer 2 Tunneling L2F und L2TP (Layer 2 Forwarding, Layer 2 Tunneling Protocol)
- ☐ Layer 3 Tunneling: IPSec (Internet Protocol Security)
- ☐ SSL over L2TP (L2Sec), IPSec over L2TP
- ☐ Unterstützung von Tokens, Smart Cards und Onetime-Password (OTP)

■ **Virtual Private Network**

Mit der in bestehende WAN-Strukturen (Wide Area Network) integrierbaren NCP VPN-Lösung erhalten Unternehmen geschützte, private Datenverbindungen über öffentliche Wählnetze und das Internet. Virtuelle Standleitungen ersetzen damit teure physikalische Festverbindungen. Alle Daten zwischen den entfernten VPN Clients und dem zentralen VPN Gateway werden End-to-End durch einen hochsicheren, performanten virtuellen Tunnel übertragen. Alle zwischengeschalteten Internetworking-Komponenten der Internet Service Provider (ISPs) und des Unternehmens werden getunnelt.

Mit dem Tunneling-Verfahren L2Sec auf Basis des L2TP-Protokolls hat NCP bereits vor der offiziellen Verabschiedung des IPSec-Standards am Remote Access VPN-Markt Zeichen gesetzt und die Möglichkeit geschaffen, Daten- und Zugangssicherheit auf Layer 2 in einem End-to-End-Tunnel zu garantieren. Die Initialisierung der Verschlüsselung erfolgt bereits beim Aufbau des VPN-Tunnels. Die Implementierung des SSL-Handshake-Protokolls (Secure Socket Layer) steht dabei für die Standardkonformität der NCP-Lösung. Für die Kompatibilität mit Drittherstellern sorgt das IPSec-Protokoll. Auch hier setzt NCP mit einer Eigenentwicklung Maßstäbe.

Die Kombination aller Vorteile des Layer 2 und Layer 3 Tunnelings integriert das Verfahren IPSec over L2TP (RFC 2888): IPSec wird auf diese Weise Remote Access-fähig.

1.2.3 Strong Security

Maximale Sicherheit im Remote Access! Das Modul Strong Security erlaubt die sichere Authentifizierung von Teilnehmern durch strenge Zugangskontrollen auf der Grundlage von Zertifikaten innerhalb einer PKI. Der Teilnehmer authorisiert sich über eine Smart Card oder ein digitales Soft-Zertifikat. Bereits vor der Übermittlung sensitiver Daten geschieht die Kommunikation zwischen Remote-Teilnehmer und dem zentralen Unternehmensnetz über eine sichere Verbindung. Zusätzlich zur Advanced Security verfügt das Strong Security-Modul über:

- ☐ Unterstützung von digitalen Zertifikaten (X.509-Standard)
- ☐ Unterstützung von Smart Cards, Kartenlesern und Tokens
- ☐ Unterstützung von Soft-Zertifikaten

■ **Public Key Infrastruktur**

Public-Key-Infrastrukturen (PKI) beschreiben ein weltweit genutztes Verfahren, um zwischen beliebigen Kommunikationspartnern auf elektronischem Wege Schlüssel sicher auszutauschen. Die PKI bedient sich dabei sogenannter Schlüsselpärchen aus jeweils einem öffentlichen und einem privaten Schlüssel.

In der Welt des elektronischen, globalen Informationsaustausches wird so eine Vertrauensbasis aufgebaut, wie wir sie in der traditionellen Geschäftswelt auf Papierbasis kennen. Die digitale Signatur in Verbindung mit Datenverschlüsselung ist das elektronische Äquivalent zur händisch geleisteten Unterschrift und belegt Ursprung sowie die Authenizität von Daten und Teilnehmer.

Eine PKI basiert auf digitalen Zertifikaten, die – von einer öffentlichen Zertifizierungsstelle (Trust Center) ausgestellt – als persönliche “elektronische Ausweise” fungieren und idealerweise auf einer Smart Card abgespeichert sind. Sicherheitsexperten und der IETF (Internet Engineering Task Force) sind sich darüber einig, dass ein nachhaltiger Schutz vor Man-In-The-Middle-Attacken nur durch den Einsatz von Smart Cards mit Zertifikaten erreicht werden kann.

■ **Smart Card**

Smart Cards sind die ideale Ergänzung für hochsichere Remote Access-Lösungen. Sie bieten doppelte Sicherheit beim Login-Vorgang, nämlich Wissen über PIN (Persönliche Identifikations Nummer) und Besitz der Smart Card. Der Anwender identifiziert sich mit der Eingabe der PIN eindeutig als rechtmäßiger Besitzer (Strong Authentication). Die PIN ersetzt das Passwort und die Eingabe der User-ID (Basistechnologie für Single Sign On). Der Anwender weist sich nur noch gegenüber der Smart Card aus.

Der Check gegenüber dem Netz erfolgt zwischen Smart Card und Security-System. Alle sicherheitsrelevanten Operationen laufen vollständig im Inneren der Karte – also außerhalb des PCs – ab. Das System ist neben individuellen Anpassungen an Schutzmechanismen offen für multifunktionalen Einsatz (z. B. als Company Card). Auch biometrische Verfahren lassen sich integrieren.

© NCP engineering GmbH

1.3 NCP Secure Communications – Einzelne Komponenten

Alle Software-Komponenten verfügen über eine modulare Softwarearchitektur. In Abhängigkeit von den genutzten Übertragungsmedien, Netzwerkprotokollen und gewünschten Sicherheitsmechanismen können Sie Ihre ganz individuelle Remote Access-Lösung zusammenstellen und nach Bedarf ausbauen.

Mit der NCP Client Software dehnen Sie Ihr Intranet auf entfernte Arbeitsplätze aus. Möglich wird dies durch die LAN-Emulation am Telearbeitsplatz. Ihren Remote-Teilnehmern stehen auf diese Weise alle Netzwerkapplikationen und -funktionalitäten am Client-PC zur Verfügung – 1:1 wie am Büroarbeitsplatz in der Zentrale.

Unterstützt werden praktisch alle gängigen Netzwerkprotokolle für Point-to-Point- und Point-to-Multipoint-Verbindungen, so dass im Remote Access neben IP auch IPX, SNA und NetBios genutzt werden können.

Der NCP Secure Client ermöglicht dem entfernten Arbeitsplatz nach jeder Einwahl die gleiche Netzwerkadresse (IP-Adresse) zuzuweisen. Hierbei handelt es sich um eine private IP-Adresse aus dem Adressraum Ihres Unternehmens. Der Remote-Teilnehmer ist – unabhängig vom Standort, von dem aus er sich in das Unternehmensnetz einwählt – immer eindeutig anhand seiner IP-Adresse identifizierbar. Ob auf Vorstandsebene, im Vertrieb oder technischen Außendienst: Accounting und Teilnehmerverwaltung können somit akkurat und bequem auch für die Teilnehmer zentral erfolgen, die häufiger von wechselnden Standorten aus einen Zugriff auf das Firmennetz benötigen. Diese Option einer zentralen Teilnehmerverwaltung und -betreuung über die IP-Adresse wird auch in einem gemischten IPSec-Umfeld (heterogenen Umgebungen) unterstützt.

1.3.1 NCP Secure Access-Komponenten

Die Kommunikationskomponenten für Direkteinwahl über öffentliche Netze sind Access Server und Access Client.

- **Access Server (Standard Security)**

Der NCP Access Server ist der zentrale Baustein für Ihre professionelle Remote-Access-Lösung. Alle ein- und ausgehenden Datenströme zu den angeschalteten dezentralen Unternehmens- und Organisationseinheiten werden von ihm organisiert und überwacht. Die Einwahl in die Firmenzentrale erfolgt direkt über alle öffentlichen Wählnetze. Der NCP Access Server bietet neben Dial-in- auch Dial-out-Funktionalitäten für Softwareverteilung, Fernwartung, etc.

- **Access Client (Standard Security)**

Mit dem NCP Access Client greift der Teleworker auf das zentrale Unternehmensnetz zu. Die Einwahl kann manuell per Mausklick oder aber automatisiert – etwa für einen turnusmäßigen Datenabgleich zwischen Vertriebsmitarbeiter und Zentralrechner – erfolgen. Hierbei unterstützt die NCP Client-Software alle öffentlichen IP-fähigen Netze (z.B. ISDN, GSM, GPRS, PSTN).

Für Sicherheit gegen jegliche Ein- und Angriffe von außen auf die Datenverbindungen sorgen die Sicherheitsmechanismen des Standard Security-Moduls.

1.3.2 NCP Secure VPN-Komponenten

Bei der Einwahl in das zentrale Datennetz via Internet sind neben der Standard Security weitere Sicherheitsfeatures erforderlich. Zielsetzungen sind u.a. die Flexibilität in der Datenkommunikation zu erhöhen und gleichzeitig die Übertragungskosten zu minimieren.

- **VPN Gateway (Advanced Security)**

Die Substitution bisheriger Datenkommunikationsverbindungen über Fest- oder Wählnetze durch das Internet eröffnet heute völlig neue Optionen, um im WAN (Wide Area Network) erhebliche Einsparungen bei den Übertragungskosten zu erzielen. Wirkungsvollen Schutz für Ihre Datenströme garantiert hier das NCP VPN Gateway dank End-to-End-Tunneling in Kombination mit leistungsstarker Verschlüsselung.

Die Tunnelendpunkte befinden sich jeweils im zentralen VPN Gateway und entfernten VPN Client, d.h. im Unternehmensbereich. Vom VPN Gateway werden die Parameter der Datenübertragung bestimmt: das Tunneling-Verfahren, den Schlüsselalgorithmus, das Netzwerkprotokoll, die Datenkompression etc.

Sichere Datenverbindungen dürfen niemals im öffentlichen Bereich enden. Ein VPN Gateway ist deshalb immer hinter dem Access Server und der Firewall zu installieren (RFC 2888).

- **VPN Client (Advanced Security)**

Mit dem NCP VPN Client hat der Remote-Teilnehmer von jedem beliebigen Ort weltweit Zugriff auf das zentrale Firmennetz. Die Einwahl zum nächstgelegenen PoP (Point of Presence) eines Internet Service-Providers kann wahlweise stationär oder mobil über alle öffentlichen Netze (z.B. ISDN, GSM, GPRS, PSTN einschließlich xDSL) erfolgen.

Die NCP Client-Software verfügt über einen eigenen NAT-fähigen Dialer, um während der Remote Sessions das Risiko potenziell erfolgreicher Attacken aus dem Internet auszuschließen. Mit der NCP Client-Software erhält der Remote-Teilnehmer somit – bei maximaler Verbindungssicherheit – mehr Flexibilität und Mobilität als im Rahmen einer alternativen Routerlösung.

VPN Clients können beim End-to-End-Tunneling sowohl Einzelplatz-PCs als auch im LAN vernetzte Rechner sein. Mittels der VPN Client-Software kann in einer LAN-Workstation unabhängig vom eingesetzten Tunneling-Verfahren ein Tunnelende hinter jedem beliebigen IP-Router abgebildet werden. Eine Variante, die ideal geeignet ist für die wirtschaftliche Anbindung vieler kleinerer, dezentraler LANs an das zentrale Datennetz.

1.3.3 NCP Secure VPN/PKI-Komponenten

Höchstmögliche Sicherheit beim Zugriff auf zentrale Netzressourcen gewährleistet die Kombination von VPN End-to-End-Tunneling mit einer Public-Key-Infrastruktur (PKI). Ziel ist es, die User-Authentisierung durch zusätzliche Security-Mechanismen sicherer zu gestalten und einen sicheren Datenaustausch mit Dritten zu ermöglichen. Hierfür ist eine neutrale Zertifizierungsstelle – ein Trust Center – einzuschalten. Auf der Basis einer PKI erfolgt dann die Festlegung aller Security-Mechanismen für eine Kommunikationsverbindung.

- **VPN/PKI Gateway (Strong Security)**

Die End-to-End-Security eines VPNs wird ergänzt durch eine starke Authentisierung aller User in einer Remote Access-Umgebung. Tunnel-Endpunkt auf der zentralen Seite ist das VPN/PKI Gateway. Jeder Remote-Teilnehmer muss sich mittels elektronischem Zertifikat auf der Grundlage asymmetrischer Verschlüsselungsverfahren (Public Key-Verfahren) in einer PKI gegenüber dem VPN/PKI Gateway ausweisen. Die Überprüfung der Zertifikate erfolgt Offline durch Überprüfung der lokal abgelegten Sperrliste oder Online durch Anfrage bei dem zuständigen Trust Center. Hierbei werden alle Daten zwischen dem VPN/PKI Client sowie dem VPN/PKI Gateway in der Unternehmenszentrale End-to-End verschlüsselt übertragen. Die Authentisierung des Remote-Teilnehmers gegenüber dem NCP VPN/PKI Gateway geschieht mittels digitaler Zertifikate auf Grundlage der Verwendung asymmetrischer Verschlüsselungsverfahren.

- **VPN/PKI Client (Strong Security)**

Bei jeder Session werden von Beginn an alle ausgetauschten Daten verschlüsselt und sicher in einem End-to-End-Tunnel übertragen. Jeder Mitarbeiter, der remote tätig ist – ob mobil oder stationär – muss sich am PC-Arbeitsplatz mittels Smart Card oder einem digitalen Soft-Zertifikat gegenüber dem NCP VPN/PKI Gateway identifizieren. Die Zertifikate werden zur sicheren Authentifizierung bei der Etablierung einer Datenverbindung eingesetzt, um einen dynamischen Schlüsselaustausch anzustoßen. Erst die Kombination von Smart Card und PIN gestattet dem Teilnehmer den Zugang zum zentralen Netzwerk des Unternehmens.

1.3.4 NCP Secure High Availability Services

Um Ausfallsicherheit und gleichmäßige Auslastung der Secure Gateways zu gewährleisten, bietet die NCP Remote Access-Komplettlösung zuverlässige Softwarekomponenten. Failsafe Server (FS Server) und Load Balancing Server (LB Server) stellen High Availability Services für ein sicheres Backup eines Gateways und eine gleichmäßige Lastverteilung über mehrere Gateways auf der Basis des Dynamic VPN Endpoint Protokolls (DVEP) zur Verfügung. Sowohl FS Server als auch LB Server sind redundant ausgelegt, hochskalierbar und flexibel an die jeweiligen Gegebenheiten anpassbar. Die Installation der Software kann entweder in NCP Gateways integriert oder dezidiert auf zwei separaten Rechnern (Primary und Secondary System) erfolgen.

- **NCP Failsafe Server (FS Server)**

Beim Betrieb eines NCP VPN Gateways gilt es Ausfallzeiten oder Stillstand zu vermeiden. Für maximale Verfügbarkeit sorgt die Installation eines zweiten VPN-Servers als Backup-System. Die automatische Umschaltung vom Primary System auf das Backup System übernimmt im Störungsfall der NCP Failsafe Server.

- **NCP Load Balancing Server (LB Server)**

Für die Verwaltung von mehreren VPN Gateways bietet NCP den Load Balancing Server. Im Mittelpunkt steht die gleichmäßige Auslastung aller angeschlossenen NCP Security Systeme. Ein fehlerhaftes System wird automatisch aus der Verteilungsroutine ausgeklammert. Die getunnelten Remote Access-Zugänge werden auf die restlichen Gateways verteilt.

Das LB Gateway prüft alle parallel geschalteten VPN Gateways auf deren Verfügbarkeit, augenblickliche Auslastung und Datendurchsatz. Wählt sich ein externer Client in das Netzwerk ein, wird die Verbindung automatisch über das Gateway geleitet, das momentan die geringste Auslastung verzeichnet. Die LB Software-Lösung ist beliebig skalierbar und kann sowohl in kleinen wie in sehr großen VPN-Netzen eingesetzt werden. Pluspunkt: Ein Umkonfigurieren der Client-Software ist nicht erforderlich, Ausfallzeiten bei der Konfiguration oder bei Wartungsarbeiten am System werden vermieden.

1.3.5 NCP Secure Administration Tools

Die NCP Secure Administration Tools sind Werkzeuge für die einfache Integration der NCP High Security Remote Access-Lösung in vorhandene IT-Landschaften. Mit ihrer Hilfe kann im Störungsfall schnell und unkompliziert eine Änderung von Konfigurationsdaten an Remote-Arbeitsplätzen vorgenommen werden. So können neue Konfigurationsdaten, Software-Updates oder Upgrades etc. automatisiert in den Client übernommen werden – ohne Eingriff des Remote arbeitenden Users.

■ NCP Secure Server Manager

Alle NCP Secure Server lassen sich einfach in eine bestehende SNMP-Umgebung integrieren. Die Konfiguration sämtlicher Systeme ist sowohl lokal als auch remote möglich. Alle relevanten Administrationsdaten und Event-Meldungen wie z. B. Netzwerkattacken werden protokolliert und lösen Alarmmeldungen nach vordefinierten Eskalationsstufen aus. Alle relevanten Parameter können auf einem LDAP- oder RADIUS-Server verwaltet werden. Der NCP Server Manager bietet ein komfortables Handling und informiert übersichtlich und schnell durch eine graphische Benutzeroberfläche.

■ NCP Secure Client Manager

NCP Secure Communications verfügen über Werkzeuge zur Vorkonfiguration und Fernadministration sämtlicher Remote-Arbeitsplätze. So lassen sich über den Client-Konfigurationsmanager für jeden Arbeitsplatz alle relevanten Parameter (z.B. IP-Adresse, User-Berechtigungen, User-ID, Passwort, Voreinstellungen von Konfigurationsgrößen am Client Monitor) vor dem Rollout definieren. Sind Konfigurationsparameter schon in Datenbanken vorhanden, können diese Angaben – etwa als Textdatei – in den Client-Konfigurationsmanager eingelesen werden.

Ein weiteres Modul des Client Managers ist eine Fernwartungssoftware – Remote Monitor – zur zentralen Verwaltung von Remote-Arbeitsplätzen. Wichtige Funktionalitäten sind u.a.: Anzeige und Änderungen von Konfigurationen, die Anzeige und Übernahme von Log-Dateien zur Fehleranalyse, die Festlegung von Limits für die Verbindungssteuerung sowie die Anzeige allgemeiner Informationen wie Softwarestand, CAPI-Version, Betriebssystem, etc. Auch diese Daten werden zwischen Remote-PC und Firmenzentrale verschlüsselt übertragen.
Ein zusätzliches Tool des NCP Client Managers sorgt dafür, dass alle Clients immer und überall über die aktuellsten Konfigurationsdaten und Softwarestände verfügen. Updates und Upgrades laufen automatisiert ab. Bei jeder Einwahl werden die vorhandenen mit den auf einem Server abgelegten User-bezogenen Daten verglichen. Abweichungen zwischen den beiden Dateien führen ohne weiteres Zutun des Administrators zu einer Übernahme der jeweils aktuellen Daten bzw. Software durch den Client.

■ NCP High Availability Manager (HA Manager)

Dieses Software-Tool wird immer dann benötigt, wenn es um die Sicherstellung der Verfügbarkeit von VPN und VPN/PKI Gateways in Ihrem zentralen Datennetz geht. Der High Availability Manager dient zur Konfiguration und Administration von Failsafe und Load Balancing Servern. Er arbeitet auf Basis von SNMP (Simple Network Management Protocol) und ist über eine komfortable Windows-Oberfläche bedienbar. Konfigurationsänderungen oder Erweiterungen können sowohl lokal als auch remote vorgenommen werden.

■ NCP Secure Update Server

Der Update Server dient zur Verwaltung von Telefonbucheinträgen (Zielsysteme) und elektronischen Zertifikaten im Rahmen einer PKI. Diese Funktionalität ist sowohl bei Massen-Rollouts als auch im späteren Realbetrieb von Bedeutung. Automatismen reduzieren den administrativen Aufwand sowohl bei der Ersteinwahl als auch bei allen folgenden Einwahlen in das zentrale Datennetz durch selbsttätigen Datenabgleich zwischen Client und Update Server.

■ NCP Secure PKI Manager

Komfortable Software für die Ausstellung und Verwaltung von Zertifikaten (z.B. Erstellen, Sperren, Anzeigen). Der PKI-Manager unterstützt die Nutzung der Technologie und Infrastruktur eines Trust Centers. Er arbeitet mit den CAs (Certification Authorities) aller führenden Hersteller zusammen. Mit dem PKI-Manager kann eine lokale RA (Registration Authority) eingerichtet werden. Die Software ist hochskalierbar und unterstützt die Public Key-Infrastruktur von Firmennetzen mit nur wenigen Anwendern bis hin zu komplexen Netzstrukturen von Großunternehmen, in denen tausende von Smart Cards bzw. Soft-Zertifikate zum Einsatz kommen. Zur User-Verwaltung ist zusätzlich ein LDAP-Server erforderlich.

1.3.6 Line Management

Um eine möglichst schnelle und kostengünstige Übertragung der Datenpakete in öffentlichen Netzen zu gewährleisten, verfügen alle NCP-Lösungen über Automatismen für ein effektives Line Management wie z. B. Timeout (Short Hold), Kanalbündelung (Channel Bundling), Datenkompression, Filtering sowie Spoofing und Local Termination.

- **Gebührenmanagement**

Für optimierte Kostentransparenz und mehr Übersicht sorgt das Gebührenmanagement: Es erlaubt dem Systemadministrator die Festlegung bestimmter Limits für Remote-Verbindungen (z. B. maximale Verbindungszeit, maximale Anzahl an Verbindungsaufbauten und Gebühreneinheiten) sowie deren automatischer Überwachung durch die Verbindungssteuerung im laufenden Betrieb.

2. Installation

Die Installation der Secure Software erfolgt komfortabel über Scripts. Der Installationsablauf ist für alle Versionen des Secure Clients identisch. Im folgenden ist die Installation unter Linux beschrieben.

Bevor Sie die Software installieren, müssen zur vollen Funktionsfähigkeit die Installationsvoraussetzungen, wie im folgenden Kapitel beschrieben, erfüllt sein.

2.1 Installationsvoraussetzungen

Betriebssystem

Die Software kann auf Computern (min. 32 MB RAM) mit den Betriebssystemen SuSe ab Version 7.3 und Red Hat ab Version 7.3 (Kernel-Versionen größer gleich 2.4.10) installiert werden.

Getestet wurde vorliegende Version unter SuSE 9.2 und Fedora Core 3 (nur für Modem).

Zielsystem

Das Zielsystem muss eine der folgenden Verbindungsarten unterstützen: ISDN, PSTN (analoges Modem), GPRS-UMTS, LAN over IP, PPP over Ethernet oder AVM-PPP over CAPI.

Lokales System

Zunächst muss ein tap-Device (ethertap – älter, oder tuntap – neuer) entweder in den Kernel kompiliert oder als Modul vorhanden sein. Dieses Modul setzt den netlink-Support im Kernel voraus.

Deweiteren muss eines der folgenden Kommunikationsgeräte installiert sein.

- **ISDN-Adapter (ISDN)**

Der ISDN-Adapter muss die ISDN CAPI 2.0 unterstützen. Wenn Sie PPP Multilink nutzen, kann die Software bis zu 8 ISDN B-Kanäle (je nach Kanalanzahl des Adapters) bündeln. Prinzipiell kann jeder ISDN-Adapter, der die ISDN-Schnittstelle CAPI 2.0 unterstützt, eingesetzt werden. (Für gewöhnlich wird die CAPI bei der Installation eines ISDN-Adapters automatisch eingerichtet.)

Beachten Sie bitte, falls Sie die CAPI-Verbindung nutzen wollen, das auf ihrem System ein Link auf die CAPI-Library gesetzt ist:

```
/usr/lib/libcapi20.so
```

- **Analoges Modem (Modem) / digitales Modem**

Für die Kommunikation über Modem muss das Modem korrekt installiert sein, sowie Modem Init. String und COM-Port Definition zugewiesen sein. Das Modem muss den Hayes-Befehlssatz unterstützen.

Ebenso können Mobiltelefone für die Datenkommunikation genutzt werden, nachdem die zugehörige Software installiert wurde, die sich für den Client genauso darstellt wie

ein analoges Modem. Als Schnittstelle zwischen Handy und PC kann die serielle Schnittstelle, die IR-Schnittstelle (Infrarot) oder Bluetooth genutzt werden. Je nach Übertragungsart (GSM, V.110, GPRS oder HSCSD) muss die Gegenstelle über die entsprechende Einwahlplattform verfügen. Der in die Modemkonfiguration des Secure Clients einzutragende Initialisierungs-String ist vom ISP oder dem Hersteller des Mobiltelefons zu beziehen.

- **LAN-Adapter (LAN over IP)**

Um die Client-Software mit der Verbindungsart “LAN” in einem Local Area Network betreiben zu können, muss zusätzlich zum bereits installierten LAN-Adapter (Ethernet oder Token Ring) kein weiterer Adapter installiert werden. Die Verbindung der LAN-Clients ins WAN stellt ein beliebiger Access Router her. Einzige Vorausetzung: IP-Verbindung zum Zielsystem muss möglich sein. Die VPN-Funktionalität liefert die Client Software.

Adapter für ein wireless LAN (WLAN-Adapter) werden genauso behandelt wie normale LAN-Adapter. Auch für WLAN muss als Verbindungsart “LAN (over IP)” gewählt werden.

- **xDSL-Modem (xDSL (PPPoE))**

Die Verbindungsart PPP over Ethernet setzt voraus, dass eine Ethernet-Karte installiert und darüber ein xDSL-Modem mit Splitter korrekt angeschlossen ist.

- **xDSL (AVM - PPP over CAPI)**

Im Telefonbuch wurde im Konfigurationsfeld “Zielsystem” die Verbindungsart “xDSL (AVM - PPP over CAPI)” hinzugefügt. Diese Verbindungsart kann gewählt werden, wenn eine AVM Fritz! DSL-Karte eingesetzt wird. Im Feld “Rufnummer (Ziel)” in der Gruppe “Netzeinwahl” können für die Verbindung über CAPI noch AVM-spezifische Intitialisierungskommandos eingetragen werden.

Bei Verwendung der AVM Fritz! DSL-Karte wird keine separate zusätzliche Netzwerkkarte benötigt.

Voraussetzungen für die Strong Security-Version

Wenn Sie die Software VPN/PKI Client (Strong Security-Version des Clients) nutzen, die Zertifizierung (X.509) unterstützt, so müssen folgende Voraussetzungen erfüllt sein:

TCP/IP

Das Netzwerk-Protokoll TCP/IP muss auf dem Rechner installiert sein.

Chipkartenleser (PC/SC-konform)

Wenn Sie die “Erweiterte Authentisierung” (Strong Authentication) nutzen wollen, muss ein Chipkartenleser an Ihr System angeschlossen sein. Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Diese Chipkartenleser werden nur in der Liste der Chipkartenleser aufgenommen, nachdem der Leser angeschlossen und die zugehörige Treiber-Software installiert wurde. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden.

Dazu stellen Sie nach dem ersten Start des Monitors den Chipkartenleser ein unter “Verbindung → Zertifikate → Konfiguration”.

Chipkartenleser (CT-API-konform)

Wenn Sie einen CT-API-konformen Chipkartenleser nutzen, beachten Sie bitte folgendes:

☑ Mit der aktuellen Software werden Treiber für die Modelle Kobil B0/B1 und Kobil KAAN mitgeliefert. Diese Chipkartenleser können im Monitor unter “Verbindung → Zertifikate → Konfiguration” eingestellt werden. Sollte der Chipkartenleser mit den mitgelieferten Treibern nicht funktionieren oder ein anderer Chipkartenleser installiert sein, wenden Sie sich unbedingt an den Hersteller des Chipkartenlesers, bzw. konsultieren Sie die entsprechende Website bezüglich aktueller Hardware-Treiber, um den aktuellsten CT-API-Treiber zu erhalten und zu installieren. Nehmen Sie außerdem folgende Einstellung in der Client Software vor:

☑ Die entsprechende Bibliotheksdatei (*.so) muss in einem Verzeichnis abgelegt sein, welches vom System durchsucht wird (i.a. /usr/lib bzw. einstellbar über die Umgebungsvariable LD.LIBRARY.PATH).

☑ Editieren Sie die Datei NCPPKI.CONF, befindlich im Verzeichnis /etc/ncp mit einem ASCII-Editor, indem Sie als “ReaderName” den Namen des angeschlossenen Chipkartenlesers eintragen und als DL_LINUX den Namen des installierten Treibers eintragen.

```
ReaderName   = Kobil B0/B1 (CT-API)
DL_LINUX     = libct_b1.so
ReaderName   = Kobil Kaan (CT-API)
DL_LINUX     = libct_kaan.so
```

 © NCP engineering GmbH

Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1" auf sichtbar gesetzt wurden!

☑ Nach einem Restart der Client-Dämonen (rncpclntd restart) erscheint der von Ihnen eingetragene “ReaderName” im Monitor-Menü unter “Verbindung → Zertifikate → Konfiguration → Chipkartenleser”. Selektieren Sie nun diesen Chipkartenleser.

■ Chipkarten

Folgende Chipkarten werden unterstützt:

☐ Signtrust

☐ NetKey 2000

☐ TC Trust (CardOS M4)

■ Soft-Zertifikate (PKCS#12)

Statt einer Smart Card können auch Soft-Zertifikate genutzt werden.

■ Chipkarten oder Token (PKCS#11)

Mit der Software für die Smart Card oder den Token werden Treiber in Form einer PKCS#11-Bibliothek (.so) mitgeliefert. Diese Treiber-Software muss zunächst installiert werden. Anschließend muss die Datei NCPPKI.CONF editiert werden.

☑ Editieren Sie die Datei NCPPKI.CONF, befindlich im Verzeichnis /etc/ncp mit einem ASCII-Editor, indem Sie als “ReaderName” den Namen des angeschlossenen Lesers oder Tokens eintragen. Als PKCS11-DLL muss der Name des installierten Treibers (xxx.so) eintragen werden. Der zugehörige “Slotindex” ist herstellerabhängig (Standard = 0).

Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1" auf sichtbar gesetzt wurden!

```
ReaderName   = xxxname
PKCS11-DLL   = xxx.so
Slotindex    =
```

☑ Nach einem Restart der Client-Dämonen (rncpclntd restart) erscheint der von Ihnen eingetragene “Modulname” im Monitor-Menü unter “Verbindung → Zertifikate → Konfiguration → Chipkartenleser”. Selektieren Sie nun diesen Chipkartenleser oder Token.

Bitte beachten Sie bei der Installation des NCP Secure Linux Clients

In der weiteren Beschreibung werden für die Versionsbezeichnung folgenden Platzhalter verwendet:

```
h.uu-bbb ... Versionsbezeichnung (z.B. 2.00-017)
h        ... Hauptversionsnummer
uu       ... Unterversionsnummer
bbb      ... Buildnummer
```

Die Installation muss unter dem User durchführt werden, der den Client später benutzt. Jedoch wird während der Installation das Root-Passwort abgefragt, da Teile der Installation nur mit Root-Rechten durchführbar sind (die Umschaltung erfolgt innerhalb des Install-Scripts).

Das Software-Paket wird als sich selbst installierendes Script ausgeliefert. Sie erhalten die Software für den NCP Secure Linux Client auf einer CD. Das Installationsscript befindet sich auf der CD in dem Verzeichnis: Products/SecCl/Bin/Linux/h_uu.

Sie können das Installationsscript direkt von CD starten.

Darüber hinaus können Sie die Software auch über den FTP-Zugang der Firma NCP beziehen.

Beachten Sie bitte, dass Sie dem Installationsscript vorher Ausführungsrechte vergeben müssen (chmod +x ncpsecsvr-h.uu-bbb.sh).

2.2 Script-gesteuerte Installation

Installation vorbereiten

```
- mount -t iso9660 /dev/cdrom /mnt-point
- cd /mnt-point/Products/SecCl/Bin/Linux/h_uu
```

Nach der Installation können Sie das CD-Laufwerk wieder aushängen:

```
- umount /mnt-point
```

Install-Script aufrufen

```
- ./ncpsecclnt-h.uu-bbb.sh [u]
```

(Option u = unattended installation, unbeaufsichtigte Installation. Die Installation erfolgt dann ohne Benutzereingaben.)

Install-Script abarbeiten

Das Installations-Script

- ☐ entpackt das integrierte Archiv in das Verzeichnis ./ncpinst
- ☐ wechselt in dieses Verzeichnis
- ☐ testet verschiedene Voraussetzungen für die Installation (s.u.)
- ☐ kopiert die zu installierenden Dateien in ihre Zielverzeichnisse und
- ☐ startet die Secure Client Dämonen (ncprwsd, rwsrsud)

Im folgenden sind die einzelnen Installationsschritte näher erläutert.

Installationsroutine

Es sind 3 mögliche Varianten der Installation zu unterscheiden:

1. **Neuinstallation**

   Eine Neuinstallation wird dann durchgeführt, wenn vor der Installation noch kein Secure Linux Client installiert war bzw. dieser vorher komplett deinstalliert wurde.

2. **Update**

   Ein Update wird immer dann durchgeführt wenn bereits eine Version des Secure Linux Clients installiert ist.

3. **Unbeaufsichtigte Installation (Option “u”):**

   Wird beim Aufruf des Installationsscripts die Option “u” genutzt (siehe oben), so erfolgt die Installation ohne Benutzereingaben. Es werden Vorgabewerte für Dialoge eingesetzt.

   Das Installationsscript prüft als erstes verschiedene Installationsvoraussetzungen und Systemeinstellungen wie

- ☑ ist die Kernel-Version größer gleich 2.4.10,
- ☑ ist eines der VPN-Device-Module installiert (tun oder ethertap),
- ☑ ist das Firewall-Modul iptables installiert.
- ☑ ist eine Version des NCP Secure Clients bereits installiert,

danach entscheidet sich die Installationsroutine für eine der drei Varianten.

Sollten Sie die Installation nicht als Benutzer “root” ausführen (was i.a. sehr zu empfehlen ist, da der Client sonst nur unter hohem Sicherheitsrisiko als Benutzer “root” genutzt werden kann), so werden Sie als erstes immer nach dem Root-Passwort gefragt.

2.2.1 Neuinstallation

Hier wird als erstes die Lizenzvereinbarung angezeigt. Dieser muss zugestimmt werden, soll die Installation fortgesetzt werden.

Innerhalb des Lizenztextes kann mittels der Tasten “Leertaste”, “Enter”, “Shift Page-Up”, “Shift Page-Down” navigiert werden.

Im nächsten Schritt kann zwischen der Installation als zeitlich limitierte Testversion oder als Vollversion gewählt werden.

Die Testversion ist 30 Tage gültig. Während dieser Zeit ist die Software ohne jede Einschränkung funktionsfähig und kann jederzeit mit einem entsprechenden Aktivierungsschlüssel und einer Seriennummer zu einer Vollversion aufgerüstet werden.

Danach kopiert die Installationsroutine die benötigten Dateien in die entsprechenden Verzeichnisse, legt Links in den Systeminitverzeichnissen, den Autostart- und Desktop-Ornders an und startet die Client-Dämonen.

2.2.2 Update

In diesem Fall wird die aktuell installierte Version angezeigt und gefragt, ob diese Version ersetzt werden soll. Bei der Antwort “nein” wird weder ein Update noch eine Installation vorgenommen. Bei ja wird zuerst das Programmverzeichnis des installierten Secure Linux Clients (/usr/local/ncpclnt) nach
`/var/adm/backup/ncpclnt-update-yymmdd[-l]`
gesichert und danach die neuen Dateien in die entsprechenden Verzeichnisse kopiert und Links angelegt.

2.2.3 Unbeaufsichtigte Installation

Diese Installationsart erfordert keine Benutzereingaben. Es wird entweder die Lizenzeinstellung der Vorgängerversion übernommen (bei einem Update) oder es wird eine 30-Tage-Testversion lizensiert (bei Neuinstallation).

Beim einem Update wird die alte Version ungefragt nach
`/var/adm/backup/ncpclnt-update-yymmdd[-l]`
gesichert. Ansonsten ist der Ablauf analog zur Neuinstallation.

2.2.4 Installation abschließen

Das Installationsscript löscht automatisch das temporäre Installationsverzeichnis und beendet sich anschließend.

2.3 Die installierten Dateien

Die Dateien werden in folgende Ordner kopiert (siehe auch → Verzeichnisstruktur):

- ausführbare Dateien in:
  `/usr/local/ncpclnt/bin`

- Links auf ausführbare Dateien:
  `/usr/local/bin und /usr/local/sbin`

- Konfigurationsdateien:
  `/etc/ncp (das Telefonbuch in /etc/ncp/rws/cfg)`

- Log-Dateien:
  `/var/log/ncp`

Damit der Client beim nächsten Systemstart automatisch geladen wird, werden die dafür notwendigen Dateien in die Init- bzw. Autostart-Scripte eingetragen (SuSE):

Die Dämonen ncprwsd und rwsrsud werden in die Init-Routinen der beiden Distributionen intergriert. Sie können auch separat mit rcncpclntd start|stop gestartet werden. Links auf die beiden GUI-Anwendungen ncppopup (Client Popup) und ncpmon (Client Monitor) werden in den Autostart-Ordnern der entspr. Windows-Manager eingetragen (KDE1, KDE2, GNOME). Zusätzlich werden ein Links auf dem Desktop abgelegt. Für andere X-Windows-Manager muss dies, wenn gewünscht, per Hand erfolgen.

2.4 Grundkonfiguration

Für das VPN-Interface wird das Device tuntap genutzt (wenn nicht vorhanden wird auf ethertap ausgewichen), das von Linux bereitgestellt wird. Alle gängigen Installationen haben dieses Device in ihren Kernel eingebunden. Falls ein Kernel selbst kompiliert wird, sollten folgende Punkte beachtet werden, um dieses Device mit einzubinden:

Nach dem Start der Kernel-Konfiguration zu folgendem Abschnitt wechseln:

“* code maturity level options”, dort aktivieren:
“* prompt for development or incomplete code/drivers”, danach wechseln zu:
“* Network options”, dort aktivieren:
“* Netlink device emulation” dann wechseln zu:
“* Network device support”, dort aktivieren:
“* Universal TUN/TAP device driver support” oder wenn nicht vorhanden
“* Ethertap network tap”

Einige Grundeinstellungen für das VPN-Device können über die Datei ncprwsd.conf vorgenommen. Diese Datei befindet sich nach der Installtion im Verzeichnis

`/etc/ncp/rws/cfg.`

Die folgenden Parameter können über diesen Weg gesetzt werden:

`host`
IP-Adresse des VPN-Devices, wenn DHCP nicht verwendet werden soll.

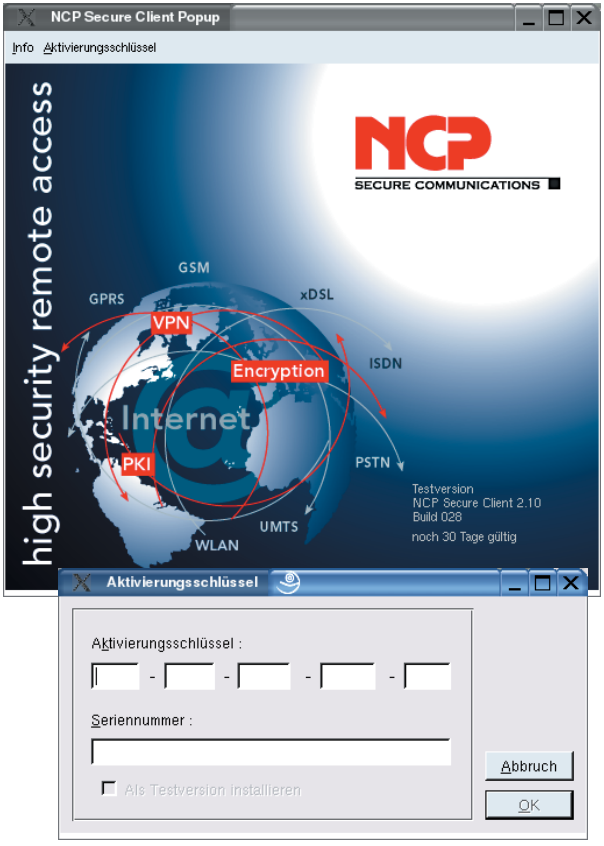
`mask`
das Gleiche für die Netzmaske.

`pppoe_if`
Name des Interfaces, über welches der PPP-OE-Verkehr laufen soll.

Nach der Installation sind alle Parameter auskommentiert, d.h. es werden Vorgabewerte für diese Parameter verwendet (die auskommentierten Einträgen entsprechen den Vorgabewerten). Möchte man andere Parametereinstellungen verwenden, muss das Kommantarzeichen am Zeilenanfang entfernt und der gewünschte Wert eingetragen werden.

2.5 Freischalten einer Vollversion

Wenn Sie bisher eine Testversion der Client Software benutzt haben und nun eine Vollversion nachinstallieren möchten, starten Sie zunächst das Client Popup.



Unter dem Menüpunkt “Info” finden Sie die nötigen Angaben, um eine Lizenz erwerben zu können.

Unter dem Menüpunkt “Aktivierungsschlüssel” können Sie die Testversion freischalten.

Vor dem Bild des Popup-Menüs erscheint ein Fenster, worin Sie Aktivierungsschlüssel und Seriennummer Ihrer Vollversion eintragen können.

Tragen Sie nun Aktivierungsschlüssel und Seriennummer ein. Wenn Sie korrekt eingetragen sind, können Sie den OK-Button bedienen. Damit ist eine Vollversion freigeschaltet.

Lizenzierung mit ncplic

Sie habe eine 2. Möglichkeit, den Aktivierungsschlüssel einzugeben. Starten Sie dazu das Programm “ncplic” auf einer Root-Konsole. Mit dem Kommandoschalter -f erscheint eine Eingabemaske. In diese tragen Sie den Aktivierungsschlüssel und die Seriennummer ein. Sie können beide Werte auch als Parameter mit dem Kommandoschalter -l eingeben:

```
ncplic -l aaaa-aaaa-aaaa-aaaa-aaaa ssssssss.
```

2.6 Deinstallation

Um die Client Software zu entfernen, starten Sie das Script ncpclntdeinstall. Bei einer Deinstallation haben Sie die Möglichkeit auch das Telefonbuch automatisch entfernen zu lassen.

2.7 Assistent für erste Konfiguration

Nachdem Sie die Software erfolgreich installiert haben und die Lizenz mittels NCPPOPUP aktiviert haben, kann der Client-Monitor NCPMON starten. Dort wird automatisch der “Assistent für die erste Konfiguration” gestartet – vorausgesetzt, Sie haben den Secure Client zum ersten Mal installiert oder das Telefonbuch gelöscht (siehe → Deinstallation).

Der “Assistent für erste Konfiguration” bietet Ihnen die Möglichkeit, Test-Verbindungen anzulegen. Wenn Sie diese Möglichkeit nutzen, führt Sie der Assistent durch die Konfiguration der wichtigsten Parameter und legt nach der Vorgabe Ihrer Daten ein Zielsystem für Testverbindungen im Telefonbuch an.

Für die Telefonbucheinträge, die Sie mit diesem Assistenten erstellt haben, werden die Zugangsdaten verwendet, die unter “Tests des Clients” beschrieben sind. Sie können diese Einträge anschließend zum Testen der Software benutzen.

Wenn Sie keine Test-Verbindungen anlegen und den “Assistent für erste Konfiguration” abbrechen, erstellen Sie die ersten Telefonbucheinträge, wie im Handbuch unter “Client Monitor” – “Neuer Eintrag – Zielsystem” beschrieben.

2.8 Start des Linux Clients

Der Secure Client besteht aus den Komponenten VPN-Device-Treiber (ncprwsd) und Monitor (ncpclnt). Für den automatischen Update werden noch die Dämonen rwsrsud und rsudlgd benötigt.

In den SuSE-Distributionen werden die Dämonen beim Systemstart geladen, da sie hier während der Installation in die Systeminit-Scripte integriert wurden. Bei allen anderen Distributionen muss man die Integration in die Init-Scripte per Hand vornehmen oder die Dämonen von einer Root-Konsole starten
(/usr/local/ncpclnt/bin/ncpclntd start).

Nach jedem Start des Client Dämons ncprwsd (z. B. nach dem Start des Systems oder nach rcncpclntd start) muss als erstes das Popup aufgerufen werden, da erst dadurch die Lizenz ihre Gültigkeit erhält. Beim Start des Systems erfolgt das im Allgemeinen automatisch, wenn Links auf die beiden GUI-Programmme in den Autostartordnern vorhanden sind.

Per Hand können die GUI-Programme entweder über ein Icon auf dem Arbeitsplatz, oder über Alt-F2 bei KDE, oder von einer Konsole gestartet werden. Diese Aufrufe müssen unter dem User erfolgen, der die Software auch installiert hat, da es ansonsten zu Rechte-Konflikten kommen kann.

Der Aufruf von der Konsole sieht z.B. so aus:

```
ncppopup &
```

und

```
ncpmon &
```

Vom Ladezustand der Dämonen kann man sich mit den beiden Aufrufen

```
rcncpclntd status
```

bzw.

```
/usr/local/ncpclnt/bin/ncpclntd status
```

überzeugen.

2.9 Tests des Clients

Das Telefonbuch des Clients enthält nach dem Einsatz des Assistenten für die erste Konfiguration folgende vorkonfigurierte Zielsysteme für Testzwecke:

- ☐ “Test Verbindung”
- ☐ “Test Verbindung L2TP”
- ☐ “Test Verbindung SSL”
- ☐ “Test Verbindung IPSec”

Ebenfalls für Testzwecke wurde ein “X.509 Soft-Zertifikat” beigegeben. Es wird bei der Installation als PKCS#12-Datei under /etc/ncp/certs gespeichert. Der Dateiname ist “user1.p12" und die PIN ”1234". Dieses Zertifikat kann genutzt werden, um die Strong Security-Version VPN/PKI Client zu testen.

2.9.1 Test Verbindung (testet ISDN, Modem, GSM)

Zugangsdaten:

```
Rufnummer                 :       +4991199682663
Benutzer                  :       ncpuser
Passwort                  :       ncpuser
Verschlüsselung           :       keine
```

2.9.2 Test Verbindung L2TP (testet L2TP-Protokoll)

Zugangsdaten für Tunneling:

```
Tunnel IP-Adresse (Ziel)  :       62.153.165.36
VPN-Protokoll             :       L2TP
Benutzer (VPN)            :       ncpuserl2tp
Passwort (VPN)            :       ncpuserl2tp
Tunnel Secret             :       secret
Verschlüsselung           :       keine
```

2.9.3 Test Verbindung SSL (testet SSL-Verschlüsselung und Zertifikat)

Zugangsdaten für Tunneling mit SSL-Verschlüsselung und Zertifikat
(Nur mit VPN/PKI Client möglich) :

```
Tunnel IP-Adresse (Ziel)  :       62.153.165.36
VPN-Protokoll             :       L2TP
Benutzer (VPN)            :       ncpuserssl
Passwort (VPN)            :       ncpuserssl
Tunnel Secret             :       secret
Verschlüsselung           :       SSL mit Zertifikat
```

Außerdem muss im Monitor-Menü unter
→ Konfiguration
→ Zertifikate
→ Dateiname “user1.p12"
eingetragen sein!

2.9.4 Test Verbindung IPSec (testet IPSec over L2TP mit Preshared Key)

Zugangsdaten für IPSec over L2TP:

```
Tunnel IP-Adresse (Ziel) : 62.153.165.36
VPN-Protokoll            : L2TP
Benutzer (VPN)           : ncpuseripsec
Passwort (VPN)           : ncpuseripsec
Tunnel Secret            : secret
Security-Modus           : IPSec
Statischer Schlüssel     :
 00.11.22.33.44.55.66.97.88.99.AA.BB.CC.DD.EE.FF
IKE-Richtlinie           : Pre-Shared Key
IPSec-Richtlinie         : ESP AES128 MD5
Austausch-Modus          : Aggressive Mode
```

2.9.5 Testen mit Ping

Bei bestehendem Tunnel können Sie die IP-Adresse 172.16.119.8 anpingen.

Geben Sie dazu in einer DOS-Kommandozeile folgendes ein:

```
C:\>ping 172.16.119.8 (<ENTER>)
```

Bei erfolgreichem Ping sehen Sie folgende oder ähnliche Ausgaben:

```
Reply from 172.16.119.8: bytes=32 time=109ms TTL=128
Reply from 172.16.119.8: bytes=32 time=96ms TTL=128
Reply from 172.16.119.8: bytes=32 time=82ms TTL=128
Reply from 172.16.119.8: bytes=32 time=69ms TTL=128
```

Im Monitor werden die versendeten (Tx) und die empfangenen (Rx) Bytes angezeigt.

2.9.6 Testen mit FTP

Bei bestehendem Tunnel können die FTP-Funktionalität testen.

Ihre Zugangsdaten:

```
IP-Adresse        :  172.16.119.8
Benutzer          :  ncptest
Passwort          :  ncptest
```

Geben Sie dazu in einer DOS-Kommandozeile folgendes ein:

```
C:\>ftp 172.16.119.8
Verbindung mit 172.16.119.8
220 Serv-U FTP-Server v2.3b for WinSock ready...
Benutzer (172.16.119.8:(none)): ncpuser
331 User name OK, send password
Kennwort: (hier "ncptest" eingeben)
230 User NCPUSER logged in
Ftp>
Ftp> ls -l
200 PORT Command OK
150 Opening data connection
total 1
drwxr-xr-x  1 User  Group  0 May 27 10:37 testfile
226 Transfer complete
Ftp: 139 Bytes empfangen in 0.00Sekunden
139000.00KB/Sek.
Ftp>bye
```

2.9.7 Testen der Web-Funktionalität

Geben Sie Ihrem geöffneten Web-Browser folgende Adresse ein:

```
192.168.1.11
```

anschließend erhalten Sie die NCP-Website auf Ihrem Bildschirm.

2.10 Verzeichnisstruktur NCP Secure Linux Client

Verzeichnis Dateien		Funktion	Erstellung
/usr/local/ncpclnt		Binaries des Clients	
/usr/local/ncpclnt/bin		GUI-Apps., Dämonen, Scripts und Hilfsroutinen	
Dämonen:			
ncprwsd		VPN-Modul	inst.
rwsrsud		Remote-Software-Update (RSU-) Client	inst.
rsudlgd		grafische Elemente des RSU-Client	inst.
GUI-Anwendungen:			
ncpclnt		Client Monitor	
ncppopup		Client Popup: Anzeige des Lizensierungs-status und Möglichkeit für Produktaktivier.	inst.
ncptrcw		Client Tracer (graf. Trace-Anzeige)	inst.
Hilfsroutinen:			
rwscmd		Konsolenprogramm, um die Steuerung des Clients per Script zu ermöglichen	inst.
ncplicclnt		Konsolen-Lizensierungstool und Möglichkeit für Produktaktivierung	inst.
ncposlog		Hilfsprogramm zum nachträglichen Einstellen der Loglevel des VPN-Moduls	inst.
killproc		beendet Prozesse	inst.
ipcdel		Setzt IPC-Semaphore zurück, falls nach einem Fehler der Secure Client nicht mehr ordungsgemäß hochfährt.	inst.
Scripte:			
ncpmon		ruft ncpclnt auf	inst.
startncppopup		ruft ncppopup auf	inst.
ncptrace		ruft ncptrcw auf diese 3 Scripte setzen vorher den Pfad auf die mitgelieferte qt-Bibliothek	inst.
ncpinststartup		dieses Script gestattet das nachträgliche Aktivieren bzw. Deaktivieren des SysV-Init-Scripts und damit das Starten bzw. Nicht-starten des VPN- und RSU-Moduls in der Boot-Phase (kann nur als root ausgeführt werden)	inst.
ncpclntd		SysV-Init-Script zum Starten/Stoppen des VPN-Moduls des Clients	inst.
clntdstart		startet die Dämonen des Secure Clients	inst.
clntdstop		stoppt die Dämonen des Secure Clients	inst.
clntdstatus		informiert über den Ladezustand der Dämonen des Secure Clients	inst.
clntconf	(**)	Hilfsscript zum Einrichten bzw. Entfernen des Secure Clients als rpm-Paket: - überprüft bzw. generiert die Lizensierung - erstellt verschiedene Softlinks - setzt verschiedene Rechte - generiert die SysV-Init-Scripte - kehrt die obige Aktionen beim Deinstal-lieren des RPM-Pakets um;	inst.
clntdeinst		Deinstallationsscript;	inst.

```
sonstige:
ncpfunc                 Script-Bibliothek, die allgemeingültige     inst.
                        Funktionen und Definitionen für die
                        verschiedenen Scripte enthält
clntfilelist            Liste der zu installierenden Dateien in     inst.
                        verschiedenen Variablen aufgeteilt
ncpclntinst.log    (*)  Installationslog                            generiert
-------------------------------------------------------------------------------
/usr/local/ncpclnt/rsudata  Download Verzeichnis für Remote Update
rwsrsud                 Kopie aus /usr/local/ncpclnt/bin            inst.
rsudlgd                 Kopie aus /usr/local/ncpclnt/bin            inst.
                        Wird benötigt, damit der Update-Dämon eine
                        neuere Version von sich selbst erkennen kann
-------------------------------------------------------------------------------
/usr/local/ncpclnt/lib  von den Binaries benötigte Bibliotheken
libbsdntif.so.1.0.0     BSD-Sockets-Wrapper                         inst.
libncpcfg.so.1.0.0      Funktionen für verschlüsselte Lizenzinfos   inst.
libncpcompr.so.1.0.0    Funktionen für Komprimierung/Dekomprimier.  inst.
libncpgacc.so.1.0.0     Funktionen für den Datenaustausch zwischen  inst.
libncpmif32.so.1.0.0    Funktionen für interne MIF-Bufferverwaltung inst.
                        und Shared Memory Handling
libncpos.so.1.0.0       Wrapper für Betriebssystemfunktionen        inst.
libncpwlan.so.1.0.0     Funktionen für autom. Hotspoterkennung      inst.
libqt.so.2.2.4          Bibl. für grafische Elemente (wird von Ent- inst.
libqtintf.so.2.2.4      wicklungsumgebung Kylix verlangt)           inst.
libqt.so.2              Softlinks auf libqt.so.2.2.4                inst.
libqtintf.so            Softlinks auf libqtintf.so.2.2.4            inst.
libct_b1.so.1           CT-Api-Bibliothek für Kobil B1 Leser        inst.
libct_kaan.so.1         CT-Api-Bibliothek für Kobil Kaan Leser      inst.
-------------------------------------------------------------------------------
/usr/lib:               Softlinks auf die Bibliotheken
libbsdntif.so                                                       inst.
libncpcfg.so                                                        inst.
libncpgacc.so                                                       inst.
libncpmif32.so                                                      inst.
libncpos.so                                                         inst.
-------------------------------------------------------------------------------
/usr/local/sbin         Softlinks auf von root zu startende Programme
rcncpclntd              /etc/init.d/ncpclntd                        inst.
-------------------------------------------------------------------------------
/usr/local/bin          Softlinks auf vom Nutzer zu startende
                        Programme + Script für Deinstallation
ncpclntdeinstall   (*)  Wrapper für clntdeinst, um die Deinstal-    inst.
                        lation als normaler User starten zu können
ncpmon                  /usr/local/ncpclnt/bin/ncpmon               inst.
ncppopup                /usr/local/ncpclnt/bin/startncppopup        inst.
ncptrace                /usr/local/ncpclnt/bin/ncptrace             inst.
ncplic                  /usr/local/ncpclnt/bin/ncplicclnt           inst.
ncposlog                /usr/local/ncpclnt/bin/ncposlog             inst.
===============================================================================
>HOME_DIR</xxx/Autostart  Softlinks der GUI-Anwendungen in diesem
ncpmon                  Ordner sorgen dafür, dass die Programme     inst.
ncppopup                autom. gestartet werden                     inst

>HOME_DIR</yyyDesktop Softlinks der GUI-Anwendungen in diesem
ncpmon                  Ordner sorgen dafür, dass die Programme     inst.
ncppopup                auf dem Desktop abgelegt werden             inst.
xxx bzw. yyy            steht für einen Windows-Manager spezi-
                        fischen Ordner/Eintrag,
                        bei KDE2 z.B. ist xxx = .kde2 und yyy = K
===============================================================================
```

/etc/ncp	Konfigurationverzeichnis	
ncppki.conf	Einstellungen für das PKI-Modul	inst.
card.dat	angeschlossene Smartcard-Reader	shm
cacert0.crt	Zwischengespeicherte Zertifikate der CA	generiert
clientcert.crt	des Clients	generiert
svrcert.crt	des Servers	generiert
/etc/ncp/certs	persönliche, vordefinierte Zertifikate	
user1.p12	vordefiniertes Nutzer-Zertifikat	inst.
/etc/ncp/cacerts	Root-Zertifikate	
ncpsupportca.pem	vordefiniertes CA-Zertifikat für die Testverbindung zu NCP	inst.
/etc/ncp/rws/cfg	Secure Client Konfiguration	
deutsch.dat	Sprachdateien für die Texte der GUI-	inst.
english.dat	Anwendungen (ncpclnt, ncppopup)	inst.
polnisch.dat	Anwendungen (ncpclnt, ncppopup)	inst.
services.dat	Mapping derTCP-/UDP-Dienste für GUI-Apps.	inst.
ncprwsd.conf	Konfiguration des VPN-Moduls (ncprwsd)	inst.
logo.bmp	Bitmaps für die GUI-Anwendungen	inst.
info_ncp.bmp		inst.
logoinfo.bmp		inst.
popup.bmp		inst.
gelb.bmp		inst.
gruen.bmp		inst.
rot.bmp		inst.
connect.sh	Scripte die beim Verbindungsauf- bzw.	inst.
disconnect.sh	abbau aufgerufen werden. Damit wird die Möglichkeit geschaffen, zusätzlich Proramme zu starten.	inst.
fwmsge.dat	Firewall-Log-Template	inst.
pindlg.conf	Pin-Dialog individuell gestalten	inst.
ncpphone.cfg	Telefonbuch (wird generiert, falls nicht vorhanden)	inst./ generiert
ncpclnt.conf	Einstellungen des Client Monitors (ncpclnt)	generiert
reader.ini	die laut ncppki.conf aktivierten Smartcard-Reader ([Interfaces])	generiert
/etc/init.d	Verzeichnis der SysV-Init-Scripte	
ncpclntd	SysV-Init-Script zum Starten/Stoppen des VPN-Moduls des Clients (Kopie aus /usr/local/ncpclnt/bin)	inst.
/etc/init.d/rc1.d	Start-/Stopp-Aufrufe für SysV-Init	
/etc/init.d/rc2.d	(s. entspr. Linux-Distribution, denn diese	
/etc/init.d/rc3.d	Verzeichnisse können sich etwas voneinander	
/etc/init.d/rc5.d	unterscheiden)	
Sxxncpclntd	Softlink auf /etc/init.d/ncpclntd	generiert
Kxxncpclntd	Softlink auf /etc/init.d/ncpclntd xx wird durch eine Zahl ersetzt, die die Startreihenfolge vorgibt. Die Zahl wird von einem entspr. Tool selbständig vergeben.	generiert
/etc/modules.conf	Einträge für tun- bzw. tap-Device, wenn noch nicht vorhanden.	vorhanden

```
var/log/ncp          Logverzeichnis
ncp>date<.log         Secure Client Log                              generiert
rwsrsu.log            RSU-Log-Datei                                  generiert

/var/log/ncp/log      (wenn kein anderes Verz. konfiguriert wurde)
fwyymmdd.log          Firewall-Log-Datei                             generiert
(yymmdd               Jahr Monat Tag)
-------------------------------------------------------------------------------
/var/run
ncprwsd.pid           pids dieser Dämonen                            generiert
rwsrsud.pid                                                          generiert
===============================================================================
/usr/share/doc/packages/ncpclnt/
                      Doku-Verzeichnis
licger.txt            Lizenzvereinbarung                             inst.
licengl.txt           Lizenzvereinbarung (en)                        inst.
infoger.txt           Info zum Update auf Vollversion                inst.
infoengl.txt          dito in engl.                                  inst.
liesmich.txt    (***) letzte Infos in deutsch                        inst.
readme.txt      (***) dito in engl.                                  inst.
(***) diese Dateien werden nur dann bei der Installation mit kopiert,
      wenn sie sich auf dem Installationsmedium zusätzlich zum
      Installationsscript befinden.

===============================================================================
/var/adm/backup/ncpclnt-deinst-yymmdd[-l]
                      enthalten die während der Deistallation     generiert
                      gesicherten Dateien, d.h. dieses Verzeichnis
                      ist erst nach einer erstmaligen Deinstal-
                      lation vorhanden (Öffnen nur mit Root-Rechten mögl.)
/var/adm/backup/ncpclnt-update-yymmdd[-l]
                      enthalten die während eines Updates         generiert
                      gesicherten Binaries aus /usr/local/ncp,
                      d.h. dieses Verzeichnis ist erst nach einem
                      erstmaligen Update (Installation auf ein
                      System, auf welchem der Secure Client
                      bereits installiert war) vorhanden

yymmdd                Jahr Monat Tag an der das Verzeichnis ange-
                      legt wird
l                     optional laufende Nummer falls das Anlegen
                      am gleichen Tag erfolgt

===============================================================================
die hier aufgelisteten Scripte werden nur für die Installation per Script
benötigt und werden nicht mit installiert:
ncpsecclnt-h.uu-bbb.sh(*) eigentlicher Installationsscript, der
                      die unten aufgeführten Scripte benutzt.
                      plus den Script clntconf
                      (s.o.)
clntchk               dieses Script überprüft die Installations-
                      voraussetzungen
clntinst              Script, der die Zielverzeichnisse erzeugt
                      und die Dateien kopiert

(*)   diese Dateien werden nur bei der Installation über Script benötigt
(**)  diese Dateien werden nur bei der RPM-Installation benötigt
shm   shared memory = generiert
```

Diese Seite ist frei →

© NCP engineering GmbH

3. Client Monitor

Wenn die Software nach den Standardvorgaben installiert wurde, kann der Monitor über das Start-Menü → Programme → NCP Management → Secure Client Monitor aktiviert werden. Damit öffnet sich das Fenster des Monitors auf dem Bildschirm.

Hinweis: Wenn der Monitor zum Icon verkleinert wird, erscheint er als Ampellicht in der Taskleiste.

Der Monitor hat 4 wichtige Funktionen:

☑ den aktuellen Status der Kommunikation wiederzugeben. Dies geschieht im grafischen Statusfeld durch die farbige Einblendung von Symbolen.

☑ den Verbindungsmodus einzustellen, zielsystemabhängig im Telefonbuch unter “Verbindungssteuerung”.

☑ die Limits der Verbindungssteuerung bestimmen. Sie werden im Hauptmenü unter “Konfiguration → Verbindungssteuerung” eingestellt.

☑ die Definition und Konfiguration der Zielsysteme mit dem Telefonbuch. Das Telefonbuch wird im Hauptmenü unter “Konfiguration → Telefonbuch” angelegt.

3.1 Die Oberfläche des Client Monitors

3.1.1 Bedien- und Anzeigefelder

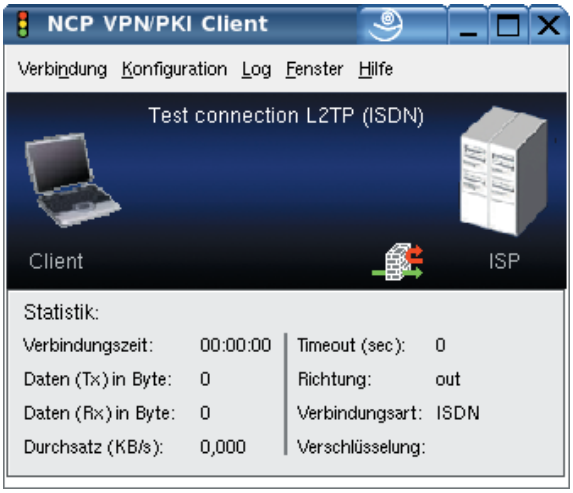
Der Client Monitor besteht aus:

- ☐ einer Titelzeile mit Anzeige der Security-Version,
- ☐ der Hauptmenüleiste,
- ☐ der Zielauswahl mit einem Feld für die Amtsholung,
- ☐ dem grafischen Statusfeld zur Anzeige des Verbindungsstatus,
- ☐ der Buttonleiste mit “Verbinden” und “Trenne”
- ☐ und einem Statistikfeld

Der Monitor kann bedient werden über die Pulldown-Menüs der Menüleiste, über die Buttons der Buttonleiste oder über das Kontextmenü (rechte Maustaste).

3.1.2 Das Erscheinungsbild des Monitors

Je nach gewählter Einstellung im Monitor-Menü “Fenster” erscheint der Monitor nach Ausblenden seiner Bestandteile (siehe → vorhergehende Seite) in verschiedenen Größen (siehe → Fenster).



Modifikationen der Oberfläche

Die Verbindungsart (siehe → Telefonbuch, Zielsystem) lässt sich im Statistikfeld ablesen oder kann bei der Namensvergabe an das Zielsystem mit eingegeben werden (siehe → Name Zielsystem), sodass sie auch im grafischen Statusfeld erscheint.

Bitte beachten Sie außerdem, dass das Erscheinungsbild des Client Monitors auch vom Leistungsumfang des Secure Clients abhängt.

Zudem kann das Erscheinungsbild vom Administrator verändert werden. Dies betrifft insbesondere die Menüpunkte “Verbindungs-Informationen”, “Zertifikate”, “Remote-Administration”, “Verbindungssteuerung” und “Logon Optionen”. Auch Parameterfelder des Telefonbuchs und einzelne Parameter können vom Administrator ausgeblendet bzw. auf “nicht konfigurierbar” gesetzt worden sein, wenn Sie von Ihrem Administrator Installations-Disketten mit einer vorkonfigurierten Version ausgehändigt bekommen. Die ausgeblendeten und deaktivierten Features erleichtern den Umgang mit der Software und haben keinen Einfluss auf die Leistungsfähigkeit der Software.

3.1.3 Statusanzeigen

Folgende Statusanzeigen werden im grafischen Feld angezeigt:

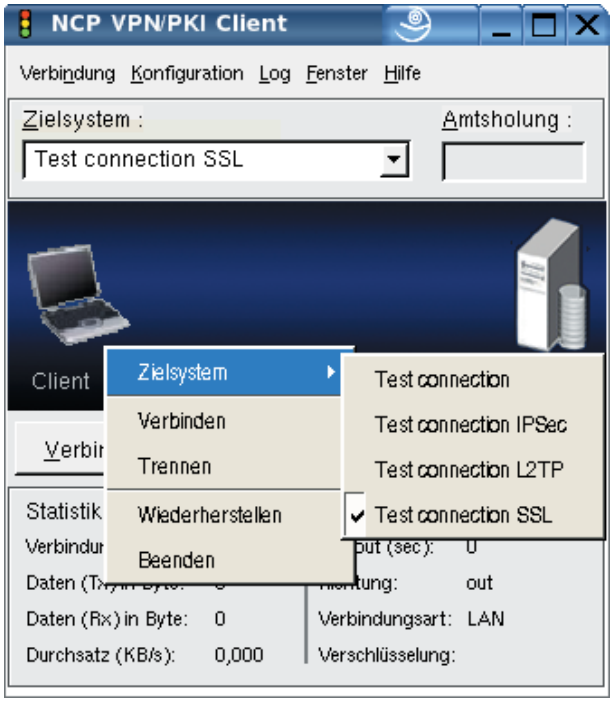
– Chipkarte
– PIN-Status
– Firewall-Option
– EAP-Status

Diese Symbole in der Statusanzeige sind um Tool-Tipps (Quickinfos) erweitert, wenn der Mauszeiger auf ein Symbol zeigt.

Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt die EAP-Verhandlung erneut.

3.1.4 Anwahl und Auswahl des Zielsystems

Sobald die Software installiert und ein Zielsystem korrekt konfiguriert wurde, kann die Anwahl an dieses Zielsystem stattfinden.



Das gewünschte Zielsystem wird über die Auswahl-Box unter dem Hauptmenü oder nach Klick auf die rechte Maustaste aus einer Liste gewählt (siehe nebenstehendes Bild).

Um eine Verbindung zum selektierten Ziel herzustellen, ist es nicht nötig, den Client Monitor eigens zu starten oder die Anwahl manuell durchzuführen. Lediglich die gewünschte Applikations-Software muss gestartet werden. Die Verbindung wird dann, entsprechend den Parametern des Zielsystems, automatisch aufgebaut (siehe → Verbindungssteuerung, Verbindungsaufbau, automatisch). Daneben ist es auch möglich, manuell die Verbindung zu einem ausgewählten Ziel herzustellen, indem Sie im Monitor den Hauptmenüpunkt “Verbindung” anklicken und “Verbinden” wählen. Alternativ kann auch der Button “Verbinden” angeklickt werden. (Siehe → Eine Verbindung herstellen).

Eine bestehende Verbindung (siehe → Bild oben) wird mit einem dicken grünen, durchgehenden Balken zwischen Client und Server dargestellt, unter dem der Text “Verbindung ist hergestellt” eingeblendet wird. Gleichzeitig wird die (Icon-)Ampel grün. Damit werden Sie darauf aufmerksam gemacht, dass für eine Remote-Verbindung Gebühren anfallen.

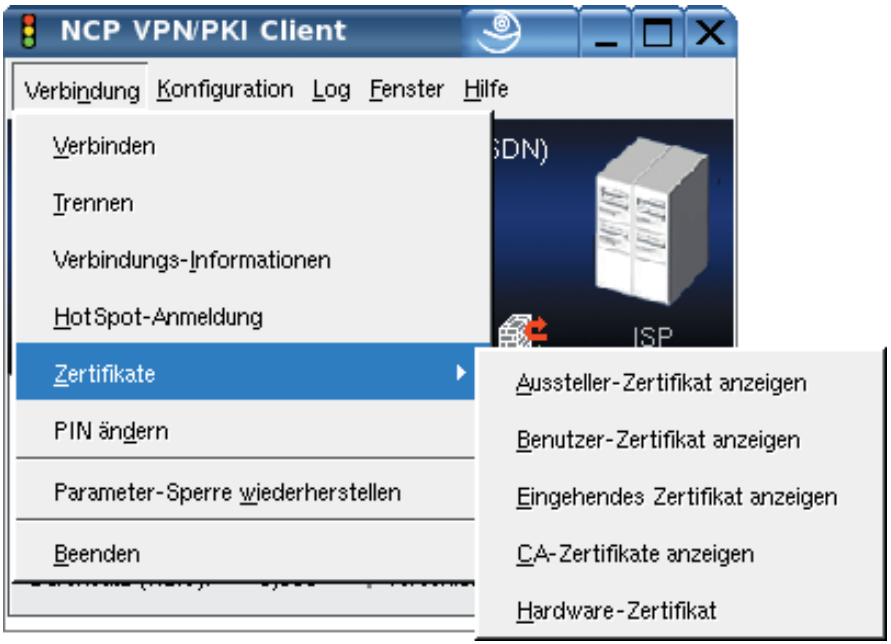
4. Das Monitor-Menü

Die Beschreibung folgt den Menüpunkten in der Menüleiste.

Die Hauptmenüpunkte in der Menüleiste von links nach rechts sind:

- ☐ Verbindung |Menü
- ☐ Konfiguration |Menü
- ☐ Log |Menü
- ☐ Fenster |Menü
- ☐ Hilfe |Menü

4.1 Verbindung



Unter diesem Menüpunkt befinden sich die Kommandos zum Aufbau und Trennen einer Verbindung, Informationsfenster zum aktuellen Verbindungsaufbau sowie zur Darstellung der eingesetzten Zertifikate. Außerdem kann hier die Statistik der Verbindungsteuerung abgelesen werden und gegebenenfalls die Sperre der Verbindungssteuerung gelöst werden, wenn ein von Ihnen gesetztes Limit überschritten wurde.

Der Untermenüpunkt "Parametersperre aufheben" erscheint nur, wenn Sie eine vorkonfigurierte Version von Ihrem Administrator erhalten haben.

Die Untermenüpunkte "Zugriff erlaubt", "Nachricht zum Administrator senden" und "Remote-Verbindung trennen" sind nur in Zusammenhang mir der Remote-Administration der Software von Bedeutung und können nur nach Absprache mit Ihrem Administrator sinnvoll genutzt werden.

4.1.1 Verbinden

Mit diesem Befahl wird eine Verbindung aufgebaut. Eine Verbindung kann nur aufgebaut werden, wenn ein “Ziel” aus dem “Telefonbuch” selektiert ist (siehe → Telefonbuch, Zielsystem). Das selektierte “Zielsystem” wird in der Monitoroberfläche unter der Menüleiste angezeigt.

Wenn Sie die Funktion “Verbinden” wählen, wird die Anwahl an das ausgewählte Zielsystem manuell durchgeführt. Der jeweilige Status des Verbindungsaufbaus wird grafisch dargestellt. Wenn Sie, je nach Zielsystem, die Verbindung manuell oder automatisch herstellen wollen, so können Sie dies im Telefonbuch mit dem Parameter “Verbindungsaufbau” im Feld “Verbindungssteuerung” definieren.

4.1.2 Trennen

Mit diesem Befehl wird eine Verbindung abgebaut. Mit der Funktion “Trennen” wird der Abbau der aktuell bestehenden Verbindung manuell durchgeführt. Wenn die Verbindung abgebaut wurde, wechselt die Ampellampe für die gesamte Offline-Dauer von grün auf rot.

4.1.3 HotSpot-Anmeldung

Voraussetzungen: Der Rechner muss sich mit aktivierter WLAN-Karte im Empfangsbereich eines HotSpots befinden. Die Verbindung zum HotSpot muss hergestellt und eine IP-Adresse für den Wireless-Adapater muss zugewiesen sein. (Unter Windows XP steht eine entsprechende Konfiguration für den Zugriff auf WLANs zur Verfügung.)

Die Firewall des NCP Secure Clients sorgt dafür, dass lediglich die IP-Adresszuweisung per DHCP erfolgen darf, weitere Zugriffe ins WLAN bzw. vom WLAN werden unterbunden. Die Firewall gibt dynamisch die Ports für http bzw. https für die Anmeldung bzw. Abmeldung am HotSpot frei. Dabei ist nur Datenverkehr mit dem HotSpot Server des Betreibers möglich. Ein öffentliches WLAN wird auf diese Weise ausschließlich für die VPN-Verbindung zum zentralen Datennetz genutzt. Direkter Internet-Zugriff ist ausgeschlossen. Damit die Anmeldeseite des HotSpots im Browser geöffnet werden kann, muss eine eventuelle Proxy-Konfiguration deaktiviert werden.

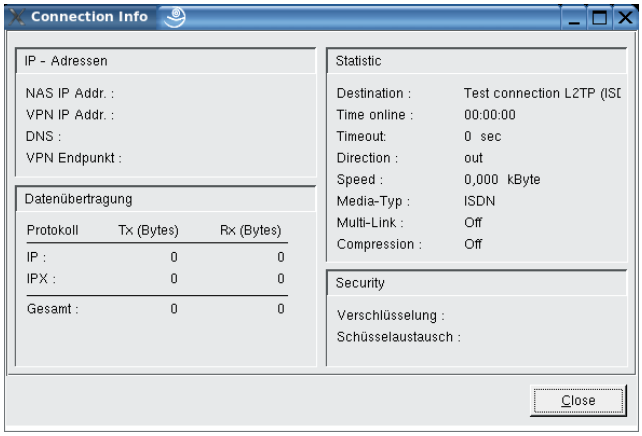
Derzeit unterstützt die HotSpot-Anmeldung des Clients ausschließlich HotSpots, die mit einer Umleitung (Redirect) einer Anfrage mit einem Browser auf die Anmeldeseite des öffentlichen WLAN-Betreibers arbeiten (z.B. T-Mobile oder Eurospot).

Sind obige Voraussetzungen erfüllt, so öffnet ein Klick auf den Menüpunkt “HotSpot-Anmeldung” die Website zur Anmeldung im Standard-Browser. Nach Eingabe der Zugangsdaten kann die VPN-Verbindung z.B. zur Firmenzentrale aufgebaut und sicher kommuniziert werden. Sollte vom Client keine HotSpot-Anmeldung durchgeführt werden, wird dies durch die Meldung “HotSpot konnte nicht gefunden werden” mitgeteilt. Für einen solchen Fall ist zu klären, ob über diesen HotSpot-Betreiber ein generelles Problem in Verbindung mit den von NCP implementierten Mechanismen besteht.

4.1.4 Verbindungs-Informationen

Wenn Sie den Menüpunkt “Verbindungs-Information” anklicken, werden parallel zur animierten Darstellung des Verbindungsaufbaus im Statusfeld zusätzliche Informationen zur Verbindung gelistet. Z.B. welche IP-Adressen über PPP-Verhandlung zwischen Client und Server ausgetauscht werden oder der aktuelle Datendurchsatz.

Die Verbindungs-Informationen können vom Administrator ausgeblendet werden, sodass der Menüpunkt vom Benutzer nicht aktiviert werden kann.



Sind die Verbindungs-Informationen ausgeblendet, so können die wichtigsten Daten aus den Feldern der Datenübertragung, der Statistik und der Sicherheit auch im “Statistik-Anhang” des Clients abgelesen werden (siehe → Fenster, Statistik anzeigen).

- **Verbindungszeit**

Als Verbindungszeit wird die gesamte Zeit angezeigt, während der Sie an ein bestimmtes Zielsystem angewählt sind unabhängig von irgendwelchen Timeouts. Der Wert für die Verbindungszeit wird nur dann auf (0) gesetzt, wenn Sie eine Verbindung zu einem neuen Zielsystem herstellen oder den PC erneut booten.

- **Timeout**

Der Monitor zeigt die Zeit an, die bis zum nächsten Timeout noch verbleibt. Unmittelbar nachdem der letzte Datenaustausch erfolgt ist (einschließlich Handshake) beginnt die Uhr für den Timeout zu laufen. Der Timeout-Wert kann im Telefonbuch unter Line Managment eingestellt werden.

- **Richtung**

Unter dieser Rubrik wird die Richtung der Kommunikation wie folgt angezeigt:

Out	=	ein ausgehender Ruf wird auf diesem Kanal registriert
In	=	ein ankommender Ruf wird auf diesem Kanal registriert.

- **Durchsatz**

Die angezeigte Zahl schwankt entsprechend dem aktuellen Datendurchsatz.

Verbindungsart

Folgende Verbindungsarten werden unterstützt: ISDN-, Modem, LAN over IP, xDSL (PPPoE) und xDSL (AVM - PPP over CAPI).

Multilink

Besteht die Verbindung über mehrere ISDN-B-Kanäle, so wird hier “on” angezeigt.

Kompression

Soll Kompression eingesetzt werden, so muss im Telefonbuch unter “Verbindungssteuerung” die Kompression aktiviert werden. Die Kompression kann nur dann erfolgreich eingesetzt werden, wenn auch das Zielsystem (NAS) die Kompression unterstützt. STAC-Kompression mit History ist CISCO-kompatibel. (IPSec-Kompression wird mit “on” angezeigt.)

Verschlüsselung

Der verwendete Verschlüsselungsalgorithmus wird angezeigt. Folgende Typen werden unterstützt: AES, Blowfish, Triple DES. Die Verschlüsselungsart wird vom Zentralsystem vorgegeben, so dass im Telefonbuch des Clients unter “Security” nur “von Gegenstelle bestimmt” eingegeben werden muss.

Schlüsselaustausch

Hier wird angezeigt, auf welche Art der Austausch des Session Keys erfolgt:

Static Key	Der Schlüssel muss am Client und am Zentralsystem übereinstimmen. Er wird unter “Security → Statischer Schlüssel” eingetragen
SSL	Der zu übertragende Session Key wird mit einem neu generierten Private Key verschlüsselt. Diese Schlüsselverhandlung wird von der Gegenstelle für den Security-Modus L2Sec vorgegeben.
SSL with Certificate	Der Private Key des verwendeten Zertifikats verschlüsselt den Session Key. Diese Schlüsselverhandlung wird von der Gegenstelle vorgegeben und unter “Security → Verschlüsselung (L2Sec)” eingegeben.
IKE (IPSec)	Zur Übertragung des Session Keys wird der verschlüsselte Kontrollkanal der Phase-1-Verhandlung verwendet. (IKE-Richtlinie, siehe → IPSec).

Rx und Tx Bytes

Rx und Tx Bytes zeigt die Datenmenge an, die gesendet (out) und empfangen (in) wird. Die Gesamtmenge (Total) und die nach Protokoll unterschiedenen Datenmnegen werden in Bytes angezeigt (1 Byte = 1 Zeichen). Die Datenübertragung mit den SNA- und NetBIOS-Protokollen ist nur in der Client Software der Enterprise-Version aktiv.

1.4.5 Zertifikate |Verbindung

Im Pulldown-Menü "Verbindung" finden Sie den Menüpunkt "Zertifikate" mit den Menüabzweigungen "Aussteller-Zertifikat anzeigen", "Benutzer-Zertifikat anzeigen", "Eingehendes Zertifikat anzeigen" und "CA-Zertifikate anzeigen".

Wird die Funktionalität der Smart Card genutzt, so wird (ggf. nach dem Tunnelaufbau zwischen Secure Client und VPN-Gateway und) nach der CHAP-Authentisierung (User ID und Passwort) die "Erweiterte Authentisierung" (Strong Authentication) mittels der auf Smart Card und Gateway hinterlegten Zertifikate durchgeführt. Dabei erfolgt die "Erweiterte Authentisierung" und die Verhandlung des Session Keys für das vorher ausgewählte Verschlüsselungsverfahren (siehe → Verschlüsselung, SSL mit Zertifikat) nach dem SSL-Protokoll.

Zertifikate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt und auf eine Smart Card (Chipkarte) gebrannt. Diese Smart Card enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen. Es können Zertifikate eingesetzt werden, die einen privaten Schlüssel bis zu einer Länge von 2048 Bits haben. Als Gegenstelle muss der NCP Secure Server 5.21 oder höher eingesetzt werden.

■ Aussteller-Zertifikat anzeigen

Wenn Sie sich das Aussteller-Zertifikat anzeigen lassen, werden die zur Erstellung des Zertifikats genutzten Merkmale gezeigt, z.B. die eindeutige E-Mail-Adresse.

Aussteller (CA)	=	Benutzer und Aussteller eines Aussteller-Zertifikates sind für gewöhnlich identisch (selfsigned certificate). Der Aussteller des Aussteller-Zertifikats muss mit dem Aussteller des Benutzer-Zertifikats identisch sein (siehe → Benutzer-Zertifikat anzeigen).
Seriennummer	=	Nach der Seriennummer werden die Zertifikate mit den in der Revocation List der Certification Authority gehaltenen verglichen.
Gültigkeitsdauer	=	Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit dem Erlöschen der Gültigkeit des Aussteller-Zertifikats erlischt automatisch die Gültigkeit eines vom gleichen Aussteller ausgestellten Benutzer-Zertifikates.
Fingerprint	=	Der Fingerprint ist ein Hash-Wert, der über das Zertifikat gebildet wird, um dessen Eindeutigkeit mit anderen Zertifikaten vergleichen zu können.

■ Benutzer-Zertifikat anzeigen

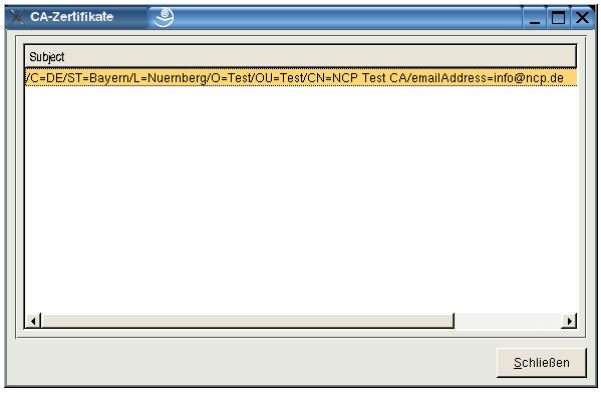
Wenn Sie sich das Aussteller-Zertifikat anzeigen lassen, werden die zur Erstellung des Zertifikats genutzten Merkmale gezeigt, z.B. die eindeutige E-Mail-Adresse.

Aussteller (CA)	=	Der Aussteller Ihres Benutzer-Zertifikates muss mit dem Aussteller des Aussteller-Zertifikates identisch sein. (siehe → Aussteller-Zertifikat anzeigen).
Seriennummer	=	Nach der Seriennummer werden die Zertifikate mit den in der Revokation List der Certification Authority gehaltenen verglichen.
Gültigkeitsdauer	=	Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit Erlöschen der Gültigkeit geht auch die Funktion des Zertifikats verloren.
Fingerprint	=	Der Fingerprint ist ein Hash-Wert, der über das Zertifikat gebildet wird, um dessen Eindeutigkeit mit anderen Zertifikaten vergleichen zu können.

Eingehendes Zertifikat anzeigen

Anzeige des Zertifikats, das bei der SSL-Verhandlung von der Gegenstelle übermittelt wird. Sie können z.B. sehen, ob Sie den hier gezeigten Aussteller in der Liste Ihrer CA-Zertifikate aufgenommen haben.

CA-Zertifikate anzeigen



Die Client Software unterstützt mehrere Aussteller-Zertifikate (Multi CA-Unterstützung). Dazu müssen die Aussteller-Zertifikate im Windows-Verzeichnis NCPLE\CACERTS\ gesammelt werden. Im Monitor wird die Liste der eingespielten CA-Zertifikate angezeigt unter dem Menüpukt “Verbindung -> Zertifikate -> CA-Zertifikate”. (Siehe auch -> Anzeige und Auswertung von Erweiterungen).

Wird das Zertifikat einer Gegenstelle empfangen, so ermittelt der NCP Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis NCPLE\CACERTS\.

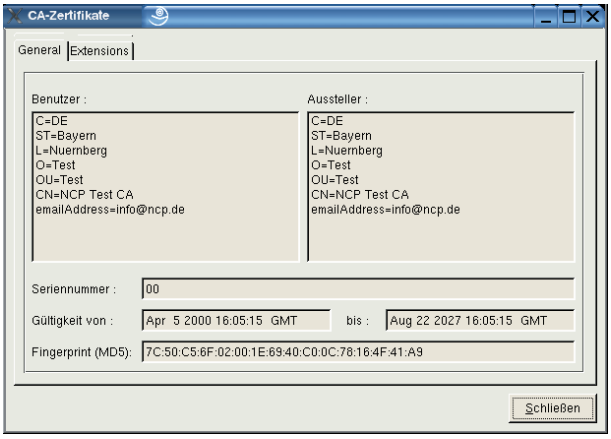
Bitte beachten Sie zum Einspielen eines CA-Zertifikats auch die Beschreibung der erweiterten Installation.

Anzeige und Auswertung von Erweiterungen bei eingehenden Zertifikaten und CA-Zertifikaten

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben. Für den Secure Client und den Secure Server sind drei Erweiterungen von Bedeutung:

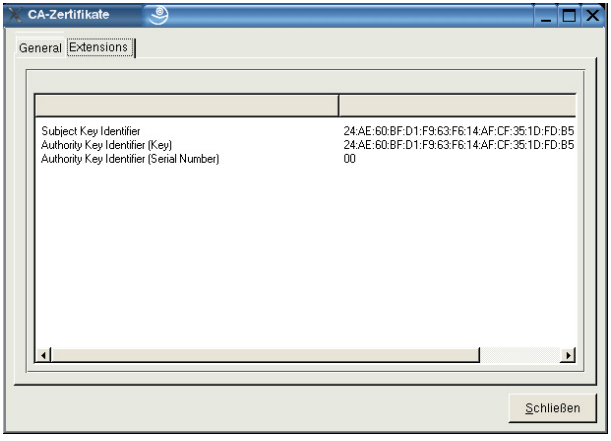
– KeyUsage
– extendedKeyUsage
– subjectKeyIdentifier
– authorityKeyIdentifier
– CPD (Certificate Distribution Point)

Anzeige der Erweiterungen (Extensions)



Um sich die Erweiterungen eines eingehenden oder CA-Zertifikats anzeigen zu lassen, kann wie folgt vorgegangen werden:

Das CA-Zertifikat, dessen Erweiterungen angezeigt werden sollen, muss mit einem Doppelklick im Fenster für CA-Zertifikate (siehe oben) geöffnet werden. Damit wird nebenstehendes Anzeigefeld mit den allgemeinen Daten (General) geöffnet.



Für das jeweils eingehende Zertifikat wird dieses Feld bereits geöffnet, nachdem “Eingehendes Zertifikat anzeigen” im Zertifikats-Menü gewählt wurde.

Das Ansichtsfeld “General” zeigt die allgemeinen Zertifikatsdaten (siehe Bild oben).

Das Ansichtsfeld “Extensions” zeigt die Zertifikatserweiterungen, sofern sie vorhanden sind (siehe Bild links).

Auswertung der Erweiterungen (Extensions)

KeyUsage

Ist in einen eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:
– Digital Signatur
– Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
– Key Aggrenment (Schlüsselaustaschverfahren)
Ist eines des Bits nicht gesetzt, wird die Verbindung abgebaut.

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Secure Client, ob der definierte erweiterte Verwendungszweck die “SSL-Server-Authentisierung” ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

Ausnahme: Bei einem Rückruf des Servers an den Client nach einer Direkteinwahl ohne VPN aber mit PKI prüft der Server das Zertifikat des Clients auf die Erweiterung extendedKeyUsage. Ist diese vorhanden, muss der Verwendungszweck “SSL-Server-Authentisierung” beinhaltet sein, sonst wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festgestellt, dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Verzeichniss ncple\crls gespeichert.

HTTP Proxy für CRL Download

In der Datei NCPPKI.CONF im Installationsverzeichnis kann in der Gruppe “HttpProxy” ein Proxy für den CRL Download über HTTP konfiguriert werden:

```
[HttpProxy]
ProxyHost = xxx.xxx.xxx.xxx
#IP Adresse des Proxy Server für CRL Download über
HTTP
ProxyPort = 80
#Port des Proxy Server für CRL Download über HTTP
ProxyUser = xyz
#Benutzername des Proxy Server für CRL Download
über HTTP
ProxyPw = xxxx
#Passwort des Proxy Server für CRL Download über
HTTP
```

Auswertung von CRLs und ARLs

Der Secure Client kann auch Revocation-Lists auswerten. Folgende Listen werden unterstützt:

- ☐ Certificate Revocation List (CRL)
- ☐ Authority Revocation List (ARL)

Die CRLs bzw. ARLs müssen in die entsprechenden Unterverzeichnisse des NCPLE-Verzeichnisses nach “\CRL” bzw. “\ARL” kopiert werden.

■ Hardware-Zertifikat

Wenn Sie ein Hardware-Zertifikat zur Authentisierung Ihres Rechners benutzen, können Sie sich an dieser Stelle dessen Merkmale anzeigen lassen. Es sind die gleichen Merkmale wie sie oben bei “Benutzer-Zertifikat anzeigen” beschrieben sind.

4.1.6 PIN eingeben

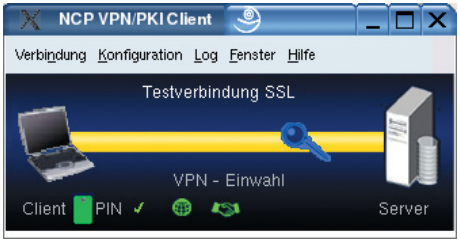
Die PIN-Eingabe kann vor einem Verbindungsaufbau erfolgen, nachdem der Monitor gestartet wurde. Wird zu einem späteren Zeitpunkt eine Verbindung aufgebaut, die ein Zertifikat erfordert, so kann dann die PIN-Eingabe unterbleiben – es sei denn, die Konfiguration zum Zertifikat verlangt es (siehe → Konfiguration, Zertifikat).

Wenn Sie den VPN/PKI Client zur Verwendung einer Smart Card konfiguriert haben (siehe → Konfiguration, Zertifikate), erscheint im Statusfeld ein hellblaues Symbol für die Smart Card. Wenn Sie Ihre Smart Card in das Lesegerät gesteckt haben, ändert sich die Farbe des Symbols von hellblau zu grün. (Bild links)

Sobald Sie die erste Verbindung aufbauen wollen, für die ein Zertifikat genutzt wird, wird ein Dialog zur PIN-Eingabe geöffnet – sofern Sie die PIN noch nicht vorher eingegeben haben. Bei einem wiederholten manuellen Verbindungsaufbau kann die PIN-Eingabe unterbleiben, wenn nicht anders konfiguriert (siehe → Konfiguration, Zertifikat).

Wird ein Soft-Zertifikat verwendet, so kann die PIN 4-stellig ein. Wird eine Chipkarte verwendet, muss die PIN mindestens 6-stellig sein.

Fehlerhafte Eingaben und falsche PINs werden nach ca. 3 Sekunden mit einer Fehlermeldung quittiert. Ein Verbindungsaufbau ist dann nicht möglich. Nach dreimaliger fehlerhafter Eingabe der PIN, wird die PIN gesperrt! Wenden Sie sich in diesem Fall an Ihren Remote-Administrator. Wenn die Chipkarte während des laufenden Betriebs entfernt wird, findet ein Verbindungsabbau statt.



Erst nach korrekter PIN-Eingabe erfolgt der Verbindugsaufbau. (Bild links)

4.1.7 PIN zurücksetzen

Dieser Menüpunkt kann gewählt werden, um die PIN zu löschen, d.h. um die aktuell gültige PIN für einen anderen Benutzer unbrauchbar zu machen. Dies kann dann sinnvoll sein, wenn der Aebeitsplatz vorübergehend verlassen wird oder wenn der Benutzer gewechselt wird. Danach muss erneut eine gültige PIN eingegeben werden, um eine Authentisierung durchführen zu können.

- **PIN-Status im Client Monitor**

Wurde die PIN bereits eingegeben, erscheint im Monitor die Einblendung “PIN” mit einem grünen Haken. Wurde die PIN noch nicht korrekt eingegeben, fehlt der kleine grüne Haken.

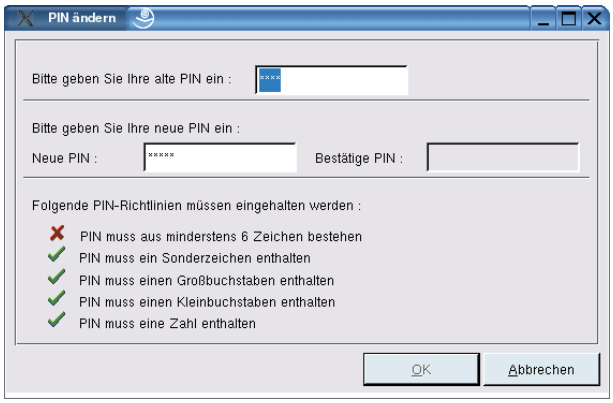
- **PIN-Eingabezwang nach Abmeldung oder Sleep-Mode**

Wird unter den Betriebssystemen Windows NT/2000/XP der Benutzer gewechselt, wird der PIN-Status zurückgesetzt und die PIN muss erneut eingegeben werden. Wechselt der Computer in den Sleep-Modus, wird ebenfalls der PIN-Status zurückgesetzt.

- **Anzeige der Meldungen des ACE-Servers für RSA-Token**

Werden vom ACE-Server auf Grund des RSA-Tokens Nachrichten versendet, werden diese am Monitor in einem Eingabefeld angezeigt (z.B. “Ablauf der gültigen PIN”).

4.1.8 PIN ändern (für Smart Cards und Soft-Zertifikate)



Unter dem Menüpunkt “PIN ändern” kann die PIN für eine Smart Card oder ein Soft-Zertifikat geändert werden, wenn vorher die richtige PIN eingegeben wurde.

Ohne die vorherige Eingabe einer gültigen PIN wird dieser Menüpunkt nicht aktiviert.

Einzuhaltende PIN-Richtlinien werden unter den Eingabefeldern eingeblendet und mit einem roten Kreuz markiert (Bild oben).

Sie können im Hauptmenü unter “Konfiguration – Zertifikate – PIN-Richtlinien” eingestellt werden. Die Richtlinien können vom Anwender nicht vorgegeben werden, wenn im Hauptmenü unter “Konfiguration – Zertifikat” ein “Entrust-Profil” gewählt wurde.

Während der Eingabe einer neuen PIN wird vor die jeweils erfüllten Richtlinien das rote Kreuz durch einen grünen Haken ausgetauscht (Bild oben).

4.1.9 Parametersperre aufheben

Dieser Menüpunkt erscheint nur, wenn die Konfiguration durch den Administrator vorgegeben wurde. Diverse Parameterfelder oder einzelne Parameter, die für Ihren Anschluss nicht von Bedeutung sind, können vom Systemadministrator ausgeblendet werden. Sie sind dann im Telefonbuch nicht mehr sichtbar.

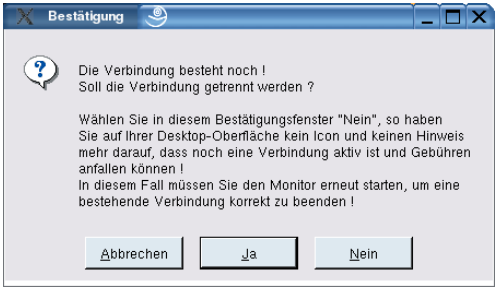
Um die Parameter wieder einzublenden, wählen Sie diesen Menüpunkt. Nach Eingabe von User ID und Passwort des Administrators werden die Sperren aufgehoben.

Danach erscheint der Menüpunkt Sperre wieder herstellen.

4.1.10 Beenden (des Monitors)

Wurde die Verbindung bereits getrennt, beendet ein Klick auf diesen Menüpunkt oder den Schließen-Button den Monitor.

Besteht noch eine Verbindung, kann nach Klick auf diesen Menüpunkt oder den Schließen-Button der Monitor ebenfalls beendet werden. Beachten Sie jedoch unbedingt, dass die Verbindung dabei nicht automatisch getrennt wird. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung von der Software verlangt (siehe Bild unten).



Klicken Sie in diesem Bestätigungsfenster auf “Nein”, so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um eine bestehende Verbindung korrekt zu beenden!

4.2 Konfiguration

Unter diesem Menüpunkt können sämtliche Einstellungen für die Arbeit mit dem Secure Client vorgenommen werden. Dies betrifft das Anlegen der Zielsysteme im Telefonbuch, die SPD-Konfiguration für IPSec-Verbindungen, die Wahl der Verbindungsart, sowie die Eingabe einer Amtsholung für Anschlüsse an Telekommunikationsanlagen.

Darüber hinaus kann eigens konfiguriert werden, wie Zertifikate genutzt werden sollen, wie die Verbindungssteuerung arbeiten soll und welche Rechte der Administrator für den Remote-Zugriff auf den Client erhält.

Sollte mit einer remote eingespielten Update-Konfiguration die Verbindung zu einem Ziel nicht mehr möglich sein und damit auch eine Korrektur vom Update Server verhindert werden, so kann durch Laden der letzen Konfiguration eine lauffähige Konfiguration des Clients wieder hergestellt werden.

4.2.1 Telefonbuch

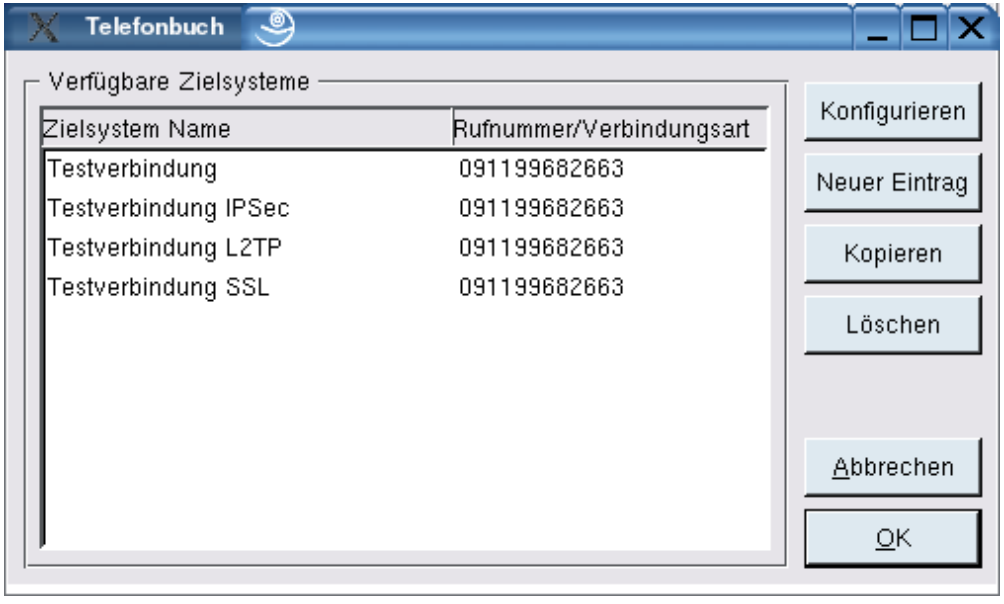
Die Einträge des Telefonbuchs

Bei einer Erstinstallation der Secure Client Software ist noch kein Telefonbuch vorhanden. In diesem Fall wird automatisch ein Assistent (siehe → Assistent für erste Konfiguration) eingeblendet, der Ihnen hilft, Test-Konfigurationen anzulegen. Damit wird zugleich das erste Telefonbuch der Secure Client Software angelegt, deren Einträge Sie nach belieben modifizieren können.

Das Telefonbuch des Monitors ist besonders leistungsstark. Mit ihm können die Zielsysteme definiert und die Übertragungsart, den Benutzeranforderungen entsprechend, bis ins Detail konfiguriert werden.

Nachdem Sie auf “Telefonbuch” in der Menüleiste des Monitors geklickt haben (oder auf das Telefonbuch-Icon in der Werkzeugleiste), öffnet sich das Telefonbuch und zeigt in einer Liste der bereits verfügbaren Zielsysteme die Namen der definierten Zielsysteme und deren Rufnummern.

Ohne definiertes Zielsystem kann keine Verbindung aufgebaut werden. Ein Zielsystem ist definiert, wenn es als neuer Eintrag im Telefonbuch angelegt wird (siehe → Neuer Eintrag, Zielsystem).



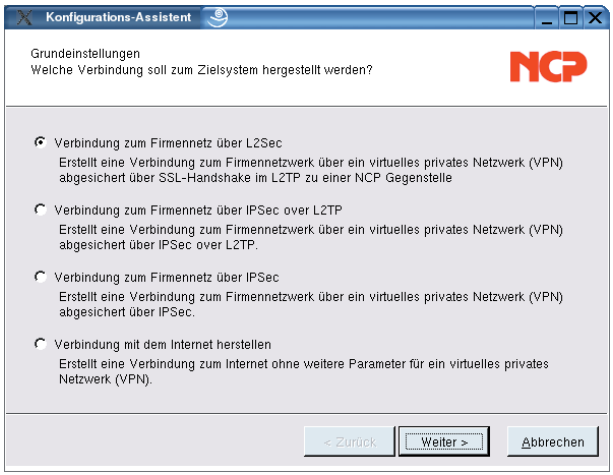
Auf der rechten Seite des Telefonbuchs sind Buttons angebracht zu folgenden Funktionen: Konfigurieren, Neuer Eintrag, Kopieren, Löschen, OK, Hilfe und Abbrechen.

Zur Konfiguration beachten Sie bitte die Beschreibung der “Konfigurationsparameter”!

Neuer Eintrag – Zielsystem (Konfigurations-Assistent)

Um ein neues Zielsystem zu definieren, klicken Sie in der Menüleiste auf “Telefonbuch”. Das Fenster des Telefonbuchs öffnet sich nun und zeigt die bereits definierten Zielsysteme.

Klicken Sie jetzt auf “Neuer Eintrag”. Jetzt legt der “Konfigurations-Assistent” mit Ihrer Hilfe ein neues Zielsystem an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Zielsystem angelegt. Für alle weiteren Parameterfelder des Telefonbuchs werden Standardwerte eingetragen, die Sie unter dem Menüpunkt “Konfigurieren” (siehe → Konfigurieren, Zielsystem) auch ändern können.



Mit dem Konfigurations-Assistenten können Verbindungen mit dem Internet oder, je nach erforderlichem VPN-Übertragungsprotokoll, zum Firmennetz rasch hergestellt werden. Je nach Auswahl der gewünschten Grundeinstellung wird das Zielsystem nach wenigen Konfigurationsabfragen im Telefonbuch angelegt.

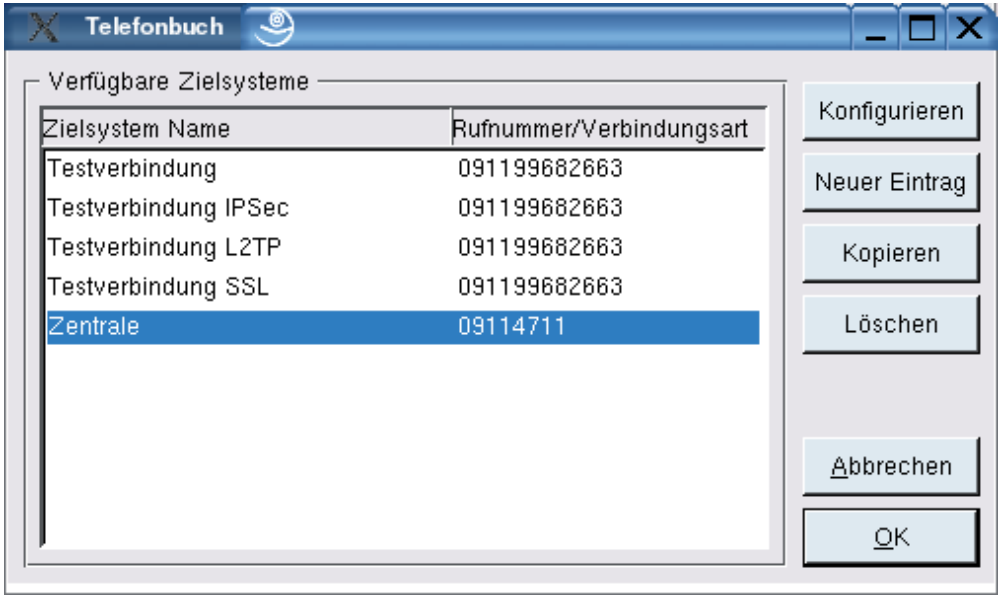
Im folgenden die jeweils nötigen Daten zur Konfiguration:

Verbindung zum Firmennetz über L2Sec:
→ Name des Zielsystems
→ Verbindungsart
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzername, Kennwort, Rufnummer)
→ VPN-Gateway-Parameter (VPN-Gateway, Tunnelsecret, Kompression)
→ Nutzung von Zertifikaten
→ Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)
→ Statischer Schlüssel (Preshared Key) sofern kein Zertifikat eingesetzt wird

Verbindung zum Firmennetz über IPSec over L2Sec:
→ Name des Zielsystems
→ Verbindungsart
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)
→ VPN-Gateway-Parameter (VPN-Gateway, Tunnelsecret)
→ Nutzung von Zertifikaten
→ Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)
→ Statischer Schlüssel (Preshared Key) sofern kein Zertifikat eingesetzt wird

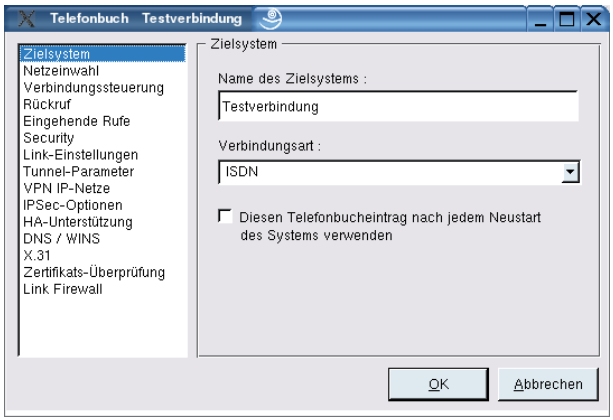
Verbindung zum Firmennetz über IPSec:
→ Name des Zielsystems
→ Verbindungsart
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)
→ VPN-Gateway-Parameter (VPN-Gateway, Tunnelsecret)
→ Nutzung von Zertifikaten
→ Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)
→ Statischer Schlüssel (Preshared Key), ohne Zertifikat (IKE ID-Typ, IKE ID)

Verbindung mit dem Internet herstellen:
→ Name des Zielsystems
→ Verbindungsart
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)



Das neue Zielsystem erscheint nun in der Liste der Zielsysteme im Telefonbuch mit dem von Ihnen vergebenen Namen. Wenn keine weiteren Parameter-Einstellungen nötig sind, können Sie das Telefonbuch mit Ok schließen. Das neue Zielsystem ist im Monitor sofort verfügbar. Es kann im Monitor ausgewählt werden und über das Menü “Verbindung → Verbinden” sofort angewählt werden.

Konfigurieren – Zielsystem



Um die (Standard-)Werte eines Zielsystems zu editieren, d.h. Parameter so einzustellen oder abzuändern, wie es den Verbindungsanforderungen zum definierten Zielsystem entspricht, wählen Sie mit der Maus das Zielsystem, dessen Werte Sie ändern möchten, aus dem Telefonbuch aus und klicken anschließend auf “Konfigurieren”.

Das Telefonbuch zeigt nun in seinem linken Fenster eine Liste von Begriffen, denen jeweils ein Parameterfeld zugeordnet ist. Abhängig von der konfigurierten “Verbindungsart” zum Ziel (siehe Abbildung oben “ISDN”) zeigt das Telefonbuch nicht immer alle Begriffe.

Je nachdem, welchen Begriff Sie markieren, zeigt sich das entsprechende Feld mit den zugehörigen Parametern (siehe → Konfigurationsparameter), in der obigen Abbildung “Zielsysem”.

Ok – Zielsystem

Die Konfiguration eines Zielsystems ist abgeschlossen, wenn Sie das Konfigurationsfenster des Telefonbuchs mit OK schließen. Das neue oder geänderte Zielsystem ist im Monitor sofort verfügbar. Es kann im Monitor ausgewählt werden und über das Menü “Verbindung → Verbinden” sofort angewählt werden.

Bitte beachten Sie, dass je nach Verbindungsart auch der zugehörige Treiber im Menü des Monitors über “Verbindung → Verbindungsart” geladen werden muss. Ist der entsprechende Treiber dort noch nicht ausgewählt, klicken Sie ihn an, schließen Sie den Monitor und starten Sie Ihr System neu. (Vgl. auch den Parameter “Verbindungsart”)

Bitte beachten Sie auch, wenn Sie das TCP/IP-Protokoll benutzen und nicht IP Network Address Translation (siehe → Link-Einstellungen, IP Network Address Tranlation) verwenden, dass es nötig sein kann, die Einstellungen Ihres Windows-Systems zu ändern. Die Änderungen betreffen die Protokolleigenschaften für TCP/IP. Vorzunehmen im Windows Startmenü unter “Start → Einstellungen → Systemsteuerung → Netzwerk → Konfiguration”. Die dort vorgenommenen Eintragungen müssen mit denen im Telefonbuch übereinstimmen. Dies betrifft insbesondere:

☑ die IP-Adresse (nicht nötig wenn DHCP genutzt wird)

☑ die Subnet Mask-Adresse:(nicht nötig wenn DHCP genutzt wird)

☑ die DNS Konfiguration: (Host-Name, Domane-Name und DNS Server Adresse)

☑ die Gateway Adresse

■ Kopieren – Zielsystem

Um die Parameter-Einstellungen eines bereits definierten Zieles zu kopieren, markieren sie das zu kopierende Zielsystem im Telefonbuch und klicken Sie auf den Kopieren-Button. Daraufhin wird das Zielsystem-Parameterfeld geöffnet. Ändern Sie nun den Eintrag in “Name Zielsystem” und klicken Sie anschließend Ok. Nur wenn Sie den Namen des Zielsystems ändern kann es auch als neuer Eintrag eines Zielsystems im Telefonbuch vermerkt werden.

Ein kopiertes Zielsystem muss einen neuen, noch nicht vergebenen, Namen erhalten. Nur so kann es im Telefonbuch abgelegt werden.

■ Löschen – Zielsystem

Um ein Zielsystem zu löschen, wählen Sie es aus und klicken den Löschen-Button.

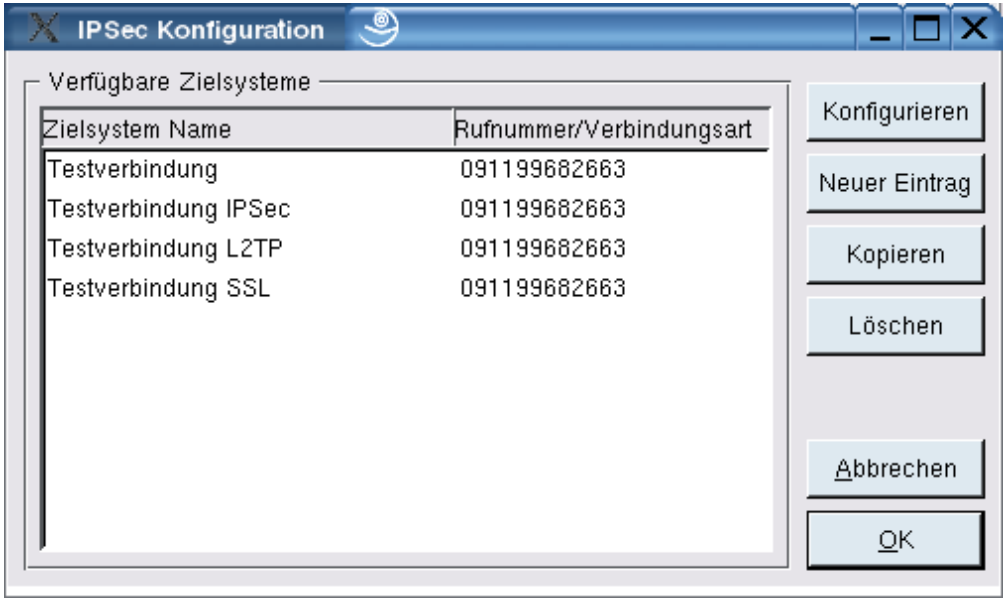
4.2.2 IPSec

Die Einträge der IPSec-Konfiguration

Zur Konfiguration der Richtlinien und gegebenenfalls einer statischen Secure Policy Database wird dieser Menüpunkt angeklickt. Damit öffnet sich ein Konfigurationsfenster mit der Verzweigung der Richtlinien und Secure Policy Database zu IPSec, sowie Buttons zur Bedienung auf der rechten Seite des Konfigurationsnfensters.

Der Secure Client wird mit vorkonfigurierten IKE-Richtlinien (Pre-shared Key / RSA-Signatur) und einer IPSec-Richtlinie (ESP-3DES-MD5) ausgeliefert.

Um die (Standard-)Werte der Richtlinien zu editieren, d.h. Parameter so einzustellen oder abzuändern, wie es den Verbindungsanforderungen zum definierten Zielsystem entspricht, wählen Sie mit der Maus die Richtlinie, deren Werte Sie ändern möchten – die Buttons zur Bedienung werden dann aktiv.



Auf der rechten Seite der IPSec Konfiguration sind Buttons angebracht zu folgenden Funktionen: Konfigurieren, Neuer Eintrag, Kopieren, Löschen, Schließen.

Zur Konfiguration beachten Sie bitte die Beschreibung der "Konfigurationsparameter"! (Siehe → Konfigurationsparameter, IPSec)

Konfigurieren – IPSec

Um eine Richtlinie oder eine SPD abzuändern, wählen Sie mit der Maus den Namen, der Gruppe deren Werte Sie ändern möchten und klicken auf “Konfigurieren”. Dann öffnet sich das entsprechende Parameterfeld mit den IPSec-Parametern.

Neuer Eintrag – IPSec

Wenn Sie eine neue Richtlinie oder SPD anlegen möchten, selektieren Sie eine der Richtlinien oder die SPD und klicken auf “Neuer Eintrag”. Die neue Richtlinie oder SPD wird erzeugt. Alle Parameter sind auf Standardwerte gesetzt, bis auf den Namen.

Kopieren – IPSec

Um die Parameter-Einstellungen eines bereits definierten Richtlinie oder SPD zu kopieren, markieren sie die zu kopierende Richtlinie oder SPD und klicken auf “Kopieren”. Daraufhin wird das Parameterfeld geöffnet. Ändern Sie nun den Namen und klikken Sie anschließend Ok. Die neue Richtlinie oder SPD ist nun angelegt. Die Parameterwerte sind zu denen der kopierten identisch, bis auf den Namen.

Löschen – IPSec

Wenn Sie eine Richtlinie oder SPD aus dem Konfigurationsbaum löschen wollen, selektieren Sie sie und klicken auf “Löschen”. Die Richtlinie oder SPD ist damit auf Dauer aus der IPSec-Konfiguration gelöscht.

Schließen – IPSec

Wenn Sie das IPSec-Feld schließen, kehren Sie zum Monitor zurück. Die Daten werden so wie sie konfiguriert wurden behalten.

4.2.3 Firewall-Einstellungen

Alle Firewall-Mechanismen sind optimiert für Remote Access-Anwendungen und werden bereits beim Start des Rechners aktiviert. D.h. im Gegensatz zu VPN-Lösungen mit eigenständiger Firewall ist der Telearbeitsplatz bereits vor der eigentlichen VPN-Nutzung gegen Angriffe geschützt.

Die Firewall bietet auch im Fall einer Deaktivierung der Client-Software vollen Schutz des Endgerätes. Alle Firewall-Regeln können zentral vom Administrator vorgegeben und deren Einhaltung erzwungen werden. Voraussetzung hierfür ist das zentrale NCP Secure Enterprise Management, mit dessen Hilfe die Konfiguration des Clients fest, für den Anwender nicht änderbar, vorgegeben werden kann.

Bitte beachten Sie, dass die Firewall-Einstellungen global, d.h. für alle Zielsysteme des Telefonbuchs gültig sind.

Dagegen ist die Einstellung der Link Firewall, die im Telefonbuch vorgenommen werden kann, nur für den dazu gehörenden Telefonbuch-Eintrag (Zielsystem) und die Verbindung zu diesem Zielsystem wirksam.

Eigenschaften der Firewall

Die Firewall arbeitet nach dem Prinzip der Paketfilterung in Verbindung mit Stateful Packet Inspection (SPI). Die Firewall prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis des konfigurierten Regelwerks, ob ein Datenpaket weitergeleitet oder verworfen wird.

Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen wird der unbefugte Zugriff auf Daten und Ressourcen im zentralen Datennetz verhindert. Zum anderen wird mittels Stateful Inspection der jeweilige Status bestehender Verbindungen überwacht. Die Firewall kann darüber hinaus erkennen, ob eine Verbindung "Tochterverbindungen" geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Wird eine Regel für eine ausgehende Verbindung definiert, die einen Zugriff erlaubt, so gilt die Regel automatisch für entsprechende Rückpakete. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf.

Die Firewall-Regeln können dynamisch konfiguriert werden, d.h. ein Anhalten der Software oder ein Reboot ist nicht nötig.

Die Firewall-Einstellungen im Konfigurationsmenü des Client-Monitors gestatten eine genauere Spezifikation von Firewall-Filterregeln. Sie wirken global. D.h. unabhängig vom aktuell gewählten Zielsystem werden immer zuerst die Regeln der erweiterten Firewall-Einstellungen abgearbeitet, bevor die Regeln der Firewall aus dem Telefonbuch angewendet werden.

Eine Kombination der globalen und link-bezogenen Firewall kann in bestimmten Szenarien durchaus sinnvoll sein. Im Allgemeinen sollten jedoch nahezu alle Anforderungen über die globalen Einstellungmöglichkeiten abzudecken sein.

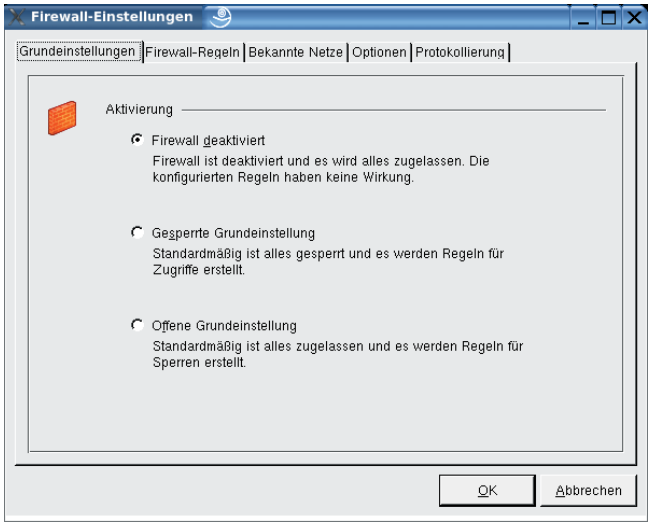
Bitte beachten Sie, dass die link-bezogenen Firewall-Einstellungen bei Aktivierung Vorrang den globalen haben. Ist z.B. die Link-Firewall auf "immer" und "Ausschließlich Kommunikation im Tunnel zulassen" eingestellt, kann trotz evtl. anders lautender Regeln der globalen Konfiguration nur ein Tunnel aufgebaut und darüber kommuniziert werden. Jeglicher anderer Verkehr wird von der Link-Firewall verworfen.

Konfiguration der Firewall-Einstellungen

Die Filterregeln der erweiterten Firewall können sowohl anwendungsbezogen als auch (zusätzlich) adressorientiert, bezüglich bekannter/unbekannter Netze, definiert werden.

Um Konflikte zwischen den Regeln der verbindungsorientierten Firewall des Telefonbuchs und der erweiterten Firewall zu vermeiden, wird empfohlen, die Firewall des Telefonbuchs auf "inaktiv" zu schalten, wenn die erweiterte Firewall eingesetzt wird. Die IP-Adressen der jeweiligen Verbindung (zum Ziel-Gateway) können stattdessen in den Filterregeln der erweiterten Firewall eingesetzt werden.

Konfigurationsfeld Grundeinstellungen



In den Grundeinstellungen wird festgelegt, mit welcher Basis-Policy die Firewall arbeiten soll.

© NCP engineering GmbH

Firewall deaktiviert

Wird die erweiterte Firewall deaktiviert, so wird in diesem Kompatibilitätsmodus nur die im Telefonbuch konfigurierte Firewall genutzt. Dies bedeutet, dass alle Datenpakete nur über die Sicherheitsmechanismen dieser verbindungsorientierten Firewall abgearbeitet werden.

Gesperrte Grundeinstellung (empfohlen)

Wird diese Einstellung gewählt, so sind die Sicherheitsmechanismen der Firewall immer aktiv. D.h. ohne zusätzlich konfigurierte Regeln wird jeglicher IP-Datenverkehr unterbunden.

Ausgenommen sind die Datenpakete, die durch eigens erstellte, aktive Firewall-Regeln gestattet (durchgelassen) werden (Permit Filter). Trifft eine der Eigenschaften eines Datenpakets auf die Definition einer Firewall-Regel zu, wird an dieser Stelle die Abarbeitung der Filterregeln beendet und das IP-Paket weitergeleitet.

Im Modus der gesperrten Grundeinstellung kann auf komfortable Weise eine L2Sec/IPSec-Tunnelkommunikation freigeschaltet werden.

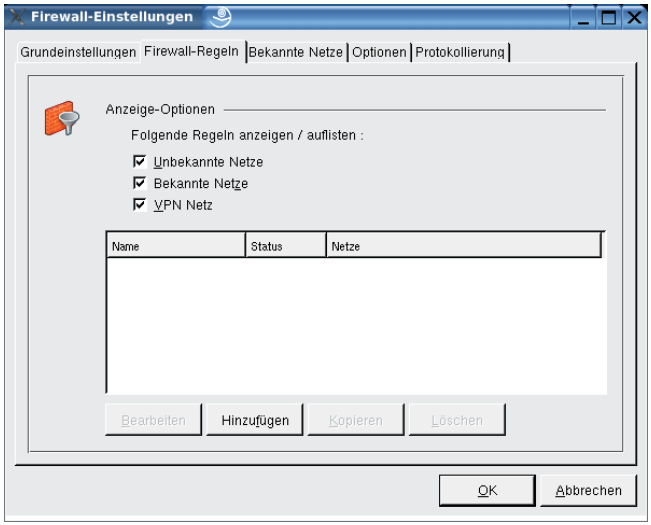
Dazu kann im Konfigurationsfeld “Optionen” der Datenverkehr über VPN-Protokolle (L2Sec, IPSec) global zugelassen werden.

Offene Grundeinstellung

In der offenen Grundeinstellung sind zunächst alle IP-Pakete zugelassen. Ohne weitere Filterregeln werden alle IP-Pakete weitergeleitet.

Ausgenommen sind die Datenpakete, die durch eigens erstellte, aktive Firewall-Regeln ausgefiltert (nicht durchgelassen) werden (Deny Filter). Trifft eine der Eigenschaften eines beim Server/Client ankommenden IP-Pakets auf die Definition eines Deny-Filters zu, wird an dieser Stelle die sequentielle Abarbeitung der Filterregeln beendet und das IP-Paket von der Weiterleitung ausgeschlossen. Daten-Pakete, die auf keinen passenden Deny-Filter treffen, werden weitergeleitet.

Konfigurationsfeld Firewall-Regeln



In diesem Konfigurations-fenster werden die Regeln für die Firewall zusam-mengestellt. Die Anzeige-Optionen sind standard-mäßig alle aktiv. Mittels dieser wird eingestellt, welche Regeln in Abhängig-keit ihrer Zuordnung in der Übersicht angezeigt werden:

– unbekannte Netze
– bekannte Netze
– VPN-Netze
– anwendungsabhängig,
– unabhängig

Diese Auswahlfelder für die Anzeigen der Regeln dienen nur der Übersichtlichkeit und haben keine Auswirkung auf die Anwendung einer Filterregel. Für jede definierte Regel werden die wichtigsten Eigenschaften gezeigt:

– Name
– Status
– Netz
– Anwendung

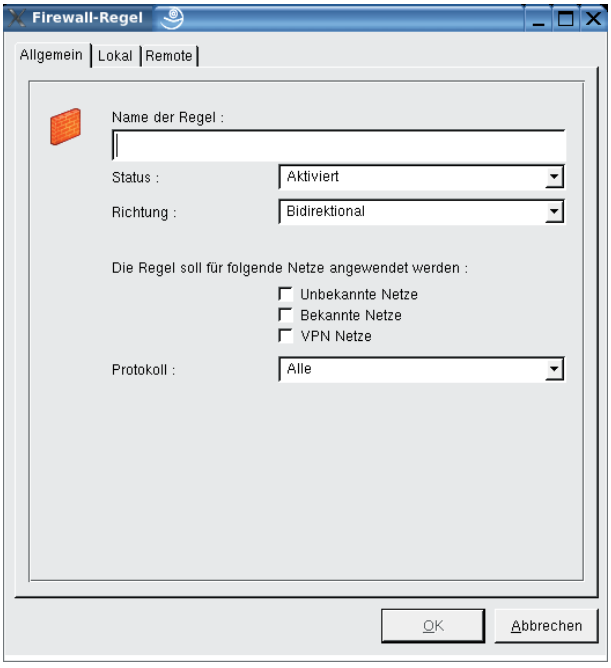
Durch Klick auf diese Eigenschafts-Buttons können die eingeblendeten Regeln sortiert werden.

Erstellen einer Firewall-Regel

Über die Buttons unterhalb der Anzeigezeilen werden die Regeln erzeugt oder bearbeitet. Um eine Firewall-Regel zu erstellen, klicken Sie auf “Hinzufügen”. Die Erstellung einer Filterregel erfolgt über vier Konfigurationsschritte bzw. Registerkarten:

– Allgemein: In diesem Konfigurationsfeld wird festgelegt für welche Netze und welches Protokoll die Regel gelten soll.
– Lokal: In diesem Konfigurationsfeld werden die Werte der lokalen Ports und IP-Adressen eingetragen.
– Remote: Im Remote-Feld werden die Port- und Adress-Werte der Gegenseite eingetragen.
– Anwendungen: In diesem Konfigurationsfeld kann die Regel einer oder mehrerer Anwendungen zugeordnet werden.

Firewall-Regel / Allgemein



Einzelregeln stellen immer Ausnahmen von der Grundeinstellung dar (siehe → Grundeinstellung).

Name der Regel

Mit diesem Namen erscheint die Regel in der Anzeigeliste.

Status

Die Regel wird nur dann auf Datenpakete angewendet, wenn der Status “aktiv” ist.

Richtung

Mit der Richtung geben Sie an, ob diese Regel für eingehende oder ausgehende Datenpakete gelten soll. Wird die Richtung auf ausgehend gesetzt, wird nach dem Prinzip von Stateful Inspectiongearbeitet (siehe → Eigenschaften der Firewall). Stateful Inspection wird jedoch nur für die Protokolle UDP und TCP angewendet.
Auf “eingehend” kann z.B. dann geschaltet werden, wenn von Remote-Seite eine Verbindung aufgebaut werden soll (z.B. für “eingehende Rufe” oder Administrator-Zugriffe).
Die Einstellung “bidirektional” ist nur sinnvoll, wenn Stateful Inspection nicht zur Verfügung steht, z.B. für das ICMP-Protokoll (bei einem Ping).

Die Regel soll für folgende Netze angewendet werden

Beim Neuanlegen einer Regel ist diese zunächst keinem Netz zugeordnet. Eine Regel kann erst dann gespeichert werden, wenn die gewünschte Zuordnung erfolgt ist und ein Name vorgegeben wurde.
Unbekannte Netze
– sind alle Netze (IP-Netzwerkschnittstellen), die weder einem bekannten noch einem VPN-Netz zugeordnet werden können. Darunter fallen z.B. Verbindungen über das DFÜ-Netzwerk von Microsoft oder auch direkte und unverschlüsselte Verbindungen mit dem integrierten Dialer des Clients, wie auch HotSpot WLAN-Verbindungen. Soll eine Regel für unbekannte Netze gelten, so muss diese Option aktiviert werden.

Bekannte Netze
– werden im gleichnamigen Register im Fenster “Firewall-Einstellungen” definiert. Solle eine Regel für bekannte Netze gelten, muss diese Option aktiviert werden.
VPN-Netze
– sind alle L2Sec- oder IPSec-Verbindungen in aufgebautem Zustand. Darüber hinaus fallen unter diese Gruppe auch alle verschlüsselten Direkteinwahlverbindungen über den integrierten Dialer des Clients. Solle eine Regel für VPN-Netze gelten, so muss diese Option aktiviert werden.

Protokoll

Je nach Anwendung oder Art der Verbindung ist das entsprechende Protokoll zu wählen:

TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 oder IPv4, Alle

MAC-Adresse

Die MAC-Adresse ist weltweit eindeutig und lässt bei eingehenden Verbindungen nur Datenpakete zu, die von dem Gateway mit dieser MAC-Adresse stammen. Bei einer ausgehenden Verbindung wird unter Angabe der MAC-Adresse des Ziel-Gateways sichergestellt, dass der Client nur eine Verbindung zu diesem Ziel-Gateway aufbauen kann. Nach Aufbau einer VPN-Verbindung über dieses Gateway hat der Client Zugriff auf das Firmennetz je nach konfiguriertem Link-Profil. Dies ist eine sehr restriktive Regel, die sich nur in ganz speziellen Situationen anwenden lässt.

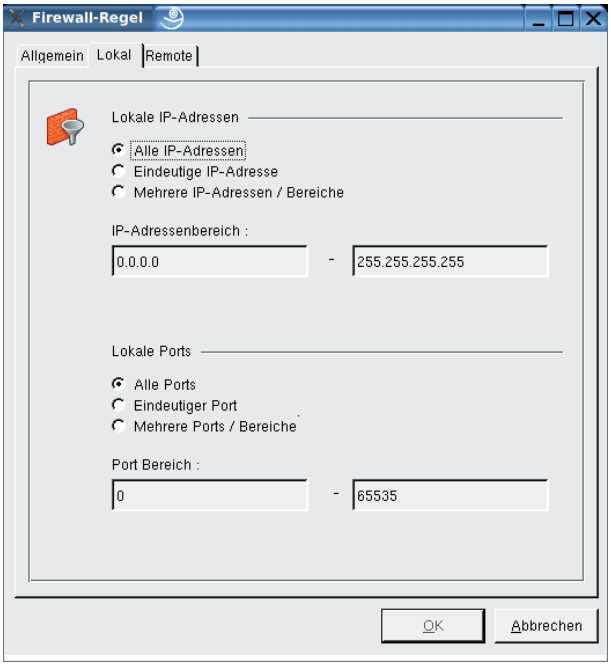
Verbindungssteuerung

Über diese Parameter wird die Art der Verbindung beeinflusst.

Sie wählen z.B. die Option, dass die hier konfigurierte Regel “nur gültig bei inaktiver VPN-Verbindung” ist, wenn Sie wünschen, dass z.B. eine Internet-Verbindung bei gleichzeitig bestehender VPN-Verbindung ausgeschlossen wird, ansonsten aber Internet-Verbindungen zu unbekannten Netzen zugelassen sein sollen. Dazu muss diese Regel für “unbekannte Netze” angewendet werden, d.h. diese Regel muss den Zugang zu unbekannten Netzen zulassen.

Die Option “kein automatischer Verbindungsaufbau” steht nur bei gesperrter Grundeinstellung zur Verfügung. Sie ist nur sinnvoll, wenn im Telefonbuch im Parameterfeld “Verbindungssteuerung” der Verbindungsaufbau auf “automatisch” gestellt wurde. Für die über diese Regel definierten Datenpakete findet bei Aktivierung dieser Funktion kein automatischer Verbindungsaufbau statt, für andere Datenpakete schon.

Firewall-Regel / Lokal



Auf dieser Registerkarte werden die Filter für die lokalen IP-Adressen und IP-Ports eingestellt.

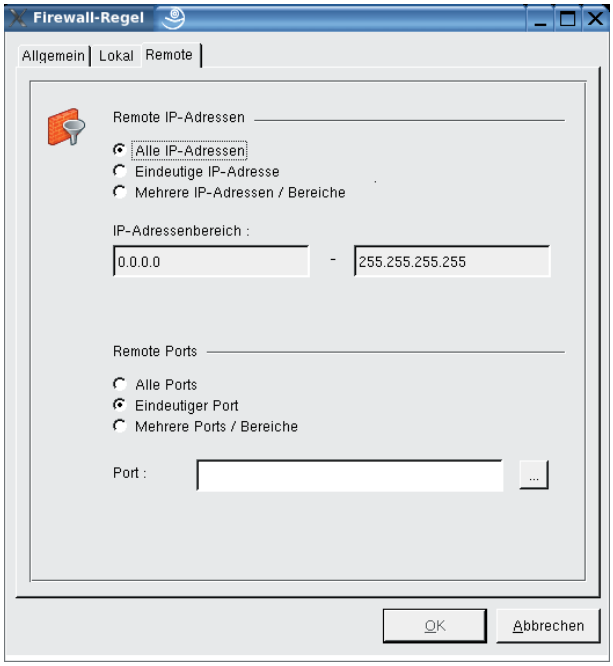
Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall nach außen durchgelassen, deren Quelladresse (Source Address) mit der unter "Lokale IP-Adressen" übereinstimmt oder im Gültigkeitsbereich liegt. Von den eingehenden Datenpaketen werden diejenigen durchgelassen, deren Zieladresse (Destination Address) mit der unter "Lokale IP-Adressen" übereinstimmt oder im Gültigkeitsbereich liegt.

Ebenso verhält es sich bei gesperrter Grundeinstellung mit den IP-Ports. Diejenigen Datenpakete werden nach außen gelassen, deren Quell-Port (Source Port) unter die Definition der lokalen Ports fällt. Von den eingehenden Datenpaketen werden die durchgelassen, deren Ziel-Port (Destination Port) unter die Definition der lokalen Ports fällt.

Alle IP-Adressen
– umfasst alle Quell-IP-Adressen abgehender bzw. Ziel-IP-Adressen eingehender Pakete, unabhängig vom lokalen Netzwerkadapter.
Eindeutige IP-Adresse
– ist die für den lokalen Netzwerkadapter definierte IP-Adresse. Sie kann je nach Verbindung z.B. der Adresse der Ethernet-Karte, der WLAN-Karte oder auch dem VPN-Adapter zugeordnet sein.
Mehrere IP-Adressen
– bezeichnet einen Adressbereich oder Pool. Z.B. kann dies der IP-Adress-Pool sein, aus dem die vom DHCP Server an den Client zugewiesene Adresse stammt.

Alle Ports
– erlaubt Kommunikation über alle Quellports bei ausgehenden und Ziel-Ports bei eingehenden Paketen.
Eindeutiger Port
– Diese Einstellung sollte nur dann verwendet werden, wenn dieses System einen Server-Dienst zur Verfügung stellt (z.B. Remote Desktop auf Port 3389).
Mehrere Ports
– Diese Einstellung sollte nur dann verwendet werden, wenn sich die lokalen Ports zu

Firewall-Regel / Remote



Auf dieser Registerkarte werden die Filter für die remote IP-Adressen und IP-Ports eingestellt.

Bei gesperrter Grundeinstellung werden diejenigen Datenpakete von der Firewall nach außen durchgelassen, deren Zieladresse (Destination Address) mit der unter “Lokale IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt. Von den eingehenden Datenpaketen werden diejenigen durchgelassen, deren Quelladresse (Source Address) mit der unter “Lokale IP-Adressen” übereinstimmt oder im Gültigkeitsbereich liegt.

Ebenso verhält es sich bei gesperrter Grundeinstellung mit den IP-Ports. Diejenigen Datenpakete werden von der Firewall nach außen gelassen, deren Ziel-Port (Destination Port) unter die Definition der lokalen Ports fällt. Von den eingehenden Datenpaketen werden die durchgelassen, deren Quell-Port (Source Port) unter die Definition der lokalen Ports fällt.

Mit den Einstellungen unter Remote-IP-Adressen lässt sich festlegen, mit welchen entfernten IP-Adressen das system kommunizieren darf.

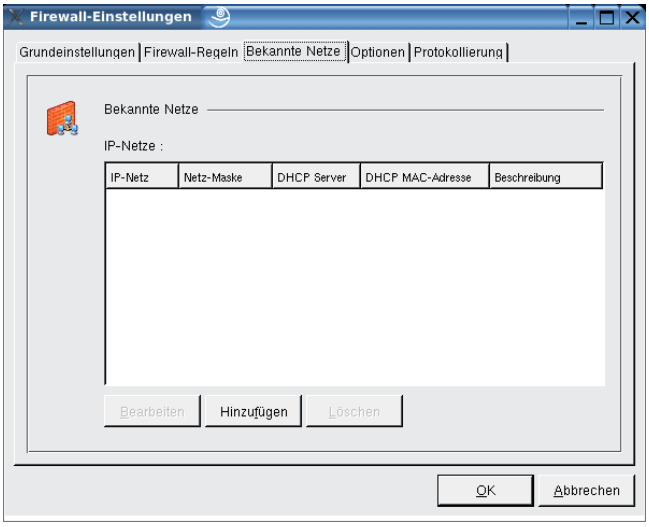
Alle IP-Adressen
– erlaubt die Kommunikation mit beliebigen IP-Adressen der Gegenseite, ohne Einschränkung.
Eindeutige IP-Adresse
– lässt nur Kommunikation mit der hier angegebenen IP-Adresse auf der Gegenseite zu.
Mehrere IP-Adressen /-Bereiche
– gestattet die Kommunikation mit verschiedenen IP-Adressen auf der Gegenseite entsprechend der Einträge.

Mit den Einstellungen unter Remote Ports lässt sich festlegen, über welche Ports mit entfernten Systemen kommuniziert werden darf.

Alle Ports
– setzt keinerlei Beschränkungen hinsichtlich Ziel-Port bei abgehenden bzw. Quell-Port bei eingehenden Paketen.

Eindeutiger Port
– lässt nur eine Kommunikation über den angegebenen Port zu, wenn dieser als Ziel-Port im abgehenden bzw. als Quell-Port im eingehenden Paket vorkommt. Soll z.B. eine Regel nur Telnet zu einem anderen System zulassen, ist hier Port 23 einzutragen.
Mehrere Ports / Bereiche
– können verwendet werden, wenn mehrere Ports für eine Regel verwendet werden sollen (z.B. FTP Port 20/21).

Konfigurationsfeld Bekannte Netze



Wurde im Konfigurationsfeld “Firewall-Regeln” definiert, dass eine Regel auf Verbindungen mit bekannten Netzen (Friendly Nets) anzuwenden ist, so wird diese Regel immer angewendet, wenn ein Netz nach den hier anzugebenden Kriterien als Friendly Net identifiziert werden kann, bzw. der LAN-Adapter sich in einem Friendly Net befindet.

Der LAN-Adapter des Clients befindet sich dann in einem Friendly Net wenn:

[IP-Netze und Netzmaske]

– die IP-Adresse des LAN-Adapters aus dem angegebenen Netzbereich stammt. Ist z.B. das IP-Netz 192.168.254.0 mit der Maske 255.255.255.0 angegeben, so würde die Adresse 192.168.254.10 auf dem LAN-Adapter eine Zuordnung zum bekannten Netz bewirken.

[DHCP Server]

– diese IP-Adresse von dem DHCP Server zugewiesen wurde, der die hier angegebene IP-Adresse besitzt;

[DHCP MAC-Adresse]

– wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt. Diese Option kann nur dann verwendet werden, wenn sich der DHCP Server im selben IP-Subnet befindet wie der DHCP Client.
Je mehr dieser Bedingungen erfüllt werden, desto präziser ist der Nachweis, dass es sich um ein vertrautes Netz handelt.
Die Zuordnung eines Adapters zu unbekannten oder bekannten Netzen wird automatisch protokolliert im Log-Fenster des Client-Monitors und in der Log-Datei der Firewall (siehe → Protokollierung).wenn dieser DHCP Server die hier angegebene MAC-Adresse besitzt.

Konfigurationsfeld Optionen

Bei gesperrter Grundeinstellung kann der Aufbau von VPN-Verbindungen über das Register “Optionen” global zugelassen werden.

Es werden die folgenden für den Tunnelaufbau benötigten Protokolle und Ports per automatisch generierter Filter freigegeben:

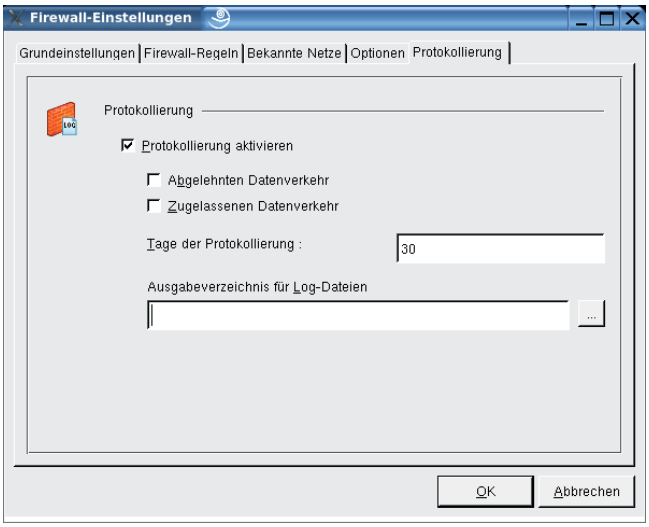
Für L2Sec: UDP 1701 (L2TP), UDP 67 (DHCPS), UDP 68 (DHCPC)

Für IPSec: UDP 500 (IKE ISAKMP), IP-Protokoll 50 (ESP), UDP 4500 (NAT-T), UDP 67 (DHCPS), UDP 68 (DHCPC)

Diese globale Definition erspart die Einrichtung dedizierter Einzelregeln für die jeweilige VPN-Variante.

Bitte beachten Sie, dass dadurch lediglich der Tunnelaufbau ermöglicht wird. Existieren keine weiteren Regeln für VPN-Netze, die eine Kommunikation im Tunnel zulassen, kann über die VPN-Verbindung kein Datenaustausch erfolgen.

Konfigurationsfeld Protokollierung



Die Aktivitäten der Firewall werden je nach Einstellung in eine Log-Datei geschrieben. Das “Ausgabeverzeichnis für Log-Dateien” befindet sich standardmäßig im Installationsverzeichnis unter:

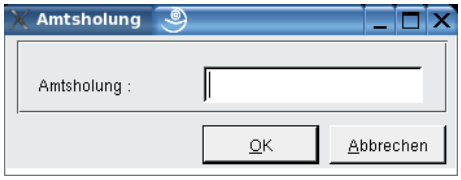
```
/var/log/ncp
```

Die Log-Dateien für die Firewall sind im reinen Textformat geschrieben und benannt als Firewallyymmdd.log. Sie beinhalten eine Beschreibung vom “abgelehnten Datenverkehr” und/oder “zugelassenen Datenverkehr”. Wurde keine dieser Optionen selektiert, so werden nur Statusinformationen zur Firewall hinterlegt.

Die Log-Dateien werden bei jedem Start der Firewall geschrieben. Maximal werden davon so viele im Log-Verzeichnis gehalten, wie als Anzahl der “Tage der Protokollierung” eingegeben wurde.

Diese Seite ist frei →

4.2.3 Amtsholung



Eine Amtsholung ist dann nötig, wenn der Secure Client an einer Nebenstellenanlage betrieben wird. Damit das Telefonbuch des Secure Clients auch im mobilen Einsatz verwendbar bleibt, ohne Rufnummern umkonfigurieren zu müssen, kann, sofern an einem Anschluss eine Amtsholung nötig wird, diese hier eingetragen werden. Die Nummer für die Amtsholung wird dann für alle Zielrufnummern des Telefonbuchs automatisch mitgewählt.

Bei der Eingabe der Amtsholung sind als Eingabezeichen nur die Zahlen 0-9 und die Zeichen ‘#’ und ‘*’ möglich. Alle anderen Zeichen werden ignoriert.

© NCP engineering GmbH

4.2.4 Zertifikate |Konfiguration

Unter diesem Menüpunkt wird konfiguriert welche Art von Zertifikaten eingesetzt werden – ob Soft-Zertifikate oder Zertifikate auf Chipkarten (Smart Cards) – und wo diese Zertifikate auf dem Rechnersystem zu finden sind. Deweiteren wird die Dauer der Gültigkeit eines Zertifikats festgelegt und können die Richtlinien für die PIN definiert werden.

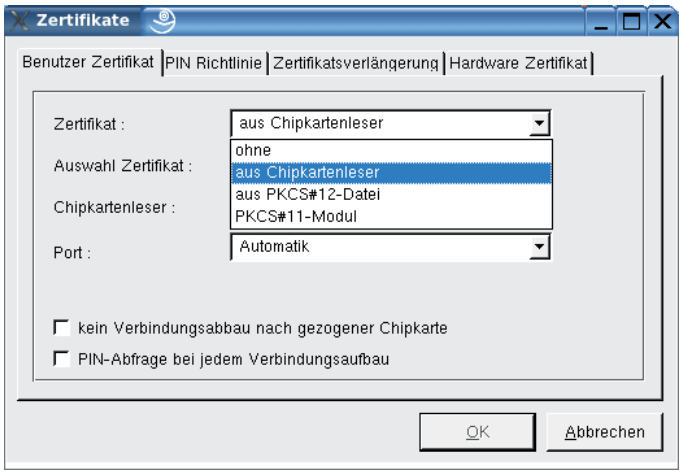
Zertifikate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt. Sie können als Soft-Zertifikat in Dateiform ausgeliefert werden oder auf eine Smart Card (Chipkarte) gebrannt werden. Diese Smart Card enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen. Es können Zertifikate eingesetzt werden, die einen privaten Schlüssel bis zu einer Länge von 2048 Bits haben. Als Gegenstelle muss der NCP Secure Server 5.21 oder höher eingesetzt werden.

Die Client Software überwacht, ob eine PKCS#12-Datei vorhanden ist. Wird eine PKCS#12-Datei (Soft-Zertifikat) eingesetzt, z.B. auf einem USB-Stick oder einer SD-Karte gespeichert, so wird nach dem Ziehen der SD-Karte die PIN zurückgesetzt und eine bestehende Verbindung abgebaut. Dieser Vorgang entspricht dem “Verbindungsabbau bei gezogener Chipkarte”, der bei Verwendung einer Chipkarte im Monitormenü unter “Konfiguration / Benutzer-Zertifikat” eingestellt werden kann. Wird später die SD-Karte wieder gesteckt, kann nach der erneuten PIN-Eingabe die Verbindung wieder hergestellt werden.

In der Zertifikats-Konfiguration können für die Pfad-Angaben die Umgebungsvariablen (Benutzer) des Betriebssystems eingesetzt werden. Die Variablen werden beim Schießen des Dialogs und beim Einlesen des Telefonbuches umgewandelt und in die Konfiguration zurück geschrieben. Existiert eine Umgebungsvariable nicht, wird sie aus dem Pfad beim Umwandeln entfernt und ein Log-Eintrag ins Logbuch geschrieben. Fehlt ein %-Zeichen (Syntax), bleibt die Variable stehen und es wird ebenfalls ein Log-Eintrag geschrieben.

VPN- und Hardware-Zertifikate können über das CMP-Protokoll (Certificate Management) verteilt werden. Das erstmalige Herunterladen ist dabei nur bei der Ersteinwahl mit einem Init-Benutzer möglich. In der Zertifikatskonfiguration des Init-Benutzers muss vor dem Herunterladen ein Dateiname für die PKCS#12-Datei angegeben sein auch wenn diese Datei noch nicht vorhanden ist. Ist keine Zertifikatskonfiguration definiert, wird auch kein Zertifikat heruntergeladen. Diese Zertifikatsverteilung ist nur mit dem Secure Enterprise Management möglich. Zwischen Update Client und Management Server wird zusätzlich der Port 829 (TCP) benötigt. Die PIN für das VPN-Zertifikat wird vor dem Speichern der PKCS#12-Datei abgefragt. Beim Hardware-Zertifikat wird diese durch die Hardware automatisch ermittelt.

Benutzer-Zertifikat



Zertifikat

Klicken Sie auf das Untermenü “Zertifikate”, so können Sie zunächst bestimmen, ob Sie die Zertifikate und damit die “Erweiterte Authentisierung” nutzen wollen – oder nicht.

ohne : Wählen Sie in der Listbox “Zertifikat” die Einstellung “ohne”, so wird kein Zertifikat ausgewertet und die “Erweiterte Authentisierung” findet nicht statt.

aus Chipkartenleser : Wählen sie “aus Chipkartenleser” in der Listbox, so werden bei der “Erweiterten Authentisierung” die Zertifikate von der Smart Card in ihrem Chipkartenleser ausgelesen.

aus PKCS#12-Datei : Wählen Sie “aus PKCS#12 Datei” aus der Listbox, so werden bei der “Erweiterten Authentisierung” die Zertifikate aus einer Datei auf der Festplatte Ihres Rechners gelesen.

aus PKCS#11-Modul : Wählen Sie “aus PKCS#11-Modul” aus der Listbox, so werden bei der “Erweiterten Authentisierung” die Zertifikate aus einer Datei auf der Festplatte Ihres Rechners gelesen.

Chipkartenleser

Wenn Sie die Zertifikate von der Smart Card mit Ihrem Lesegerät nutzen wollen, wählen Sie Ihren Chipkartenleser aus der Listbox. (Siehe auch → PIN eingeben)

Chipkartenleser (PC/SC-konform)
Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden.

Chipkartenleser (CT-API-konform)
Mit der aktuellen Software werden Treiber für die Modelle Kobil B0/B1 und Kobil KAAN mitgeliefert. Diese Chipkartenleser können im Monitor unter "Verbindung → Zertifikate → Konfiguration" eingestellt werden. Sollte der Chipkartenleser mit den mitgelieferten Treibern nicht funktionieren oder ein anderer Chipkartenleser installiert sein, wenden Sie sich unbedingt an den Hersteller des Chipkartenlesers, bzw. konsultieren Sie die entsprechende Website bezüglich aktueller Hardware-Treiber, um den aktuellsten CT-API-Treiber zu erhalten und zu installieren. Nehmen Sie außerdem folgende Einstellung in der Client Software vor:

Editieren Sie die Datei NCPPKI.CONF, befindlich im Verzeichnis /etc/ncp mit einem ASCII-Editor, indem Sie als "ReaderName" den Namen des angeschlossenen Chipkartenlesers eintragen und als DL_LINUX den Namen des installierten Treibers eintragen. Nur die Treiber sind in der Liste sichtbar, die mit "visible = 1" auf sichtbar gesetzt wurden!

```
ReaderName   = Kobil B0/B1 (CT-API)
DL_LINUX     = libct_b1.so
ReaderName   = Kobil Kaan (CT-API)
DL_LINUX     = libct_kaan.so
```

Nach einem Boot-Vorgang erscheint der von Ihnen eingetragene "ReaderName" im Monitor-Menü. Selektieren Sie nun diesen Chipkartenleser.

Port

Haben Sie oben “aus Chipkartenleser” gewählt, so muss hier der Port für den Chipkartenleser eingegeben werden.

Automatik :	Der Port wird bei korrekter Installation des Lesegeräts automatisch bestimmt.
COM1 ... COM4 :	Bei Unstimmigkeiten können die COM Ports 1-4 gezielt angesteuert werden.

Auswahl Zertifikat

1. Zertifikat ...4.	(Standard = 1) Aus der Listbox kann aus bis zu drei verschiedenen Zertifikaten gewählt werden, die sich auf der Chipkarte befinden. Die Anzahl der Zertifikate auf der Chipkarte ist abhängig von der Registration Authority, die diese Karte brennt. Wenden Sie sich zu weiteren Fragen bitte an Ihren Systemadministrator.

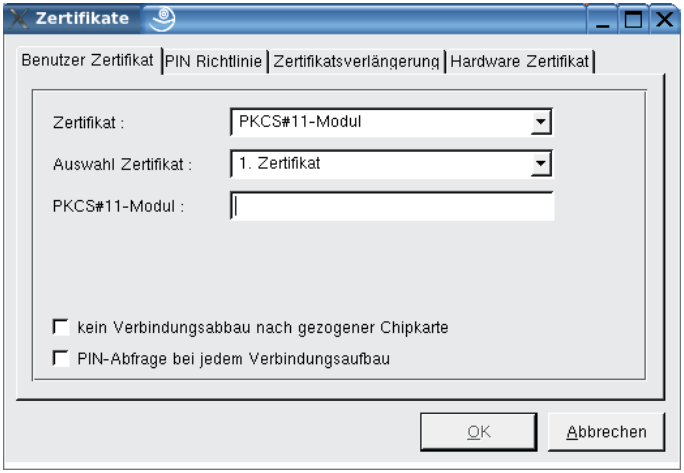
Auf den Chipkarten von Signtrust und NetKey 2000 befinden sich drei Zertifikate:
(1) zum Siginieren
(2) zum Ver- und Entschlüsseln
(3) zum Authentisieren (optional bei NetKey 2000)

PKCS#12-Dateiname

Nutzen Sie das PKCS#12-Format, so erhalten Sie von Ihrem Systemadministrator eine Datei, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname der PKCS#12 Datei eingegeben, bzw. nach einem Klick auf den [...]-Button (Auswahl-Button) die Datei ausgewählt werden.

Statt den Verzeichnisnamen für die PKCS#12-Datei komplett einzugeben, kann der Name dynamisch zusammengesetzt werden.

PKCS#11-Modul



Mit der Software für die Smart Card oder den Token werden Treiber in Form einer PKCS#11-Bibliothek (.so) mitgeliefert. Diese Treiber-Software muss zunächst installiert werden. Anschließend muss die Datei NCPPKI.CONF editiert werden.

Statt den Verzeichnisnamen für die PKCS#11.DLL komplett einzugeben, kann der Name dynamisch zusammengesetzt werden.

Wichtig: Die Strings für das Modul können mit Variablen eingegeben werden. Dies erleichtert insbesondere das Handling der Konfigurationsdateien mit dem Client Manager, da nun für alle Benutzer die gleichen Strings mit Umgebungsvariablen eingegeben werden können.

Editieren Sie die Datei NCPPKI.CONF, befindlich im Verzeichnis /etc/ncp mit einem ASCII-Editor, indem Sie als “ReaderName” den Namen des angeschlossenen Lesers oder Tokens eintragen. Als PKCS#11-DLL muss der Name des installierten Treibers (xxx.so) eintragen werden. Der zugehörige “Slotindex” ist herstellerabhängig (Standard = 0).

Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1" auf sichtbar gesetzt wurden!

```
ReaderName   = xxxname
PKCS11-DLL   = xxx.so
Slotindex    =
```

Nach einem Restart der Client-Dämonen (rcncpclntd restart) erscheint der von Ihnen eingetragene “Modulname” im Monitor-Menü. Selektieren Sie nun diesen Chipkartenleser oder Token.

Sie können auch mit Hilfe eines Assistenten nach installierten PKCS#11-Modulen suchen und das gewünschte Modul mit dem dazugehörigen Slot selektieren. Dazu klicken Sie auf den Button in der Zeile mit “PKCS’11-Modul (siehe Bild oben).

Verbindungsabbau bei gezogener Chipkarte

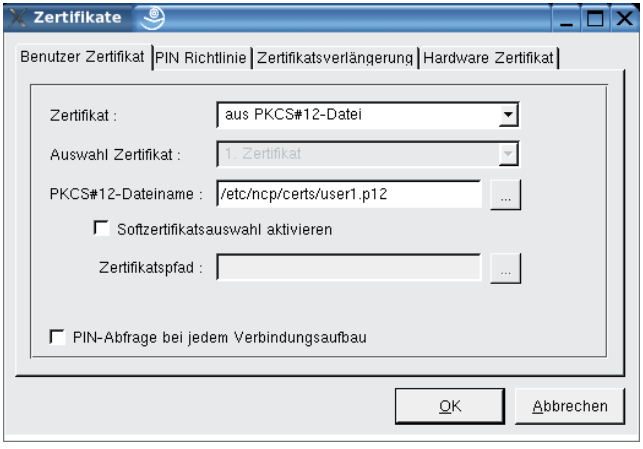
Beim Ziehen der Chipkarte wird nicht unbedingt die Verbindung abgebaut. Ob “Kein Verbindungsabbau bei gezogener Chipkarte” erfolgt, wird an dieser Stelle eingestellt.

PIN-Abfrage bei jedem Verbindungsaufbau

Hier kann eingestellt werden, dass die PIN nicht nur nach jedem ersten Verbindungsaufbau nach dem Booten des PCs sondern vor jedem Verbindungsaufbau korrekt eingegeben werden muss. Diese Funktionalität, die für alle Verbindungsmodi (manuell, automatisch, wechselnd) genutzt werden kann, erfordert, dass der Monitor gestartet ist. Der Monitor darf allerdings minimiert sein.

Wichtig: Ist der Monitor nicht gestartet, kann kein PIN-Dialog erfolgen. In diesem Fall wird bei einem automatischen Verbindungsaufbau die Verbindung ohne erneute PIN-Eingabe hergestellt!

Softzertifikatsauswahl aktivieren



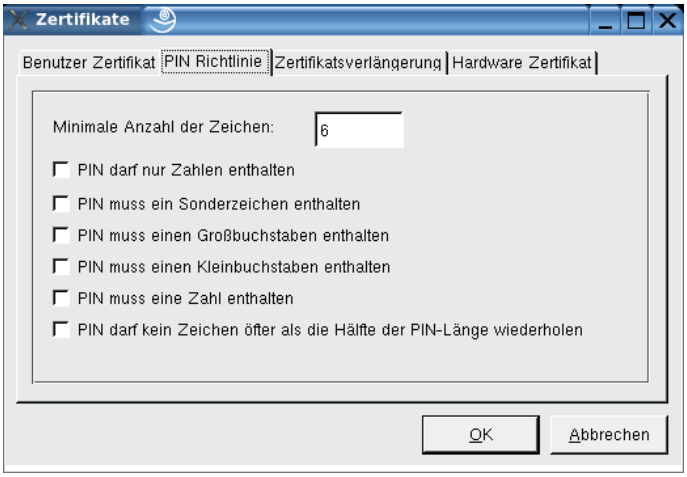
Diese Funktion wird nur für PC-Sharing benötigt, wenn die Benutzer des PCs mit Soft-Zertifikaten arbeiten. Beachten Sie dazu unbedingt die Beschreibung “Nutzung mehrerer Soft-Zertifikate an einem Client-PC” im Kapitel “Beispiele und Erklärungen” in diesem Handbuch.

Bei Einsatz von Soft-Zertifikaten kann der Zertifikatspfad für die PKCS#12-Dateien festgelegt werden, nachdem die “Soft-Zertifikatsauswahl” aktiviert wurde. Unter dem Parameterfeld des Monitors erscheint dann ein Auswahlfeld mit allen Zertifikaten unter dem angegeben Verzeichnis. Wird ein Soft-Zzertifikat ausgewählt, wird die zu diesem Zertifikat gehörige Konfiguration aktiv und entsprechend die Verbindung abgebaut und die PIN zurückgesetzt. Alternativ kann bei einem Benutzerwechsel die PIN über den Button “Abmelden” oder über das Menü “PIN zurücksetzen” zurückgesetz werden.

Zertifikatspfad

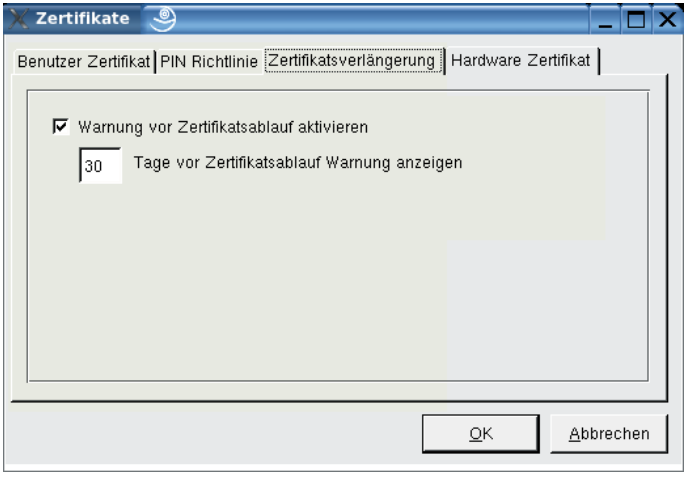
Der Zertifikatspfad wird nur bei PC-Sharing benötigt.

PIN-Richtlinie



Der Administrator (oder Benutzer) kann jetzt PIN-Richtlinien festlegen, die bei der PIN-Eingabe oder -Änderung beachtet werden müssen. Die hier ausgewählten Richtlinien erscheinen als Liste von Bedingungen, die bei der Änderung der PIN eingehalten werden müssen.

Zertifikatsverlängerung



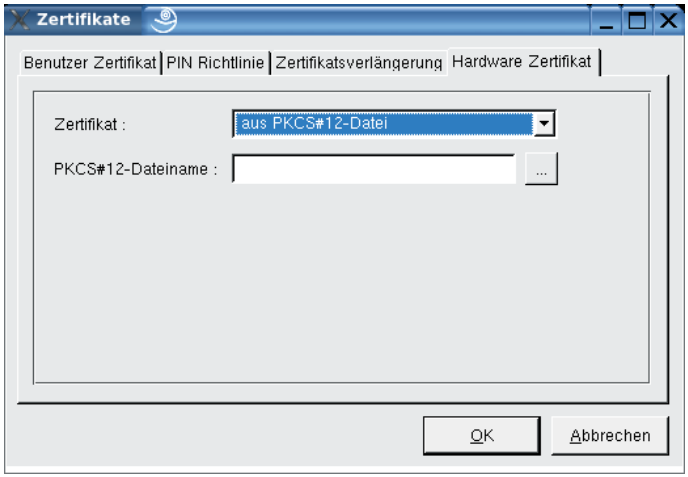
Hier wird eingestellt, ob und wie viele Tage vor Ablauf der Gültigkeit des Zertifikats eine Meldung ausgegeben werden soll, die vor dem Ablauf der Gültigkeit warnt. Sobald die eingestellte Zeitspanne vor Ablauf in Kraft tritt, wird bei jeder Zertifikatsverwendung eine Meldung aufgeblendet, die auf das Ablaufdatum des Zertifikats hinweist.

Gültigkeitsverlängerung von PKCS#12-Dateien über Update Server

Im Client wird zunächst die PKCS#7-Datei im RSUDATA-Verzeichnis gespeichert. Nach dem Verbindungsabbau wird überprüft, ob für diesen Benutzer eine PKCS#7 Datei vorhanden ist. Ist dies der Fall, wird das alte Zertifikat unter einem neuen Dateinamen gespeichert und anschließend das neue Zertifikat mit neuem Private-Key in der konfigurierten PKCS#12-Datei mit der eingebenen PIN gespeichert. Der Benutzer erhält danach einen Hinweis, das sein Zertifikat erneuert wurde. Voraussetzung ist der Einsatz des PKI-Managers ab Version 1.01 und des Update-Servers ab Version 2.03 Build 8.

Hardware-Zertifikat

Die zusätzliche Authentisierung mit einem Hardware-Zertifikat kann nur mit IPSec genutzt werden. Zur Aktivierung der Funktion muss am Gateway ab Version 6.02 Build 14 die Option “Hardware-Zertifikat CN” unter Link-Profile eingeschaltet werden.

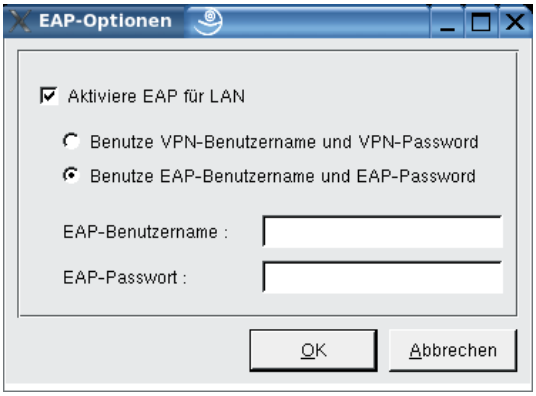


Mit einem Hardware-Zertifikat authentisiert sich der Rechner gegenüber dem Gateway. Wird es zusätzlich zu einem Benutzer-Zertifikat eingesetzt, so kann sichergestelltwerden, dass sich der Benutzer immer vom gleichen Rechner aus einwählt.

Ein Hardware-Zertifikat kann als PKCS#12-Datei oder als Entrust-Profil eingespielt werden. Der entsprechende Dateiname ist anzugeben. Die Eingabe einer PIN entfällt bei dem Hardware-Zertifikat. Sie erfolgt automatisch im Hintergrund, ohne dass der Anwender eine Eingabe machen muss. Als PIN für das Zertifikat wird die Seriennummer des Rechners oder der Festplatte verwendet.

Beim Erzeugen eines Hardware-Zertifikats als PKCS#12-Datei muss die PIN manuell vergeben werden. Mit dem Programm HWINFO.EXE kann die Seriennummer des Rechners, welche als PIN verwendet wird, ausgelesen werden. Die PIN ist mindestens 8 und maximal 20 Zeichen lang.

4.2.5 EAP-Optionen



Hier kann der Einsatz des Extensible Authentication Protocols Message Digest5 (EAP MP5) eingestellt werden. Dieses Protokoll kann dann zum Einsatz kommen, wenn für den Zugang zum LAN ein Switch oder für das wireless LAN ein Access Point verwendet werden, die 802.1x-fähig sind und eine entsprechende Authentisierung unterstützen.

Mit dem Extensible Authentication Protocol (EAP MP5) kann verhindert werden, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Zur Authentisierung kann wahlweise “VPN-Benutzername” mit “VPN-Passwort” verwendet werden oder ein eigener “EAP-Benutzername” mit einem “EAP-Passwort”.

Nach Konfiguration des EAP erscheint eine Statusanzeige im grafischen Feld des Monitors. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt die EAP-Verhandlung erneut.

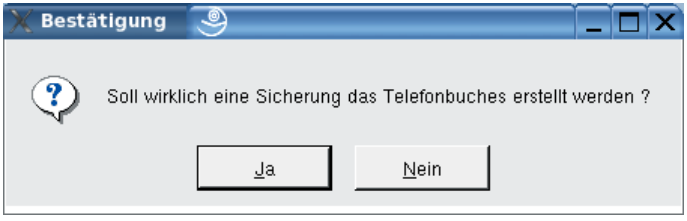
4.2.6 Letzte Konfiguration laden

Dieser Menüpunkt erscheint nur, wenn vom Update Server eine Datei (Telefonbuch) übertragen wurde und eine VPN-Verbindung besteht.

Sollte nach einem Update eine der vorher möglichen Verbindungen zum Update Server (Management Server) nicht mehr möglich sein, etwa aufgrund eines Konfigurationsfehlers, so besteht die Möglichkeit, über diesen Menüpunkt auf die letzte funktionierende Konfiguration zurück zu greifen.

4.2.7 Telefonbuch-Sicherung

Unter diesem Menüpunkt kann das “Erstellen” und das “Wiederherstellen” eines Telefonbuchs veranlasst werden. Existiert noch kein gesichertes Telefonbuch, zum Beispiel bei einer Erstinstallation, so wird automatisch ein erstes angelegt (NCPPHONE.SAV).

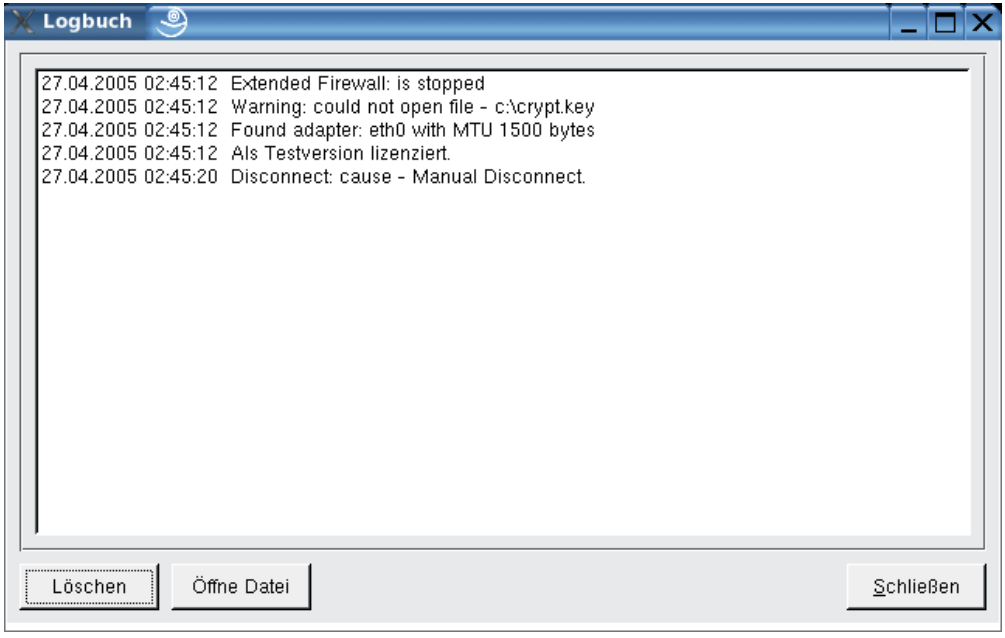


Nach jedem Klick auf den Menüpunkt “Erstellen” wird nach einer Sicherheitsabfrage (links) ein Telefonbuch-Backup angelegt, das die Konfiguration zu diesem Zeitpunkt enthält.

Nach jedem Klick auf “Wiederherstellen” wird das letzte Telefonbuch-Backup eingelesen. Änderungen in der Konfiguration, die seit dem letzten Telefonbuch-Backup vorgenommen wurden gehen damit verloren.

4.3 Log

Logbuch

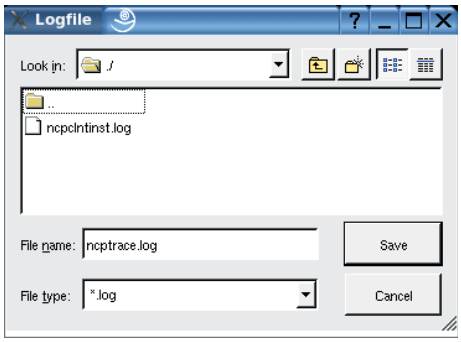


Mit der Log-Funktion werden die Kommunikationsereignisse der Secure Client Software mitprotokolliert. Wählen Sie die Log-Funktion an, öffnet sich das Fenster der "Protokollierung". Die hier abgebildeten Daten werden bis zum nächsten Reboot im Speicher gehalten.

Löschen – Fensterinhalt

Wenn Sie auf diesen Button drücken wird der Inhalt des Log-Fensters gelöscht.

Öffne Datei

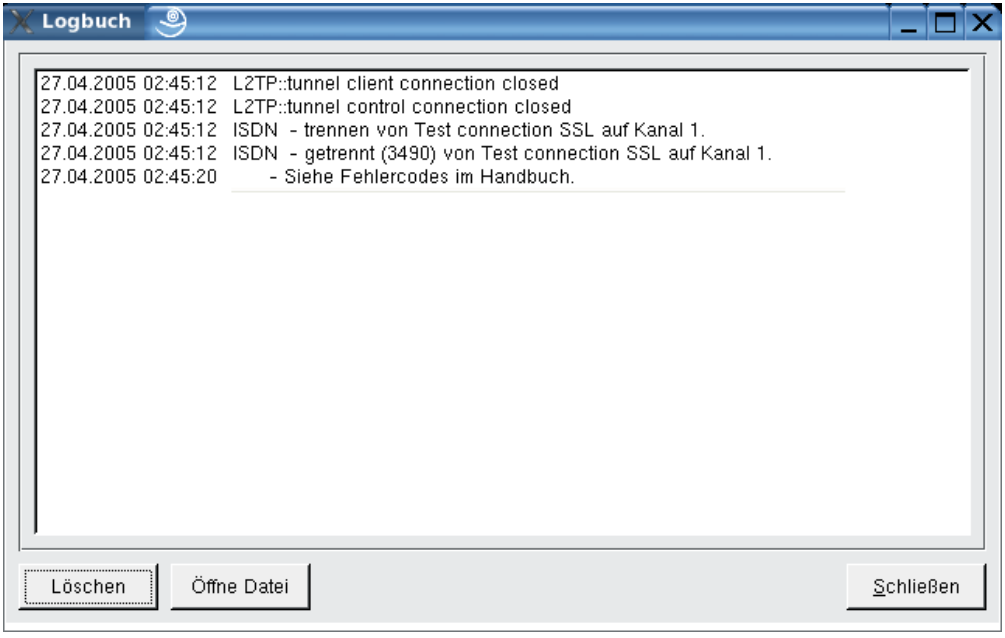


Wenn Sie auf diesen Button klicken, erhalten Sie in einem weiteren Fenster die Möglichkeit Name und Pfad einer Datei einzugeben, in die der Inhalt des Log-Fensters geschrieben wird (Standard: ncptrace.log). Alle Transaktionen wie Anwahl und Empfang, einschließlich der Rufnummern, werden automatisch mitprotokolliert und in diese Datei geschrieben, bis Sie auf den Button mit "Schließe Datei" klicken. Wenn Sie eine Datei anlegen, können Sie die Transaktionen über einen längeren Zeitraum verfolgen.

Schließen – Log-Fenster

Wenn Sie auf “Schließen” klicken, schließen Sie das Fenster der “Protokollierung” und kehren zum Monitor zurück.

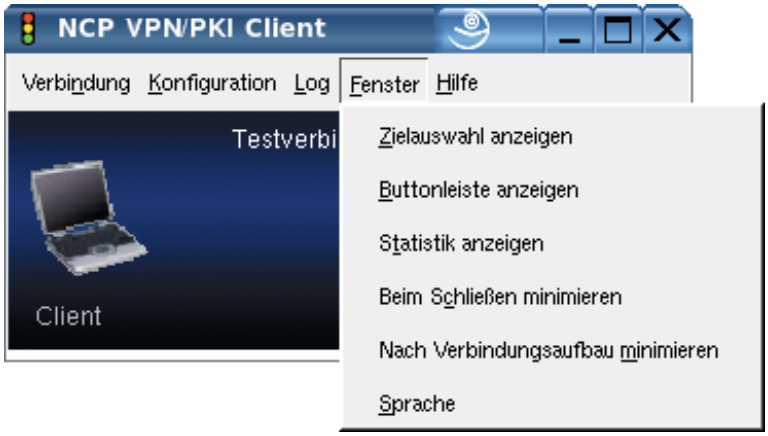
Schließe Datei



Wenn Sie auf “Schließe Datei” klicken, wird die Datei geschlossen, die Sie mit “Öffne Datei” angelegt haben. Die geschlossene Log-Datei kann zur Analyse der Transaktionen mit dem Secure Client oder zur Fehlersuche verwendet werden.

Eine zusätzliche Log-Datei speichert die Aktionen des Clients selbständig für die letzten sieben Tage. Log-Ausgaben, die älter als sieben Betriebstage sind, werden automatisch gelöscht. Die Datei steht unter NCPLE\LOG und heißt NCPyymmdd.LOG. Sie wird mit Datumsangabe (yymmdd) immer bei Beenden des Monitors geschrieben. Die Datei kann mit einem Texteditor geöffnet und analysiert werden.

4.4 Fenster



Unter dem Menüpunkt "Fenster" können Sie die Bedienoberfläche des Monitors variieren und die Sprache für die Monitoroberfläche festlegen.

4.4.1 Zielauswahl anzeigen

Links: die minimierte Darstellung.

Wenn "Zielauswahl anzeigen" angeklickt wird, wird die Zeile mit dem Namen des Zielsystems und dem Eingabefeld für die Amtsholung angezeigt Siehe Bild unten.

4.4.2 Button-Leiste anzeigen

Wenn Sie auf “Button-Leiste anzeigen” klicken (Bild links), werden Buttons für die Menüpunkte “Verbinden” und “Trennen” aus dem Hauptmenü “Verbindung” eingeblendet und das Firmenlogo wird sichtbar.

4.4.3 Statistik anzeigen

Wenn Sie auf “Statistik anzeigen” klicken, werden Informationen zu Datenmenge, Verbindungszeit, Timeout etc. angezeigt. Die Monitor-Oberfläche ist dann entsprechend größer.

4.4.4 Beim Schließen minimieren und Beenden des Monitors

Wird der Monitor bei einer bestehenden Verbindung über den Schließen-Button [x] rechts in der Kopfzeile oder das Systemmenü links in der Kopfzeile geschlossen [Alt + F4], so informiert ein Meldungsfenster darüber, dass kein Ampelsymbol (Tray Icon) mehr in der Task-Leiste erscheint, worüber der Status dieser Verbindung kontrolliert werden könnte, d.h. der Benutzer kann dann auf der Oberfläche seines Desktops nicht erkennen, ob und wie lange noch Verbindungsgebühren anfallen, oder ob die Verbindung bereits beendet wurde. (Um in diesem Fall den Status der Verbindung zu erfahren und sie gegebenenfalls korrekt zu beenden, muss der Monitor erneut gestartet werden.)

Im Hauptmenü wurde der Menüpunkt “Beim Schließen minimieren” hinzugefügt. Ist dieser Menüpunkt aktiviert, so wird der Monitor beim Schließen über den Button [x] rechts in der Kopfzeile oder über [Alt + F4] nur minimiert und erscheint als Ampelsymbol in der Task-Leiste, worüber der Status der Verbindung abgelesen werden kann. Der Klick auf den Schließen-Button [x] der Kopfzeile hat in dieser Einstellung die gleiche Wirkung wie der Klick auf den Minimieren-Button [-] der Kopfzeile.

(In der Darstellung des Ampelsymbols in der Task-Leiste kann nach einem rechten Mausklick auf das Symbol das mögliche Zielsystem abgelesen und die Verbindung aufgebaut oder getrennt werden, bzw. bei abgebauter Verbindung der Monitor auch beendet werden.)

Das Beenden des Monitors ist nur noch über das Hauptmenü “Verbindung – Beenden” möglich.

4.4.5 Nach Verbindungsaufbau minimieren

Wird diese Funktion aktiviert, so erscheint nach einem Verbindungsaufbau der Client-Monitor nur noch als Ampelsymbol in der Taskleiste.

4.4.6 Sprache

Die Secure Client Software ist mehrsprachig angelegt. Die Standardsprache bei Auslieferung ist Deutsch. Um eine andere Sprache zu wählen, klicken Sie “Language / Sprache” im Pulldown-Menü Fenster und wählen die gewünschte Sprache.

4.5 Hilfe

Die “Hilfe” zeigt Ihnen den kompletten Hilfetext mit Inhaltsverzeichnis und Index.

Unter dem Menüpunkt Hilfe finden Sie mit Klick auf “Info” die Versionsnummer Ihrer eingesetzten Software und Treiber.

5. Konfigurationsparameter

Nachdem Sie die Client Software mit dem Monitor installiert haben, wird ein Konfigurations-Assistent gestartet. Mit seiner Unterstützung können Sie Testverbindungen herstellen lassen, um die PKI-, VPN- oder IPSec-Funktionalität zu überprüfen. Außerdem können mit dem Konfigurations-Assistenten neue Zielsysteme angelegt werden. Die Zielsysteme werden mit Unterstützung des Konfigurations-Assistenten so weit wie möglich vorkonfiguriert. Um Modifikationen oder Erweiterungen vornehmen zu können, ist es aber unumgänglich, dass einzelne Parameter, die nicht vom Konfigurations-Assistenten abgefragt werden, über das Telefonbuch- oder IPSec-Menü gesetzt werden.

Zur Bedienung des Telefonbuch- und des IPSec-Menüs beachten Sie bitte die Beschreibung in diesem Handbuch unter “Monitor-Menü, Konfiguration, Telefonbuch / ISPec”.

Im folgenden sind alle Parameterbeschreibungen aufgeführt, und sie sind so angeordnet, wie sie auf der Oberfläche des Client Monitors erscheinen. Beschreibungen der funktionalen Zusammenhänge in PKI-, VPN- oder IPSec-Architekturen finden Sie in den Beispiel-Texten des Handbuchs (siehe → Beispiele und Erklärungen).

Ordnungsprinzip der Parameter

Die Parameter sind in verschiedenen Parameterfeldern gesammelt. In der Kopfzeile steht der Name des Zielsystems (im Telefonbuch-Menü) oder der Name der Richtlinie (im IPSec-Menü). Sie erreichen die Konfigurationsparameter über die Untermenüs

Konfiguration / Telefonbuch (5.1)

Konfiguration / IPSec (5.2)

Die Beschreibung der einzelnen Parameter folgt der Reihenfolge ihres Erscheinens in den einzelnen Parameterfeldern wie sie von oben nach unten angeordnet sind.

Zum schnellen Auffinden eines Parameters kann die Überschrift eines Parameterfelds oder der Index herangezogen werden.

Um Verwechslungen bei gleichlautenden Parametern vorzubeugen, wurden die Namen der übergeordneten Parameterfelder dahinter gesetzt. Diese Begriffe haben nur die Funktion, die Orientierung zu erleichtern!

© NCP engineering

5.1 Telefonbuch

Parameterfelder:

1 *Zielsystem*

2 *Netzeinwahl*

3 *Modem (nur bei Verbindungsart “Modem”)*

4 *Verbindungssteuerung*

5 *Rückruf*

6 *Eingehende Rufe*

7 *Security*

8 *Link-Einstellungen*

9 *Tunnel-Parameter*

10 *VPN IP-Netze*

11 *IPSec-Optionen*

12 *HA-Unterstützung*

13 *DNS/WINS*

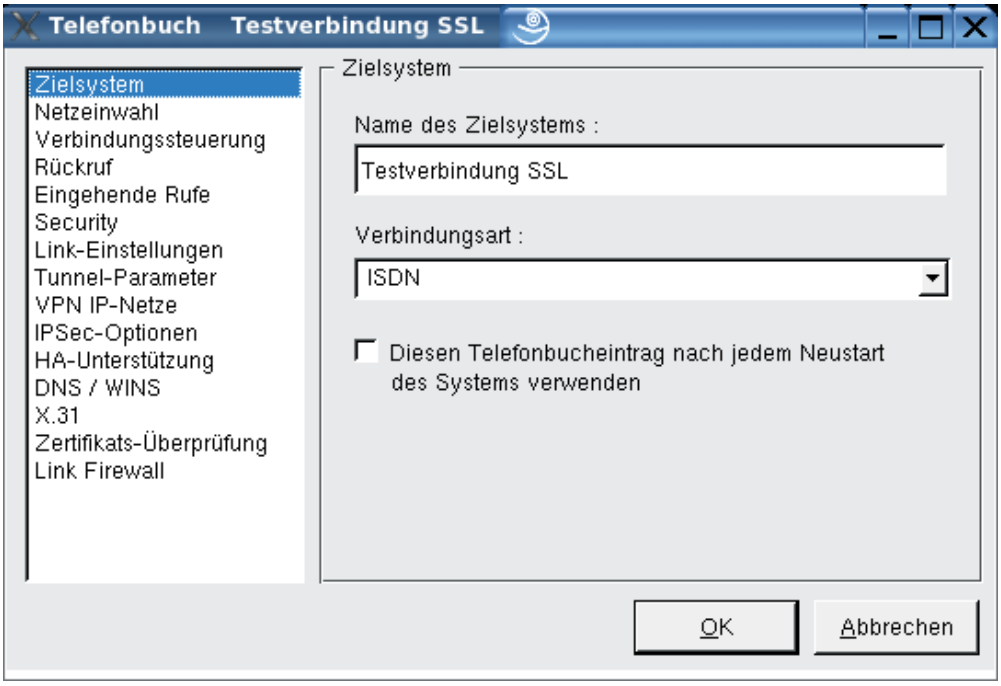
14 *X.31*

15 *Zertifikats-Überprüfung*

16 *Link Firewall*

Parameter und Parameterfelder werden nach der jeweils gewählten Verbindungsart automatisch ein- oder ausgeblendet (z.B. Modem). Einzelne Parameterfelder oder Parameter, die Sie für Ihre Arbeit mit dem Client nicht benötigen, können von Ihrem Systemadministrator ausgeblendet worden sein.

5.1.1 Zielsystem



Die Client Software gestattet die Einrichtung individueller Ziele bzw. Zielsysteme, die den Benutzeranforderungen entsprechend konfiguriert werden können. Um ein neues Zielsystem zu definieren, klicken Sie in der Menüleiste des Monitors auf "Telefonbuch" (oder auf das Telefonbuch-Icon in der Werkzeugleiste). Das Fenster des Telefonbuchs öffnet sich nun und zeigt die bereits definierten Zielsysteme. Klicken Sie jetzt auf "Neuer Eintrag". Jetzt legt der "Assistent für ein neues Ziel" mit Ihrer Hilfe ein neues Zielsystem an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Zielsystem angelegt. Für alle weiteren Parameterfelder des Telefonbuchs werden Standardwerte eingetragen.

Um diese Standardwerte zu editieren, wählen Sie mit der Maus das Zielsystem aus, dessen Werte Sie ändern möchten und klicken anschließend auf "Konfigurieren". (siehe → Telefonbuch – Konfigurieren). Einträge für Testzwecke können gelöscht oder entsprechend abgeändert werden.

Parameter:

- ☐ Name Zielsystem
- ☐ Verbindungsart
- ☐ Diesen Telefonbucheintrag nach jedem Neustart des System verwenden

■ Name des Zielsystems

Wenn Sie ein neues Zielsystem definieren, sollten Sie zunächst einen unverwechselbaren Namen für dieses System eintragen (z.B. IBM London). Der Name des Ziels darf jeden gewünschten Buchstaben wie auch Ziffern beinhalten und darf, Leerzeichen mitgezählt, bis zu 39 Zeichen lang sein.

■ Verbindungsart

Die Verbindungsart kann für jedes Zielsystem eigens eingestellt werden, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem (Windows-) System installiert.

Bitte beachten Sie, dass sich je nach gewählter Verbindungsart die Liste der Parameterfelder ändert!

Folgende Verbindungsarten können eingestellt werden:

ISDN

Hardware: ISDN-Hardware (Karte, ISDN-Box oder PCMCIA-Karte)
mit Capi 2.0-Unterstützung;
Netze: ISDN-Festnetz;
Gegenstellen: ISDN-Hardware;

Modem

Hardware: Asynchrone Modems (Tischmodem, PCMCIA-Modem,
GSM-Karte) mit Com Port-Unterstützung;
Netze: Analoges Fernsprechnetz (PSTN) (auch GSM und GPRS);
Gegenstellen: Modem oder ISDN-Karte mit digitalem Modem;

LAN (over IP)

Hardware: LAN-Adapter;
Netze: Local Area Network mit Ethernet oder Token Ring;
Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im LAN;

PPP over Ethernet

Hardware: Ethernet-Adapter, xDSL-Modem, Splitter;
Netze: xDSL;
Gegenstellen: Access-Router im xDSL;

xDSL (AVM - PPP over CAPI)

Diese Verbindungsart kann gewählt werden, wenn eine AVM Fritz! DSL-Karte eingesetzt wird. Im Feld “Rufnummer (Ziel)” in der Gruppe “Netzeinwahl” können für die

Verbindung über CAPI noch AVM-spezifische Intitialisierungskommandos eingetragen werden. Unter Windows Betriebssystemen wird jedoch empfohlen den Standard “xDSL (PPPoE)” zu verwenden, da damit direkt über die Netzwerkschnittstelle mit der Karte kommuniziert wird. Bei Verwendung der AVM Fritz! DSL-Karte wird keine separate zusätzliche Netzwerkkarte benötigt.
Netze: xDSL;
Gegenstellen: Access-Router im xDSL;xDSL (AVM - PPP over CAPI):

Bitte beachten Sie, dass je nach gewählter Verbindungsart die dafür erforderliche Hardware und ggf. die Treiber dazu installiert sein müssen.

GPRS / UMTS

Dieses Einwahlmedium wählen Sie, wenn die Einwahl über das Mobilfunknetz (GPRS oder UMTS) erfolgen soll. Beachten Sie dazu den Hinweis unter den Installationsvoraussetzungen zu “Analoges Modem”.

PPTP

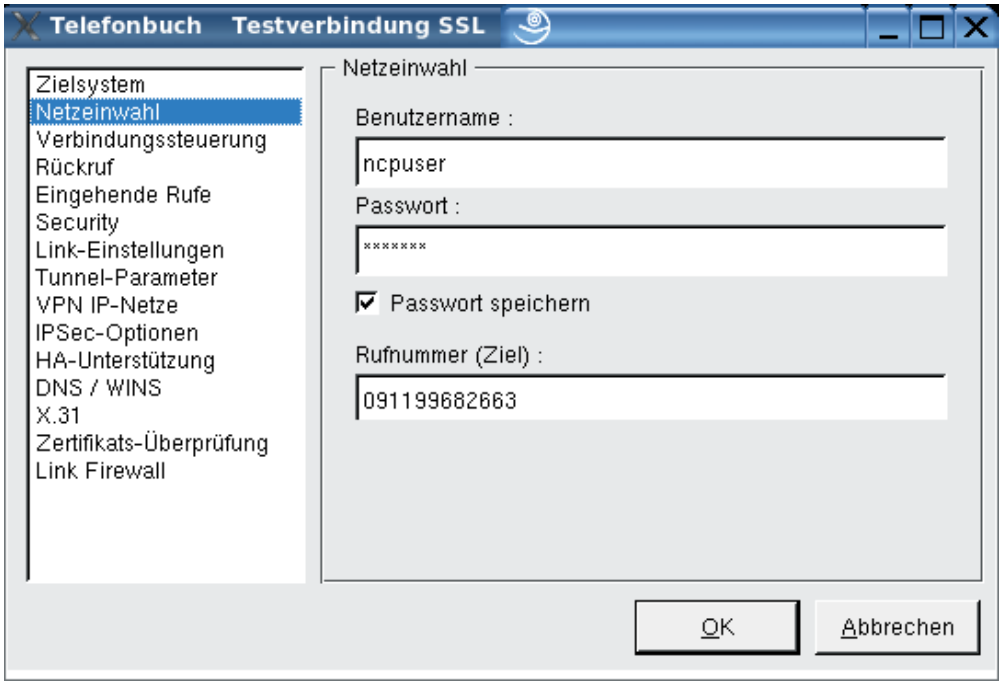
Microsoft Point-to-Point Tunnel Protocol;
Angeschlossene Hardware: Ethernet-Adapter, xDSL-Modem;
Netze: xDSL;
Gegenstellen: Access-Router im xDSL;

Wird dieses Protokoll gewählt, so muss im Parameterfeld “Netzeinwahl” unter “PPTPEndpunkt” die IP-Adresse des Access-Routers im xDSL eingetragen werden.

■ Diesen Telefonbucheintrag nach jedem Neustart des Systems verwenden

Normalerweise wird der Client-Monitor nach einem Neustart mit dem zuletzt genutzten Profil geöffnet. Wird diese Funktion aktiviert, wird nach einem Neustart des Systems immer das hierzu gehörige Profil geladen, unabhängig davon, welches Profil zuletzt genutzt wurde.

5.1.2 Netzeinwahl



Über dieses Parameterfeld werden die Angaben zur Netzeinwahl ausgewertet. In der Verbindungsart "PPP over Ethernet" entfällt in diesem Parameterfeld die "Rufnummer Ziel".

Das Parameterfeld erscheint überhaupt nicht, wenn der Secure Client in der Verbindungsart "LAN over IP" betrieben wird.

Parameter:

☐ Benutzername

☐ Passwort

☐ Passwort speichern

☐ Rufnummer (Ziel)

☐ Alternative Rufnummern

Benutzername

Mit dem Benutzernamen weisen Sie sich gegenüber dem Network Access Server (NAS) aus, wenn Sie eine Verbindung zum Zielsystem aufbauen wollen. Der Name für den Benutzer kann bis zu 256 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Benutzername vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten ihn von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Passwort

Das Passwort benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 256 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Hinweis: Für den Fall, dass Sie den Parameter “Passwort speichern” nicht aktiviert haben, gilt: Auch wenn Sie für den Verbindungsmodus “automatisch” gewählt haben, müssen Sie die Verbindung beim ersten Mal manuell aufbauen. Dabei werden Sie nach dem Passwort gefragt. Für jeden weiteren automatischen Verbindungsaufbau wird dieses Passwort selbständig übernommen, bis Sie den PC erneut booten oder Sie das Zielsystem wechseln.

Passwort speichern

Dieser Parameter muss aktiviert (angeklickt) werden, wenn gewünscht wird, dass das Passwort und das Passwort Ziel (sofern es eingegeben ist) gespeichert wird. Andernfalls werden die Passwörter gelöscht, sobald der PC gebootet wird oder ein Zielsystem gewechselt wird. Standard ist die aktivierte Funktion.

Wichtig: Bitte beachten Sie, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

Rufnummer (Ziel)

Für jedes Ziel muss eine Rufnummer definiert sein, da der Client sonst keine Verbindung herstellen kann. Diese Rufnummer muss genauso eingetragen werden, als würden Sie diese Telefonnummer per Hand wählen. D.h. Sie müssen alle notwendigen Vorwahlziffern berücksichtigen: Landesvorwahl, Ortsvorwahl, Durchwahlziffern, etc. etc.

Tragen Sie jedoch nicht die Amtsholung ein, auch wenn Sie an einer Nebenstellenanlage angeschlossen sind! Die Amtsholung wird unter dem Monitor-Menüpunkt “Konfiguration” eingetragen und hat auf diese Weise Gültigkeit für alle Rufe (→ siehe – Amtsholung).

Beispiel: Sie wollen eine Verbindung von Deutschland nach England herstellen
00 (für die internationale Verbindung, wenn Sie von Deutschland aus wählen)
44 (dies ist die landesspezifische Vorwahl für England)
171 (Vorwahl für London)
1234567 (die Nummer, die Sie zu erreichen wünschen)

Insgesamt wird nach diesem Beispiel folgende Nummer im Telefonbuch gespeichert und für die Anwahl verwendet: 00441711234567
Die Rufnummer des Ziels kann bis zu 30 Ziffern beinhalten.

Hinweis: Wenn ein Zielsystem eine Verbindung zu Ihrem PC über Rückruf aufbauen will, benötigt der Client diese Rufnummer in diesem Feld, um den Rückruf, entsprechend des gewählten Rückrufmodus annehmen zu können.

■ Alternative Rufnummern

Möglicherweise ist das Zielsystem ein Network Access Server (NAS), der mit mehreren S0-Anschlüssen für verschiedene Rufnummern ausgestattet ist. In diesen Fall empfiehlt es sich, alternative Rufnummern einzugeben – falls zum Beispiel die erste Nummer besetzt ist. Die alternativen Rufnummern werden der ersten Nummer angehängt, nur mit einem Doppelpunkt (:) oder einem Semikolon (;) getrennt.

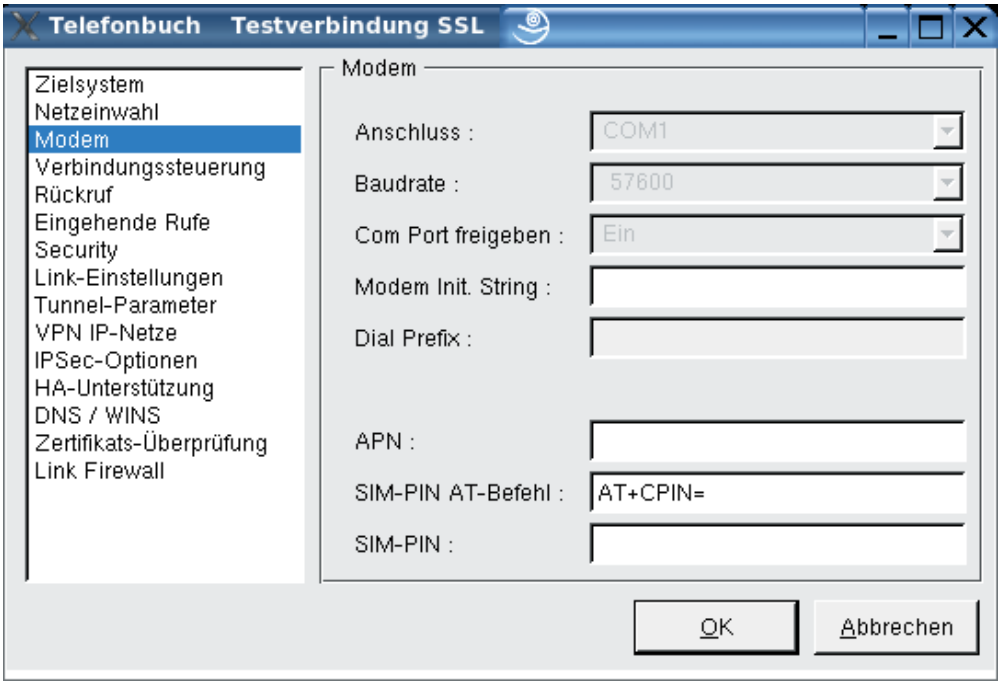
Maximal werden 8 alternative Rufnummern unterstützt.

Beispiel : 000441711234567:000441711234568

Die erste Nummer ist die Standard-Rufnummer und wird immer zuerst gewählt. Kann keine Verbindung hergestellt werden, weil besetzt ist, wird die zweite Nummer gewählt, usw.

Wichtig: Bitte beachten Sie, dass der Verbindungsaufbau nur funktionieren kann, wenn die Protokoll-Eigenschaften für die Anschlüsse der alternativen Rufnummern die gleichen sind.

5.1.3 Modem



Dieses Parameterfeld erscheint ausschließlich, wenn Sie als "Verbindungsart" "Modem" gewählt haben. Alle nötigen Parameter zu dieser Verbindungsart sind hier gesammelt.

Parameter:

- ☐ Anschluss
- ☐ Baudrate
- ☐ Com Port freigeben
- ☐ Modem
- ☐ Modem Init. String
- ☐ Dial Prefix
- ☐ APN
- ☐ SIM PIN AT-Befehl
- ☐ SIM PIN

Anschluss

An dieser Stelle bestimmen Sie, welcher Com Port von Ihrem Modem genutzt werden soll. Wenn Sie bereits Modems unter Windows installiert haben, wird der während dieser Installation festgesetzte Com Port automatisch übernommen, sobald Sie das entsprechende Gerät unter “Modem” auswählen.

Hinweis: Wenn Sie ein bereits unter Ihrem System installiertes Modem nutzen möchten, so wählen Sie vor der Einstellung des Com Ports zuerst das gewünschte Gerät unter “Modem” aus – der entsprechend konfigurierte Com Port wird dann automatisch gesetzt.

Baudrate

Die Baudrate beschreibt die Übertragungsgeschwindigkeit zwischen Com Port und Modem. Wenn Ihr Modem z.b. mit 14.4 Kbits übertragen kann, sollten sie die nächsthöhere Baudrate 19200 wählen.

Folgende Baudraten können gewählt werden:

1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200

Com Port freigeben

Wenn Sie für Ihren Client ein analoges Modem verwenden, kann es wünschenswert sein, dass der Com Port nach Beendigung der Kommunikation für andere Applikationen freigegeben wird (z.B. Fax). In diesem Fall stellen Sie den Parameter auf “Ein”. Solange der Parameter in der Standardstellung auf ”Aus” bleibt, wird der Com Port ausschließlich von der Client Software genutzt.

Modem

Die Geräte, die Sie in der Windows-Systemsteuerung unter “Modems” konfiguriert haben, werden für dieses Konfigurationsfeld des Telefonbuchs zur Auswahl gestellt. Je nachdem, welches Modem Sie wählen, werden die zugehörigen Parameter ”Com Port” und “Modem Init. String” automatisch in die Konfigurationsfelder des Telefonbuchs aus der Treiberdatenbank des Systems übernommen.

Hinweis: Bitte beachten Sie, dass Sie das Modem vor der Konfiguration der Verbindung im Telefonbuch installiert haben müssen, um es korrekt für Kommunikationsverbindungen nutzen zu können.

Modem Init. String

Sofern Ihr Modem korrekt im Windows-System installiert ist, wird der entsprechende “Modem Init. String” automatisch in dieses Feld übernommen. In Ausnahmefällen kann der String mit (Hayes-) Befehlen erweitert werden.

Jeder AT-Befehl innerhalb des Initialisierungs-Strings muss mit <cr> abgeschlossen werden, da ansonsten das Kommando nicht abgesetzt wird. Dies bedeutet, dass in jedem Fall der Init-String mit <cr> abgeschlossen werden muss.

Dial Prefix

Dieses Feld ist optional. Ist das Modem korrekt installiert und steht der Software als Standardtreiber zur Verfügung, so muss hier kein Eintrag vorgenommen werden. Der Dial Prefix ist nur in seltenen Ausnahmefällen nötig. Ziehen Sie dazu das Modem-Handbuch zu Rate. Im folgenden einige Beispiele für Dial Prefix:
ATDT
ATDP
ATDI
ATDX

Die folgenden Parameter sind nur von Bedeutung bei einer Verbindungsart über UMTS / GPRS

APN

Der APN (Access Point Name) wird für die GPRS und UMTS-Einwahl benötigt. Sie erhalten ihn von Ihrem Provider. Der APN wird insbesondere zu administrativen Zwecken genutzt.

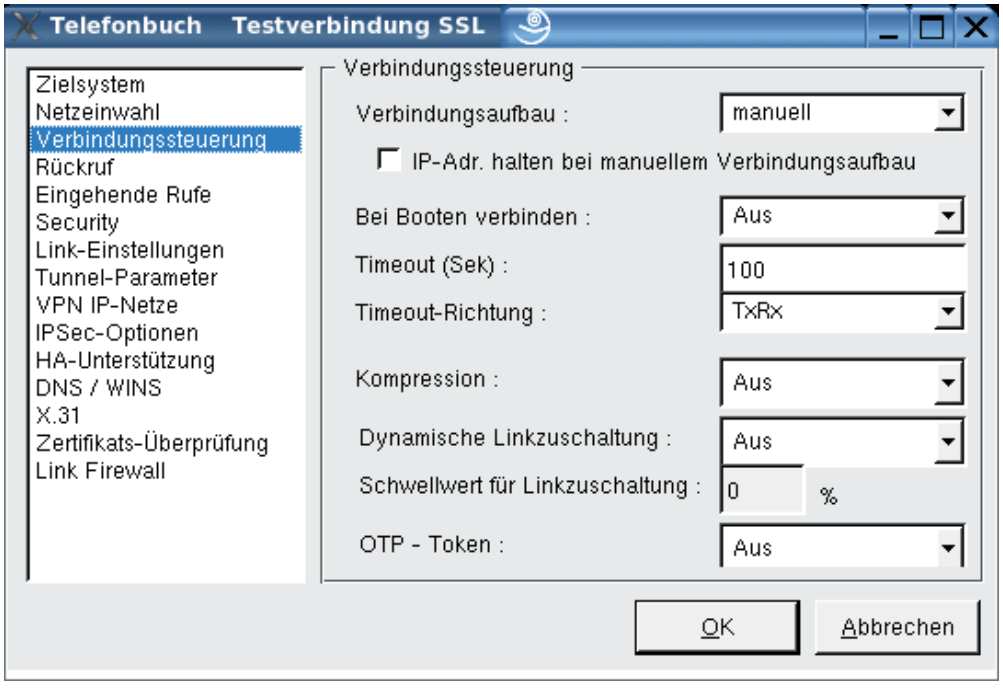
SIM PIN AT-Befehl

Bei Verwendung einer GPRS/UMTS-Karte muss der jeweils spezifische AT-Befehl eingegeben werden. Dieses Kommando bewirkt, dass die SIM PIN richtig erkannt wird.

SIM PIN

Benutzen Sie eine SIM-Einsteckkarte für GPRS oder UMTS, so geben Sie hier die PIN für diese Karte ein. Benutzen Sie ein Handy, so muss diese PIN am Mobiltelefon eingegeben werden.

5.1.4 Verbindungssteuerung



In diesem Parameterfeld bestimmen Sie, wie der Verbindungsaufbau erfolgen soll und stellen die Timeout-Werte ein. Zudem können Sie Kompression aktivieren und die Art der Kompression bestimmen. Mit Kompression kann der Datendurchsatz um den Faktor 3 bis 5 erhöht werden, je nachdem um welche Daten es sich handelt.

Wenn Sie den Secure Client in der "Verbindungsart" "ISDN" betreiben, können Sie in diesem Parameterfeld auch eine Kanalbündelung aktivieren. Bitte beachten Sie dabei, dass die Kanalbündelung nur funktionieren kann, wenn sowohl der Client als auch der NAS für eine Verbindung über gleich viele mögliche Kanäle verfügen.

Parameter:

- ☐ Verbindungsaufbau
- ☐ IP-Adr. halten bei manuellem Verbindungsaufbau
- ☐ Bei Booten verbinden
- ☐ Timeout
- ☐ Timeout-Richtung
- ☐ Dynamische Linkzuschaltung (nur bei "Verbindungsart" "ISDN" möglich)
- ☐ Schwellwert für Linkzuschaltung (nur bei "Verbindungsart" "ISDN" möglich)
- ☐ OTP-Token
- ☐ Kompression

Verbindungsaufbau

Hier definieren Sie, wie die Verbindung zu einem, im Telefonbuch eingetragenen Zielsystem, aufgebaut werden soll. Drei Modi stehen zur Wahl:

automatisch	=	(default) Dies bedeutet, dass die Client Software die Verbindung zum Zielsystem automatisch herstellt. Das Trennen der Verbindung erfolgt je nach Protokoll Ihres Systems, entsprechend den Anforderungen der Anwendung und den Einstellungen im Telefonbuch.
manuell	=	In diesem Fall müssen Sie die Verbindung zum Zielsystem manuell herstellen. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout.
wechselnd	=	Wird dieser Modus gewählt, muss zunächst die Verbindung “manuell” aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau: – Wird die Verbindung nun mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung “automatisch” hergestellt, – wird die Verbindung manuell abgebaut, muss sie auch wieder manuell aufgebaut werden.

Ist der Timeout auf Null (0) gesetzt, d.h. kein Timeout eingestellt, müssen Sie in jedem Fall die Verbindung manuell trennen.

Wichtig: Sollten Sie den Verbindungsaufbau auf “manuell” setzen, so sollten Sie den Timeout aktivieren, um den Verbindungsabbau zu automatisieren. Andernfalls könnten unnötige Verbindungskosten für Sie entstehen.

IP-Adr. halten bei manuellem Verbindungsaufbau

Wird eine Verbindung getrennt – auch durch Timeout – so verliert der Client standardmäßig die IP-Adresse, die ihm das VPN Gateway aus dem Firmennetz für die Session zugewiesen hatte. Ist die Funktion “IP-Adr. halten bei manuellem Verbindungsaufbau” aktiviert, so behält der Client die IP-Adresse nach Beendigung der Verbindung bis zum nächsten manuellen Verbindungsaufbau, sodass die logische Verbindung ununterbrochen bestehen bleibt.

Hinweis: Diese Funktionalität kann nur für manuellen oder wechselnden Verbindungsmodus genutzt werden.

Bei Booten verbinden

In manchen Fällen kann es wünschenswert sein, dass die Verbindung zu einem bestimmten Ziel bereits während der Boot-Phase aufgebaut wird. Dies kann insbesondere für Benutzer interessant sein, die ihren Remote Client-PC genauso booten möchten wie ihren Büro-PC, der an ein LAN angeschlossen ist. Bitte beachten Sie, dass in diesem Fall der Remote-PC so vorkonfiguriert sein muss, dass der LAN-Client in den Boot-Prozeß einbezogen wird.

Wenn Sie “Bei Booten verbinden” aktivieren wollen, schalten Sie dieses Feature auf ”Ein”. Die Standardeinstellung ist “Aus”.

Timeout

Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 0 und 65535 angegeben. Der Standardwert ist “40".

Wenn Ihr Anschluss (ISDN oder analog) einen Gebührenimpuls erhält, verwendet die Client Software das Impulsintervall, um den optimalen Zeitpunkt des Verbindungsabbaus bezüglich dem von Ihnen gesetzten Wert zu ermitteln. Der nach Gebührentakt optimierte Timeout läuft im Hintergrund und hilft die Verbindungskosten zu reduzieren.

Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65356 einzutragen. Mit dem Wert “0" wird der automatische Timeout (Verbindungsabbau) nicht ausgeführt. Der Wert ”0" bedeutet, dass das Trennen der Verbindung manuell durchgeführt werden muss. Ziehen Sie bei diesem Parameter bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

Wichtig: Der Timer für das gewählte Zeitintervall läuft erst dann an, wenn keine Datenbewegung oder Handshaking mehr auf der Leitung stattfindet.

Timeout-Richtung

Mit diesem Parameter bestimmen Sie, für welche Übertragungsrichtung der Timeout gelten soll. Drei verschiedene Einstellungen sind möglich:

TxRx	(standard) in diesem Fall achtet der Client sowohl auf das Ende der gesendeten (out) als auch der empfangenen (in) Daten, bevor der Timer angestoßen wird.
Tx	nur die Senderichtung (out) wird beobachtet.
Rx	nur die Empfangsrichtung (in) wird beobachtet.

Hinweis: Um die Timeout-Richtung zur Geltung kommen zu lassen, muss der Wert für den Timeout zwischen 1 und 65356 gewählt sein.

Kompression

Mit diesem Parameter bestimmen Sie den Typ der eingesetzten Kompression. Drei Einstellungen sind möglich:

Aus	(standard), d.h. ohne Kompression
STAC	(without History)
STAC mit History	Cisco-kompatibel

Wichtig: Der hier gewählte Typ der Kompression muss auch vom Network Access Server (NAS) unterstützt werden.

Ziehen Sie zu weiteren Informationen bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

Dynamische Linkzuschaltung (Nur für ISDN)

Mit dynamischer Linkzuschaltung (für ISDN) kann die Client Software bis zu 8 ISDN B-Kanäle bündeln. Um diese Funktion in vollem Umfang nutzen zu können, muss allerdings Ihr PC wie auch das Zielsystem mit der nötigen Anzahl von So-Schnittstellen (4) ausgestattet sein.

Die dynamische Linkzuschaltung funktioniert nur, wenn sie auch vom Network Access Server des Zielsystems unterstützt wird. Mit dynamischer Linkzuschaltung erhöhen sich zwar die Kosten für jeden zugeschalteten B-Kanal, gleichzeitig verringern sie sich jedoch in gleichem Maße, weil sich die Übertragungsdauer entsprechend verkürzt!

Mit diesem Parameter bestimmen Sie, wie die Linkzuschaltung erfolgen soll. Drei Möglichkeiten stehen zur Auswahl:

Aus	(standard)
Tx	Links werden zugeschaltet, entsprechend der Bitrate abgehender Daten
Rx	Links werden zugeschaltet, entsprechend der Bitrate eingehender Daten
TxRx	Links werden sowohl nach der Bitrate sowohl eingehender als auch abgehender Daten zugeschaltet

Schwellwert für Linkzuschaltung (Nur für ISDN)

Der Wert dieses Parameters teilt der Client Software die Bitrate mit, ab der ein weiterer Link (Kanal) zugeschaltet werden soll. Der Wert entspricht Prozenten der maximalen Bitrate. Mögliche Werte sind von 1 bis 100 (Prozent). Standardwert ist “20". Diese Einstellung gilt für Sender und Empfänger.

Die Zuschaltung eines weiteren Links erfolgt 8 Sekunden nach dem Erreichen des eingestellten Schwellwerts.

Diese Einstellung kommt nur zum Tragen, wenn die Linkzuschaltung aktiviert wurde.

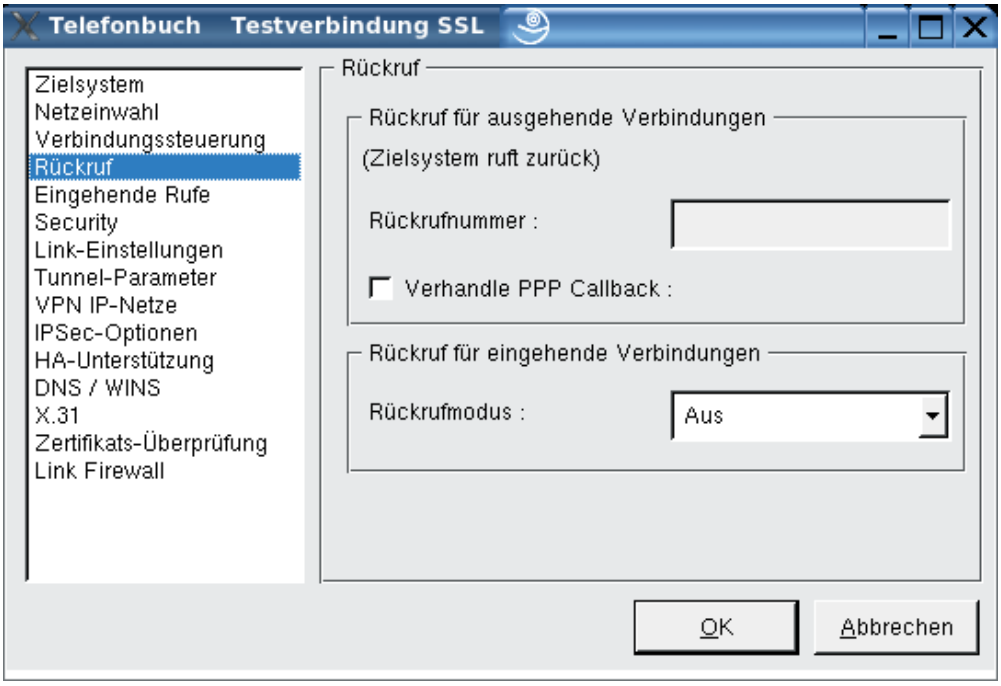
■ OTP-Token

Wird ein OTP-Token verwendet, so kann statt "Passwort" für die Einwahl die PIN und das Onetime-Passwort des Tokens eingegeben werden. Wofür der OTP-Token genutzt wird, wird mit folgenden Einstellungen bestimmt:

Aus	=	(standard) OTP wird nicht genutzt
NAS-Einwahl	=	Wird ein OTP für die Einwahl an einem NAS geutzt, wird das Feld für "Passwort" unter "Netzeinwahl" inaktiv geschaltet.
VPN-Einwahl	=	Wird ein OTP für die Einwahl zum VPN Gateway genutzt, wird entsprechend das Feld für "Passwort (VPN)" unter "Tunnel-Parameter" inaktiv geschaltet.

Bei der Einwahl erscheint ein Dialogfenster für die Eingabe des "Einmalpassworts", in welches PIN und Einmalpasswort des Tokens eingetragen werden müssen.

5.1.5 Rückruf



Dieses Parameterfeld hat keinerlei Bedeutung und erscheint nicht im Telefonbuch, wenn Sie den Secure Client in den Verbindungsarten "LAN (over IP)" oder "PPP over Ethernet" betreiben.

In diesem Parameterfeld erscheinen Parameter, die für Rückruf in Verbindung mit "ausgehenden" und "eingehenden" Rufen definiert werden können.

Parameter:

☐ (Rückruf für ausgehende Verbindungen)
Rückrufnummer
Verhandle PPP Callback

☐ (Rückruf für eingehende Verbindungen)
Rückrufmodus

Rückruf für ausgehende Verbindungen (Zielsystem ruft zurück)

Wichtig ist zunächst zu wissen, dass ein Rückruf der vom zentralseitigen NAS zum Client ausgeführt wird, von den Rechten abhängt, die dem Client entsprechend seiner Benutzer-ID und seines Passworts vom NAS zugewiesen sind.

Wenn kein Rückruf im zentralseitigen Zielsystem zum Client mit dieser Benutzer-ID und diesem Passwort konfiguriert wurde, findet auch kein Rückruf statt, unabhängig davon, welche Rückruf-Parameter im Telefonbuch des Clients konfiguriert wurden.

Wenn jedoch am zentralseitigen NAS (Zielsystem) für den Client mit dieser Benutzer-ID und diesem Passwort eine Rückruf-Option eingerichtet wurde, ist es wichtig zu wissen, wie dieser Rückruf vom NAS ausgeführt wird. Prinzipiell gibt es zwei Rückruf-Methoden, die die meisten Network Access Server ausführen können (und dort im Zielsystem festgelegt werden):

1. Fester Rückruf, der immer zu einem Client mit einer bestimmten (festen) Rufnummer ausgeführt wird. Diese Rückruf-Methode wird zum Beispiel bevorzugt dann angewendet, wenn der Teleworker immer vom Home Office aus kommuniziert.

2. Variabler Rückruf, der dann genutzt wird, wenn sich die Rufnummer zu der der zentralseitige NAS einen Rückruf ausführt ändert (variiert), je nachdem, wo sich der Client gerade befindet. Diese Methode wird zum Beispiel bevorzugt, wenn es sich um Service- oder Verkaufspersonal handelt, das von einem zum nächsten Einsatzort unterwegs ist.

Auch wenn sich der Client zunächst beim zentralseitigen Zielsystem (NAS) einwählt, was eine “ausgehende” Verbindung von Seiten des Clients ist, wird die Rückruf-Methode vom zentralseitigen Zielsystem (NAS) bestimmt.

Zur genaueren Bestimmung ausgehender Verbindungen dienen die folgenden Parameter.

■ Rückrufnummer

Hier tragen Sie die Rufnummer für einen variablen Rückruf ein, unter der der Client erreichbar ist, wenn das zentralseitige Zielsystem (NAS) zurückruft. Die Rufnummer wird in Verbindung mit der PPP-Verhandlung beim Verbindungsaufbau vom Client zum NAS übertragen. Tragen Sie die komplette Rufnummer ein, unter der der Client aktuell zu erreichen ist. Die Rufnummer kann bis zu 30 Ziffern lang sein.

Für einen festen Rückruf muss die Rückrufnummer nicht eingetragen sein, da sie im zentralseitigen NAS hinterlegt ist.

■ Verhandle PPP Callback

Sie aktivieren die PPP Callback-Verhandlung nur, wenn ein Rückruf von der Remote-Seite erfolgen soll und die Remote-Seite den Rückrufmodus PPP Callback verwendet. Erst dann können Sie auch eine Rückrufnummer eintragen.

Diese Funktion muss auch aktiviert werden, wenn die Logon Option unter Windows NT/2000 genutzt wird, unabhängig von der Art des Rückrufs. (Siehe → Logon Optionen)

Rückruf für eingehende Verbindungen

■ Rückrufmodus

Dieser Parameter wird nur für den Rückruf benötigt, den die Client-Software an das Zielsystem ausführt.

Die Standardeinstellung ist “Aus”. Dies bedeutet, dass die Client-Software keinen Rückruf ausführt.

Damit die Client-Software einen Rückruf an das remote Zielsystem ausführen kann, ist es unbedingt nötig, dass im Parameterfeld “Eingehende Rufe” folgende Einstellungen vorgenommen werden:

☑ Die Client-Software muss abgehende und eingehende Rufe abarbeiten können. Deshalb muss der Parameter “Richtung” in ”Eingehende Rufe” auf “bidirektional” gesetzt sein.

☑ Das remote Zielsystem muss sich zuerst gegenüber der Client-Software mit “Benutzer lokal” und ”Passwort lokal” in “Eingehende Rufe” ausweisen.

☑ Die Client-Software führt den Rückruf an die Rufnummer aus, die im Parameterfeld “Netzeinwahl” für ”Rufnummer Ziel” eingetragen wurde.

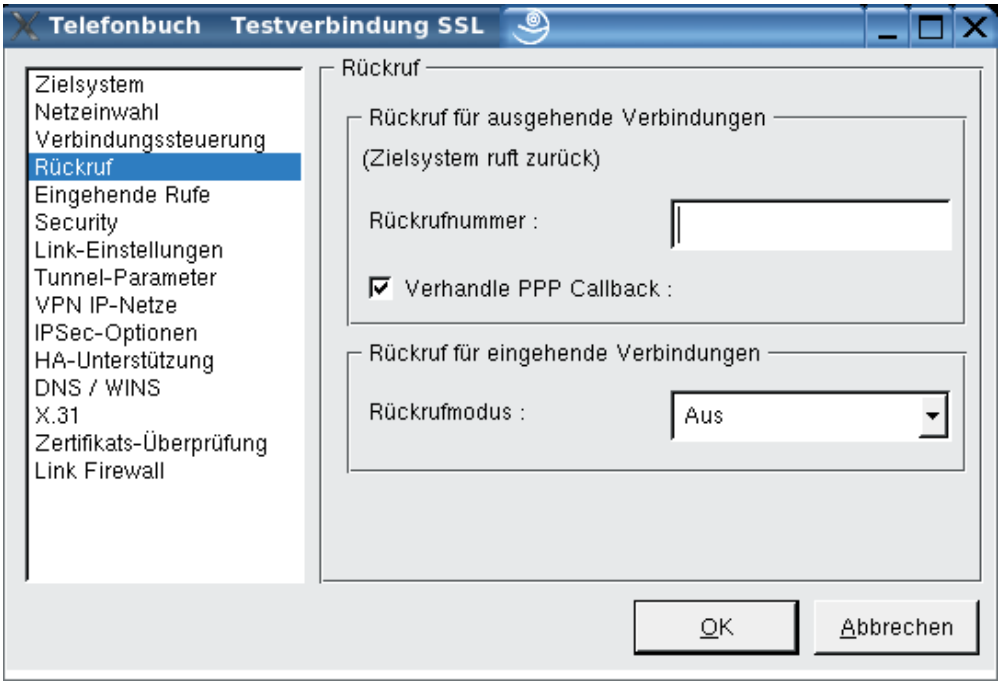
☑ Dabei muss sich die Client-Software auch gegenüber dem remote Zielsystem ausweisen. Dies geschieht mit “Benutzer” und ”Passwort” im Parameterfeld “Netzeinwahl”.

Rückrufmodi:

Aus	(standard)
PPP	(RFC 1570 konform) wird von den meisten NAS unterstützt
NCP	(NCP-spezifisch) kann mit NARAC Enterprise eingesetzt werden
COSO	(Charge-One-Side-Only) auch Low-Level- oder D-Kanal-Rückruf. Im ISDN D-Kanal fallen keine (lokalen) Gebühren für den Client an. COSO ist auch Cisco-kompatibel.

Zu weitergehenden Fragen zu diesem Thema befragen Sie bitte Ihren Systemadministrator.

5.1.6 Eingehende Rufe



In diesem Parameterfeld legen Sie fest, ob eingehende Rufe oder ein Tunnelaufbau von der Zentrale (Zielsystem) an diesen Client zugelassen wird und wie der Client damit umgehen soll.

Parameter:

- ☐ Richtung
- ☐ Benutzername der Gegenstelle
- ☐ Passwort der Gegenstelle
- ☐ Rufnummer lokal
- ☐ gegenseitige Authentisierung

Richtung

Mit der Richtung legen Sie die zulässigen Kommunikationsrichtungen zwischen Ihrem Client und der Remote-Seite (Zielsystem) fest:

abgehend	=	(Standardeinstellung) Der Client wählt sich an die Remote-Seite (Zielsystem) an.
eingehend	=	Das von Ihnen definierte Zielsystem wählt sich an den Client an.
bidirektional	=	Die Kommunikation kann in beide Richtungen stattfinden. Dies ist insbesondere dann nötig, wenn ein automatischer Rückruf von der Remote-Seite (Zielsystem) an den Client konfiguriert wurde (siehe → Rückruf).

“Benutzer lokal” und ”Passwort lokal” teilen Sie Ihrem Remote-Partner zu. Dies ist nur möglich, wenn Sie “gegenseitige Authentisierung” aktiviert haben (siehe Bild rechts). Damit ist gewährleistet, dass nur der Partner, der über diese Codes verfügt, sich bei Ihnen einwählen kann.

Benutzername der Gegenstelle

Den hier eingetragenen Benutzernamen muss der Kommunikationspartner verwenden, der sich an diesen Client anwählen will. Die Client Software prüft nach CHAP, wer sich anmeldet. Der Remote-Partner muss sich als genau der Benutzer anmelden, als der er in diesem Feld eingetragen ist, ansonsten wird die Verbindung abgewiesen.

Der Name darf bis zu 256 Zeichen lang sein.

Wichtig: Dieser Parameter kommt nur zur Geltung, wenn gegenseitige Authentisierung aktiviert wurde oder ein Rückruf an den Client erfolgt.

Passwort der Gegenstelle

Das hier eingetragene Passwort muss der Kommunikationspartner verwenden, der sich an diesen Client anwählen will. Die Client Software prüft nach CHAP wer sich bei Ihnen anmeldet. Der Remote-Partner muss sich als genau der Benutzer anmelden, als der er mit dem Passwort in diesem Feld eingetragen ist, ansonsten wird die Verbindung abgewiesen.

Der Name darf bis zu 256 Zeichen lang sein.

Wichtig: Dieser Parameter kommt nur zur Geltung, wenn gegenseitige Authentisierung aktiviert wurde oder ein Rückruf an Ihren Client erfolgt.

Rufnummer lokal

Dieser Parameter hat keine Bedeutung und wird ausgeblendet, wenn der Client mit der Verbindungsart “LAN (over IP)” oder ”PPP over Ethernet” betrieben wird.

Die lokale Rufnummer wird benötigt, wenn verschiedene ISDN-Geräte an einem NTBA oder ISDN-Bus angeschlossen sind und jedes über eine eigene Nummer oder MSN verfügt. Wenn Sie die korrekte Rufnummer (MSN) für Ihren PC eintragen (die Rufnummer ohne Vorwahl!), und auch die Gegenstelle genau diese Nummer (im Fernbereich mit Vorwahl!) wählt, ist sichergestellt, dass bei eingehenden Rufen nur Ihr PC (Gerät) angesprochen wird. Diese Rufnummer wird dann im ISDN D-Kanal übertragen, wenn keine Rufnummernunterdrückung eingeschaltet ist. Dann kann sie auch zur gesonderten Gebührenabrechnung und zur Identifikation am Zielsystem verwendet werden.

Die Rufnummer kann bis zu 30 Ziffern lang sein.

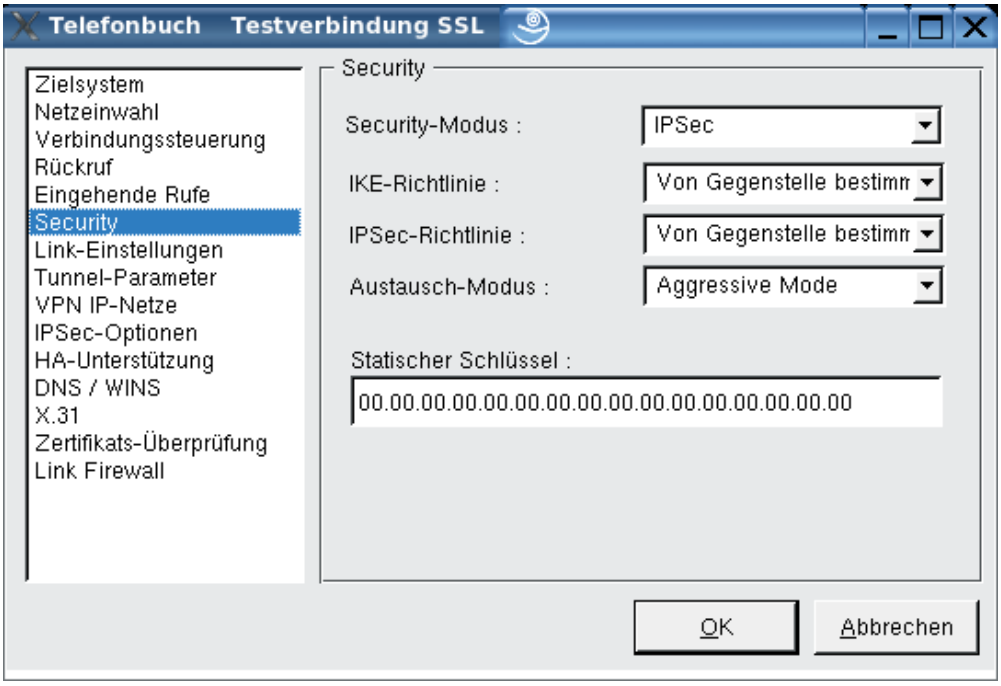
Hinweis: Sollte gewünscht sein, dass alle für diesen Anschluss eingehenden Rufe empfangen werden, so muss dieses Feld leer bleiben.

gegenseitige Authentisierung

Wenn gewünscht wird, dass sich der Remote-Partner und der Client immer gegenseitig per CHAP oder PAP identifizieren, bevor eine Verbindung hergestellt wird, so muss diese Funktion durch Anklicken aktiviert werden.

Diese Seite ist frei →

5.1.7 Security



Im Parameterfeld "Security" sind die Konfigurationsparameter zu L2Sec und IPSec für den Einsatz in Remote Access-Umgebungen gesammelt. Je nach eingestelltem Sicherheits-Modus, L2Sec oder IPSec, kann eine weitergehende Parametrisierung vorgenommen werden.

Der Sicherheits-Modus "L2Sec" wurde in früheren Versionen der Secure Software standardmäßig immer eingesetzt, wenn eine der angebotenen Verschlüsselungsarten gewählt wurde! In früheren Versionen der Secure Software hieß das Parameterfeld "Security" "Verschlüsselung".

Sofern IPSec für Remote Access eingesetzt wird, wird die Secure Policy Database (SPD) nach Vorgabe der hier eingestellten Parameter dynamisch aufgebaut (siehe im Handbuch → IPSec für Remote Access – IPSec over L2TP). Alle IP-Pakete für dieses Ziel werden über die dynamische SPD abgearbeitet. In diesem Fall wird eine statische SPD-Konfiguration nicht benötigt – so dass eventuell im Konfigurationsbaum vorhandene statische SPDs "inaktiv" geschaltet werden können!

Sind statische SPDs aktiv geschaltet, so werden im IPSec-Prozess zunächst für jedes IP-Paket die Filter der statischen SPDs abgearbeitet.

Aus Sicherheitsgründen ist IPSec für Remote Access nur im Tunnelmodus nutzbar. Der Transportmodus mit Authentication Header ist in diesem Parameterfeld für eine dynamische SPD nicht konfigurierbar und kann nur für statische SPDs eingestellt weren (siehe → Beispiele und Erklärungen, IPSec, AH und ESP im Tunnel- und Transportmodus).

Mit der Verschlüsselung werden wichtige Datenbestände eines Computer-Netzwerks und -Systems geschützt. Vor allem bei der Übertragung sensibler Daten über öffentliche Netze, die jedermann nutzen kann, ist die Verschlüsselung von größter Bedeutung. In der Secure Client Software ist eine Reihe von Sicherheitsmechanismen implementiert, um den Zugriff unautorisierter Personen zu verhindern und eine unbefugte Nutzung auszuschließen. Obwohl Standards zur Verschlüsselung existieren (DES oder AES), sind bislang noch keine ausreichenden Sicherheits-Standards entwickelt worden, die auch für die Interoperabilität zwischen verschiedenen Systemen ähnlich hohe Sicherheit gewähren. Daher ist es unbedingt erforderlich, dass die Gegenstelle des Secure Clients die entsprechend gleichen Standards unterstützt. Weiterhin ist NCP bemüht jeden neu verfügbaren Verschlüsselungs-Standard zu implementieren.

Parameter:

☐ Security-Modus

☐ Verschlüsselung |Security

☐ Index |Security

☐ Statischer Schlüssel |Security

☐ Preshared Key |Security

☐ Dateiname |Security

☐ IKE-Richtlinie |Security

☐ IPSec-Richtlinie |Security

☐ Austausch-Modus |Security

☐ IKE ID-Typ

☐ IKE ID

Security-Modus

Hier legen Sie den Sicherheits-Standard für eine Verbindung fest, L2Sec oder IPSec. Bitte beachten Sie dabei, dass nur mit L2Sec neben IP-Paketen auch NetBios-, IPX- und SNA-Daten übertragen werden können.

inaktiv	=	Verschlüsselung und Authentisierung sind ausgeschaltet
L2Sec	=	NCP Standard. Alle Sicherheits-Verhandlungen erfolgen verschlüsselt und sicher in einem End to End-Tunnel (Layer 2) zwischen Client und Secure Server (siehe → Beispiele und Erklärungen, L2Sec – Layer 2-Verbindungen mit Security).
IPSec	=	Zusätzlich kann mit dieser Option über jeden Layer-2-Medientyp (siehe → verfügbare Verbindungsarten), wie ISDN oder L2TP, zwischen Client und Secure Server der Standard IPSec im Tunnel-Modus (Layer 3) eingesetzt werden (siehe → Beispiele und Erklärungen, IPSec für Remote Access – IPSec over L2TP).

Verschlüsselung |Security

In diesem Feld bestimmen Sie, ob eine Verschlüsselung eingesetzt wird, und welche Art der Verschlüsselung verwendet werden soll.

Aus	=	Verschlüsselung nicht aktiv (standard)
Von Gegenstelle bestimmt	=	Die Daten werden je nach Verschlüsselungstechnik des Zielsystems nach Blowfish 128 / 448 oder Triple DES verschlüsselt übertragen.
SSL mit Zertifikat	=	Mit dieser Verschlüsselung ist ein Verbindungsaufbau nur möglich, wenn vorher eine gültige PIN eingegeben wurde. Diese Verschlüsselungsart (wie auch Blowfish und 3DES unter “ Von Gegenstelle bestimmt”) wird vom Zentralsystem vorgegeben.

Index |Security

An dieser Stelle wird der Index für die Schlüsseldatei eingegeben. Dazu muss zuvor die Verschlüsselung aktiviert worden sein.

Mögliche Werte sind von 1 bis 512. Standard ist “1".

Wichtig: Der Index muss abgestimmt sein mit dem in der Konfiguration der Remote-Seite.

Statischer Schlüssel |Security

Der Schlüssel kann nur eingegeben werden, wenn vorher die Verschlüsselung aktiviert wurde. Der Schlüssel ist ein String mit 16 hexadezimalen Zahlen, die durch einen Punkt (.) getrennt sind.
Standard ist: 00.11.22.33.44.55.66.77.88.99.AA.BB.CC.DD.EE.FF

Wichtig: Der Schlüssel muss abgestimmt sein mit dem in der Konfiguration der Remote-Seite (Zielsystem).

Preshared Key |Security

Der Preshared Key ist ein String beliebiger Zeichen in einer maximalen Länge von 255 Zeichen. Der Preshared Key muss nur dann eingegeben werden, wenn eine Verbindung mit “IPSec-Tunneling” zu einem fremden IPSec Gateway aufgebaut werden soll und diese Gegenstelle als IKE-Richtlinie “Preshared Key” erwartet.

Dateiname |Security

An dieser Stelle wird Name und Pfad der Schlüsseldatei eingetragen. Die Schlüsseldatei muss 512 Bytes groß sein und wird als Bestandteil des Verschlüsselungsverfahrens zusammen mit dem Schlüssel verwendet. Die

Verschlüsselungsdatei kann in einem beliebigen Verzeichnis auf der Festplatte abgelegt werden. Name und Pfad der Datei müssen dann unter “Dateiname” mit dem Prefix “\??\” eingeben werden (z.B.: \??\c:\winnt\ncple\crypt.key).

Wichtig: Der Dateiname muss abgestimmt sein mit dem in der Konfiguration der Remote-Seite (Zielsystem).

IKE-Richtlinie |Security

Die IKE-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IKE-Richtlinien aufgeführt, die Sie im Konfigurationsbaum unter der Verzweigung “IPSec – IKE-Richtlinie” angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig vorkonfiguriert mit der Software ausgeliefert werden (siehe → Beispiele und Erklärungen, IPSec, IKE-Modi). Sie finden sie unter Konfiguration unter “IPSec – IKE-Richtlinie” als “Preshared Key” und “RSA-Signatur”. Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf (siehe → IPSec, IKE-Richtlinie, Authentisierung, Verschlüsselung), d.h. eine Richtlinie besteht aus verschiedenen Vorschlägen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Von Gegenstelle bestimmt:

In diesem Fall kann die Konfiguration der IKE-Richtlinie im IPSec-Menü entfallen.

Preshared Key:

Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden. Beidseitig wird der gleiche “Statische Schlüssel” verwendet (siehe oben → Statischer Schlüssel).

RSA-Signatur:

Diese vorkonfigurierte Richtlinie kann nur mit PKI-Unterstützung eingesetzt werden. Als zusätzliche, verstärkte Authentisierung ist der Einsatz der RSA-Signatur nur sinnvoll unter Verwendung einer Smartcard oder eines Soft-Zertifikats.

■ IPSec-Richtlinie |Security

Die IPSec-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IPSec-Richtlinien aufgeführt, die Sie unter “Konfiguration” unter der “IPSec – IPSec-Richtlinie” angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Funktional unterscheiden sich zwei IPSec-Richtlinien nach dem IPSec-Sicherheitsprotokoll AH (Authentication Header) oder ESP (Encapsulating Security Payload). Da der IPSec-Modus mit AH-Sicherung für flexiblen Remote Access völlig ungeeignet ist, wird nur eine IPSec-Richtlinie mit ESP-Protokoll standardmäßig vorkonfiguriert mit der Software ausgeliefert (siehe → Beispiele und Erklärungen, IPSec, AH und ESP). Sie finden sie unter “Konfiguration” unter “IPSec – IPSec-Richtlinie”. Inhalt und Name dieser Richtlinie können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPSec-Protokoll und Authentisierung auf (siehe → IPSec, IPSec-Richtlinie, Protokoll, Authentisierung), d.h. eine Richtlinie besteht aus verschiedenen Vorschlägen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Von Gegenstelle bestimmt:

In diesem Fall kann die Konfiguration der IKE-Richtlinie im IPSec-Menü entfallen.

Austausch-Modus |Security

Der Austausch-Modus bestimmt wie der Internet Key Exchange vonstatten gehen soll. Zwei unterschiedliche Modi stehen zur Verfügung, der Main Mode, auch Identity Protection Mode und der Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch deren Verschlüsselung (siehe → Beispiele und Erklärungen, IPSec, IKE-Modi).

Main Mode:

Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

Aggressive Mode:

Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

IKE ID-Typ |Security

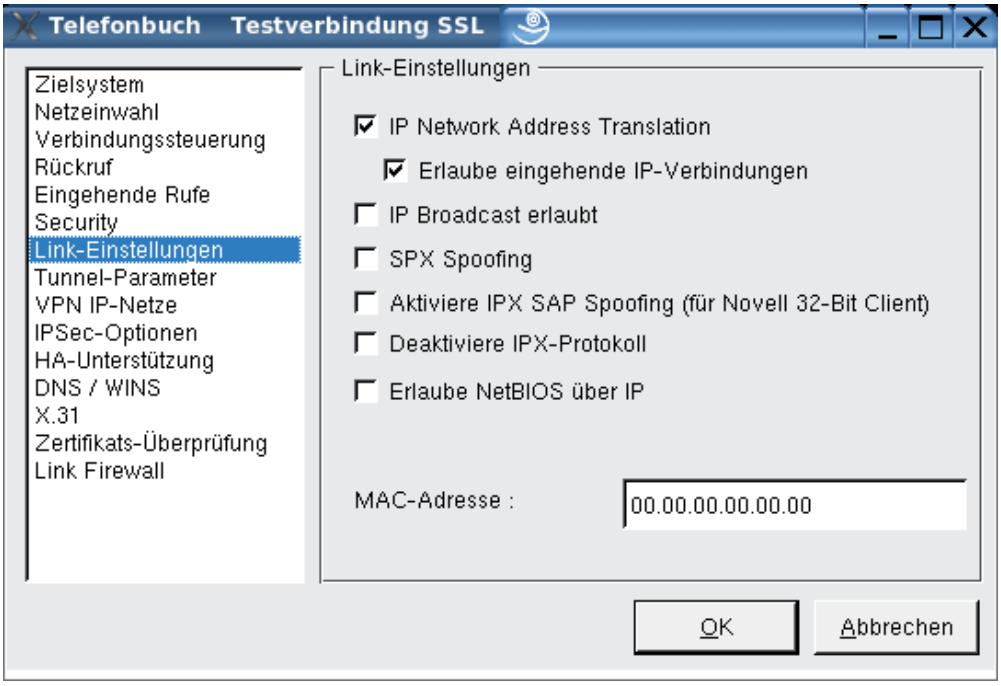
Bei “IPSec-Tunneling” (native IPSec) werden die Parameter “IKE ID-Typ” und “IKE ID” eingeblendet. Für den “IKE ID-Typ” stehen folgende Alternativen zur Auswahl:

– IP Address
– Fully Qualified Domain Name
– Fully Qualified Username
– IP Subnet Address
– ASN1 Distinguished Name
– ASN1 Group Name
– Free String used to identify Groups

IKE ID |Security

Entsprechend dem “IKE ID-Typ” muss die zugehörige “IKE ID” als String eingetragen werden.

5.1.8 Link Einstellungen



Die Einstellungen in diesem Parameterfeld hängen vom Network Access Server des jeweiligen Zielsystems ab. Wenn Ihnen diese Parameter nicht bekannt vorkommen, oder Sie unsicher bei der jeweiligen Einstellung sind, wird empfohlen sich an Ihren Systemadministrator oder Ihren Internet Service Provider zu wenden, um weitere Informationen zu bekommen.

Parameter:

☐ IP Network Address Translation

☐ Erlaube eingehende IP-Verbindungen

☐ IP Broadcast erlaubt

☐ SPX Spoofing

☐ Aktiviere IPX/SAP Spoofing

☐ Deaktiviere IPX-Protokoll

☐ Erlaube NetBios over IP

☐ MAC-Adresse

IP Network Address Translation

IP Network Address Translation wird bei der Installation der Client Software bereits vorgesehen und ist standardmäßig beim Anlegen eines neues Zielsystems aktiviert!

Wenn IP Network Address Translation aktiviert ist, werden alle übertragenen Frames mit der ausgehandelten (PPP) IP-Adresse verschickt. Wenn Sie IP Network Address Translation nutzen, können Sie jede beliebige IP-Adresse in Ihren Systemeinstellungen konfigurieren, da die Client Software die ausgehandelte (PPP) IP-Adresse in Ihre systemeigene übersetzt. Die DHCP Wartezeit wird in diesem Fall ignoriert.

Wenn Sie die Eigenschaften des Protokolls ändern wollen, um DHCP zu nutzen oder eine feste IP-Adresse einzustellen, gehen Sie wie folgt vor:

→ IP Network Address Translation deaktivieren
→ Windows Startmenü
→ Einstellungen
→ Systemsteuerung
→ Netzwerk
→ Protokoll hinzufügen oder konfigurieren
→ Eigenschaften

Hinweis: Die meisten Internet Service Provider nutzen die Network Address Translation zur Kommunikation.

Erlaube eingehende IP-Verbindungen

Mit dem Schalter “Erlaube eingehende IP-Verbindungen” kann IP NAT modifiziert werden. Wenn dieser Schalter gesetzt ist, kann eine Verbindung aktiv von außerhalb aufgebaut werden, und die Gegenstelle kann auf den Rechner zugreifen.

Bitte beachten Sie, dass es nur sinnvoll ist, diesen Schalter zu setzen wenn der Zugriff von einer definierten Gegenstelle erfolgen, z.B. aus dem Firmennetz, da mit dem Setzen dieses Schalters der Schutzmechanismus von IP-NAT (private Firewall) aufgehoben wird.

D.h. potentiell kann jeder Teilnehmer aus dem eingewählten Netz auf den Rechner mit der Client Software zugreifen. Wenn Sie also eingehende IP-Verbindungen erlauben, und sich über ISDN in das Internet eingewählt haben, hat jeder Internet-Teilnehmer die Möglichkeit zur Einwahl. Anders in einem Virtual Private Network (VPN). Nur die Teilnehmer dieses VPN haben die Möglichkeit zur Einwahl, der Tunnel blockt alle sonstigen Verbindungsversuche ab.

IP Broadcast erlaubt

Mit diesem Parameter entscheiden Sie, ob die Client Software die Übertragung von IP-Broadcasts zulassen soll. IP-Broadcasts werden z.B. dann eingesetzt, wenn ein LAN-

Client (wie etwa die Client Software) im Netz nach einem File Server sucht. Im Fall des Clients wäre das Netz ein Remote-LAN, an welches der Client via ISDN angeschlossen ist. IP-Broadcasts werden unterdrückt, wenn das Feld nicht angeklickt ist (standard).

Hinweis: IP-Broadcasts müssen Sie zulassen, wenn Sie DHCP nutzen um eine IP-Adresse vom Zielsystem anzufordern.

■ SPX Spoofing

Dieser Parameter entscheidet über die Verwendung von SPX-Spoofing. SPX wird häufig in Novell-Netzen gefahren und kann zusätzliche Kommunikationskosten verursachen, da durch das Polling von SPX ein Timeout verhindert wird. SPX-Spoofing wird mit einem Klick auf das Feld aktiviert.

Wichtig: SPX-Spoofing muss auch vom Network Access Server der Remote-Seite unterstützt werden

■ Aktiviere IPX/SAP Spoofing

Dieser Parameter kann in Verbindung mit einem Novell 32-Bit Client genutzt werden. IPX/SAP-Frames werden nicht übertragen, wenn die Funktion mit einem Haken aktiviert ist.

■ Deaktiviere IPX-Protokoll

Mit diesem Parameter wird ein Filter gesetzt, der IPX Frames unterdrückt. Diesen Filter zu setzen ist immer dann zweckmäßig, wenn das Zielsystem in einer reinen IP-Umgebung liegt, zum Beispiel im Internet.

In der Standardeinstellung ist dieser Filter nicht gesetzt, das heißt der Checkbutton nicht mit einem Haken markiert, so dass IPX Frames nicht unterdrückt werden.

Wenn Sie eine E-Version der Software nutzen, beachten Sie bitte auch die Beschreibung zum Parameter “Deaktiviere SNA-, NetBeui-Protokoll” unter ”Bridge-Parameter”.

■ Erlaube NetBios over IP

Mit diesem Parameter wird ein Filter aufgehoben, der Microsoft NetBios Frames unterdrückt. Diesen Filter aufzuheben, um den Verkehr von NetBios Frames zu gestatten, ist immer dann zweckmäßig, wenn Sie zum Beispiel Microsoft Networking über den Secure Client nutzen.

In der Standardeinstellung ist dieser Filter gesetzt, das heißt der Checkbutton nicht mit einem Haken markiert, so dass Microsoft NetBios Frames unterdrückt werden, damit sie den Datenverkehr nicht unnötig belasten. Markieren Sie den Checkbutton mit einem Haken, werden NetBios Frames over IP erlaubt.

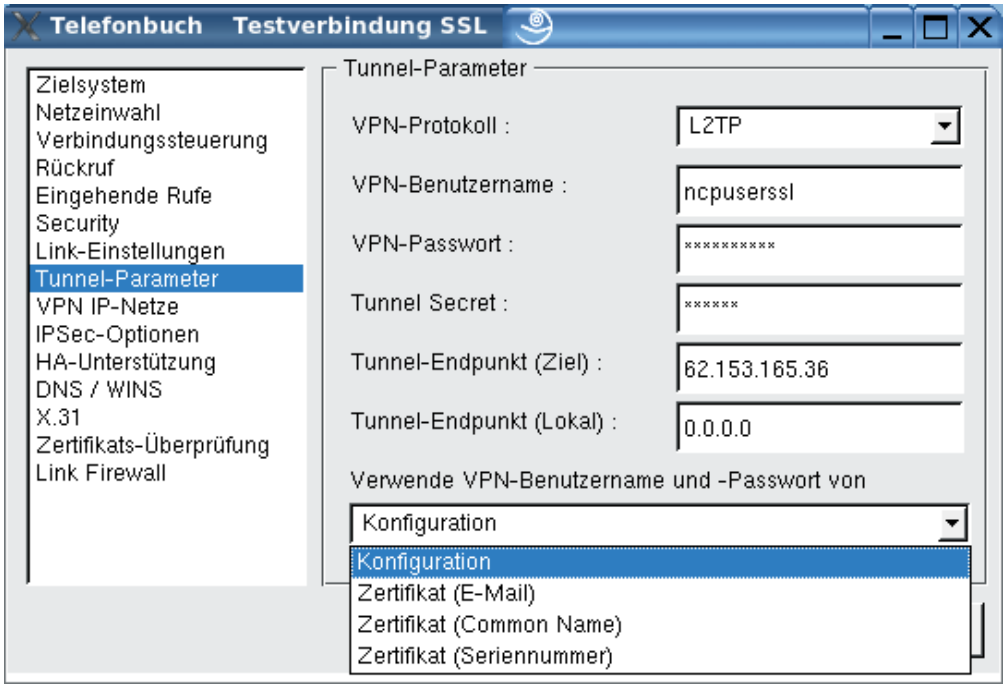
■ MAC-Adresse

Die MAC-Adresse ist die Adresse des Netzwerkadapters im LAN. Sie wird für Identifikationszwecke benötigt (DHCP). Sie ist eine Adresse mit 6 hexadezimalen Zahlen, die durch einen Punkt "." getrennt sind.

Die Standardadresse ist 00.00.00.00.00.00

Ziehen Sie bei diesem Parameter bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

5.1.9 Tunnel – Parameter



Diese Parameter sind nur von Bedeutung, wenn zwischen dem Client und dem VPN-Gateway ein Tunnel (VPN) aufgebaut werden soll, d.h. das Zielsystem IPSec oder L2TP unterstützt. Die jeweiligen Einstellungen hängen vom Network Access Server des Zielsystems (VPN-Gateway) ab. Wenn Sie unsicher bei der jeweiligen Einstellung sind, wenden Sie sich bitte an Ihren Systemadministrator oder Ihren Internet Service Provider.

Parameter:

- ☐ VPN-Protokoll
- ☐ VPN-Benutzername
- ☐ VPN-Passwort
- ☐ Tunnel Secret
- ☐ Tunnel-Endpunkt (Ziel)
- ☐ Tunnel-Endpunkt (Lokal)
- ☐ Verwende VPN-Benutzername und -Passwort von

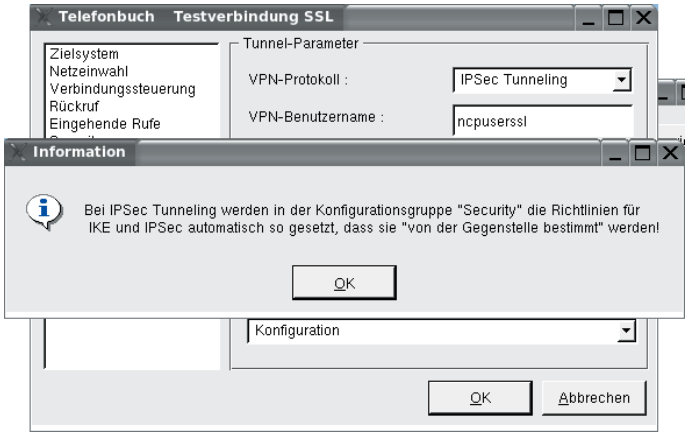
■ VPN-Protokoll

Nicht benutzen = Zwischen dem Client und dem Zielsystem wird kein Tunnel aufgebaut.

L2TP = Mit diesem Schalter bestimmen Sie, ob das L2TP-Protokoll (Layer 2 Tunneling Protokoll) gefahren werden soll. Dieses Protokoll wird für Tunneling über VPN benötigt.

IPSec-Tunneling = Wird das VPN-Protokoll “IPSec-Tunneling” (native IPSec) gewählt, so wird die IPSec-Verbindung ohne einen Layer 2-Tunnel (L2TP) hergestellt.

Verbindung zu IPSec Gateways anderer Hersteller:



Bei Auswahl von “IPSec-Tunneling” wird darauf hingewiesen, dass im Konfigurationsfeld “Security” automatisch folgende Einstellungen vorgenommen werden:

Security-Modus = IPSec
IKE-Richtlinie = Von Gegenstelle bestimmt
IPSec-Richtlinie = Von Gegenstelle bestimmt
Austausch-Modus = Main Mode

Diese automatisch vorgenommenen Einstellungen können je nach den Anforderungen des fremden IPSec Gateways auch modifiziert werden. Weiterhin ist für den Einsatz von IPSec-Tunneling folgendes zu beachten:

Im Konfigurationsfeld “Security” werden die Parameter “IKE ID-Typ” und “IKE ID” zur Konfiguration eingeblendet (siehe → Security).

“Preshared Key” oder “RSA Signatur”: Entsprechend den Vorgaben durch die Gegenstelle kann als “IKE-Richtlinie” die automatisch vorgenommene Einstellung “Von Gegenstelle bestimmt” auf “Preshared Key” oder “RSA Signatur” (Zertifikat) abgeändert werden. Erwartet die Gegenstelle “Preshared Key”, so muss der Schlüssel in das Feld

eingetragen werden. (Der Preshared Key muss in diesem Fall für alle Clients identisch sein.)

IP-Adressen und DNS Server werden über das Protokoll IKE-Config Mode (Draft 2) zugewiesen (kompatibel derzeit nur gegen Cisco). Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

Wird “IPSec-Tunneling” genutzt, so erfolgt die Authentisierung über Extended Authentication (XAUTH Protokoll, Draft 6). Dazu müssen noch folgende Parameter im Konfigurationsfeld “Tunnel-Parameter” gesetzt werden:

VPN-Benutzername = Benutzername des IPSec-Benutzers
VPN-Passwort = Kennwort des IPSec-Benutzers
Verwende VPN-Benutzername und -Passwort von = optional

Bei “IPSec-Tunneling” wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der IPSec Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Der Einsatz von NAT Traversal erfolgt beim IPSec Client automatisch und ist immer nötig, wenn auf Seiten des Zielsystems ein Gerät mit Network Address Translation zum Einsatz kommt.

■ VPN-Benutzername

Ihre User ID, in diesem Fall für das VPN-Gateway, erhalten Sie von Ihrem Systemadministrator. Der Name kann bis zu 256 Zeichen lang sein.

■ VPN-Passwort

Das Passwort, in diesem Fall für das VPN-Gateway, erhalten Sie von Ihrem Systemadministrator. Das Passwort kann bis zu 256 Zeichen lang sein.

■ Tunnel Secret

“Tunnel Secret” ist ein Passwort, das für den Tunnelaufbau benötigt wird. Nur wenn dieses Passwort beim VPN-Gateway und dem VPN-Client übereinstimmt, wird der Tunnel aufgebaut. Das Passwort kann bis zu 16 Zeichen lang sein.

■ Tunnel-Endpunkt (Ziel)

Dies ist die IP-Adresse des VPN-Gateways, auch Tunnel Endpoint. Die Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen. Für jede

Zahl stehen 8 Bits zur Verfügung, wodurch sie 256 Werte annehmen kann. Sie erhalten die IP-Adresse von Ihrem Administrator.

■ Tunnel-Endpunkt (Lokal)

Dies ist die IP-Adresse des Clients. Die Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennt Zahlen. Für jede Zahl stehen 8 Bits zur Verfügung, wodurch sie 256 Werte annehmen kann. Sie erhalten die IP-Adresse von Ihrem Systemadministrator.

■ Verwende VPN-Benutzername und -Passwort von

Als Zugangsdaten für ein VPN können folgende Einträge ausgelesen und verwendet werden:

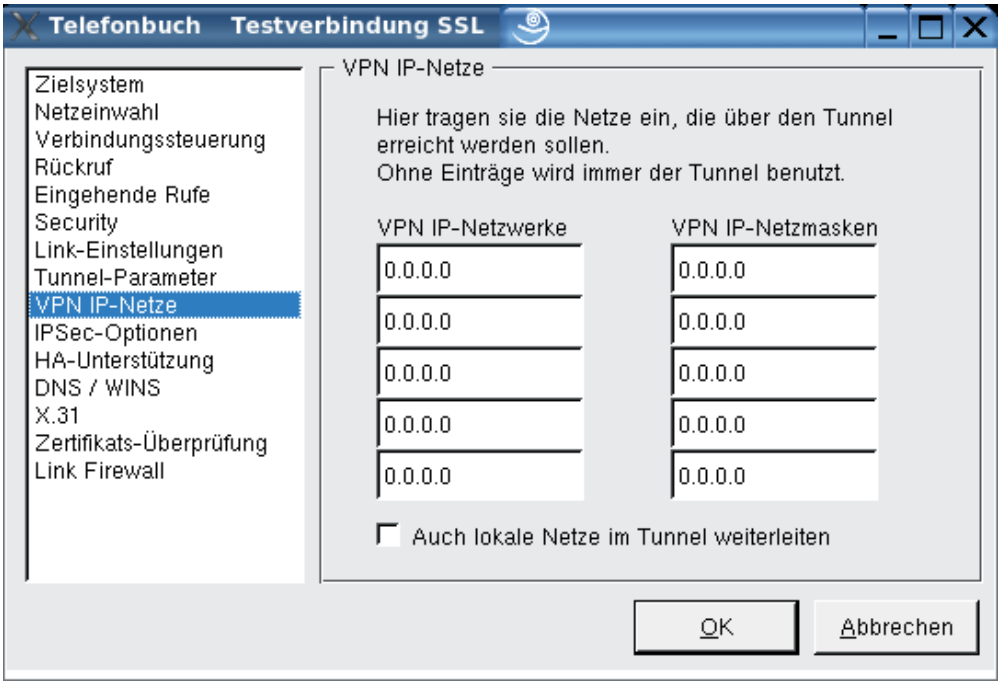
☑ Konfiguration: Dies bedeutet, dass die in diesem Parameterfeld unter “VPN-Benutzername” und ”VPN-Passwort” gemachten Angaben zur VPN-Authentisierung verwendet werden.

☑ Zertifikat (E-Mail): Dies bedeutet, dass statt “VPN-Benutzername” und ”VPN-Passwort” der E-Mail-Eintrag des Zertifikats verwendet wird.

☑ Zertifikat (Common Name): Dies bedeutet, dass statt “VPN-Benutzername” und ”VPN-Passwort” der Benutzer-Eintrag des Zertifikats verwendet wird.

☑ Zertifikat (Seriennummer): Dies bedeutet, dass statt “VPN-Benutzername” und ”VPN-Passwort” die Seriennummer des Zertifikats verwendet wird.

5.1.10 VPN IP-Netze



Hier können genau die IP-Netze definiert werden, über die der Client via VPN-Tunnel kommunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so wird die Verbindung immer zum Tunnel-Endpunkt des Gateways aufgebaut. Soll alternierend einerseits ein Tunneling zur Zentrale erfolgen, andererseits über das Internet kommuniziert werden, so müssen hier die IP-Netze eingetragen werden, die vom Client erreicht werden sollen. Sie können dann zwischen dem Internet und dem Gateway der Firmenzentrale hin und her springen. Dies wird auch als "Split Tunneling" bezeichnet.

Parameter:

☐ VPN IP-Netzwerke

☐ VPN IP-Netzmasken

☐ Auch lokale Netze im Tunnel weiterleiten

VPN IP-Netzwerke

Hier tragen Sie die Adresse des IP-Netzes ein, das vom Client über das VPN-Gateway erreicht werden soll. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Machen Sie in dieser Liste keinen Eintrag, so werden alle IP-Pakete über den VPN-Tunnel gesendet.

Bitte achten Sie ferner darauf, daß die IP-Adresse des VPN-Gateways nicht im Bereich der Netz-Adresse liegt.

VPN IP-Netzmasken

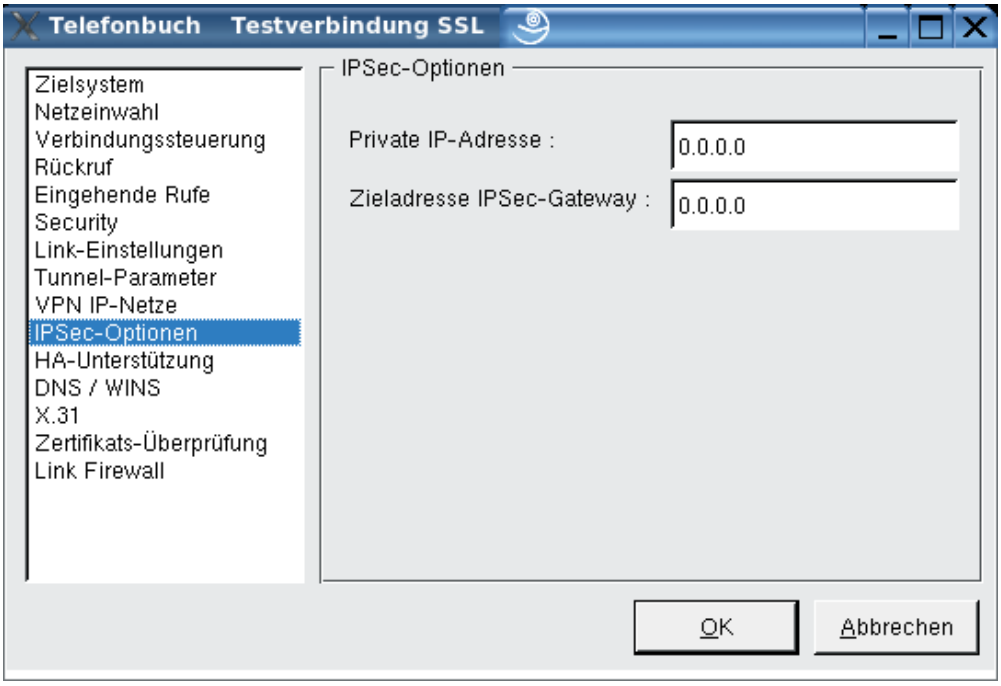
Hier tragen Sie die zugehörige Netzmaske des IP-Netzes ein. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie darauf, daß die IP-Adresse des VPN-Gateways nicht im Bereich der Netz-Adresse liegt.

Auch lokale Netze im Tunnel weiterleiten

Wenn der Datenverkehr des lokalen Netzes über VPN-Tunneling weitergeleitet werden soll, so muss diese Funktion aktiviert werden.

5.1.11 IPSec-Optionen



Die IPSec-Optionen werden benötigt, wenn eine Verbindung von einem NCP Secure Client zu einer nicht NCP-Gegenstelle aufgebaut werden soll.

Parameter:

☐ Private IP-Adresse

☐ Destination IPSec Gateway

Private IP-Adresse

Dies ist die IP-Adresse des Clients, welche im inneren IP-Header des IPSec-Tunnelpaketes als Source Adresse vom Client verwendet wird.

Destination IPSec Gateway

Dies ist die IP-Adresse des IPSec-Gateways der Gegenstelle.

5.1.12 HA-Unterstützung

Dieses Parameterfeld ist nur von Bedeutung, wenn das Zielsystem ein HA-Server (High Availability) ist, der das Tunnelaufkommen je nach Konfiguration an VPN-Gateways weiterleitet. Außerdem erscheint das Parameterfeld nur im Telefonbuch, wenn ein VPN-Protokoll für die Verbindung zum Zielsystem selektiert wurde.

Ein DVE (Dynamic VPN Endpoint) kann zum Lastausgleich (Loadbalancing) oder zur Ausfallsicherung (Backup) eines Virtual Private Networks mit zwei VPN-Gateways genutzt werden. Mit DVE wird, je nach Konfiguration im HA-Manager des Zielsystems, sichergestellt, dass kein Engpass beim Tunnelaufbau auftritt. Je nach Lastaufkommen wird vom HA-Server zum Tunnelaufbau zwischen den Tunnel-Endpunkten der VPN-Gateways gewechselt. (siehe → Beispiele und Erklärungen).

Parameter:

☐ Aktivierung

☐ Erster / Zweiter HA-Server

☐ DVE Secret

☐ Zuletzt zugewiesenes Gateway benutzen

Aktivierung

Mit diesem Parameter wird die DVE-Funktionalität eingechaltet (Dynamic Virtual Endpoint). Im Parameterfeld “Tunnel-Parameter” wird daraufhin die ”Tunnel IP-Adresse (Ziel)” ausgeblendet. Stattdessen muss die IP-Adresse des HA-Servers (→ siehe “Erster / Zweiter HA-Server”) angegeben werden. Dieser HA-Server führt den Tunnel dann je nach Konfiguration weiter an eines der VPN-Gateways.

Erster / Zweiter HA-Server

Hier tragen Sie die IP-Adresse der HA-Server ein. Die Adresse erhalten Sie von Ihrem System-Administrator.

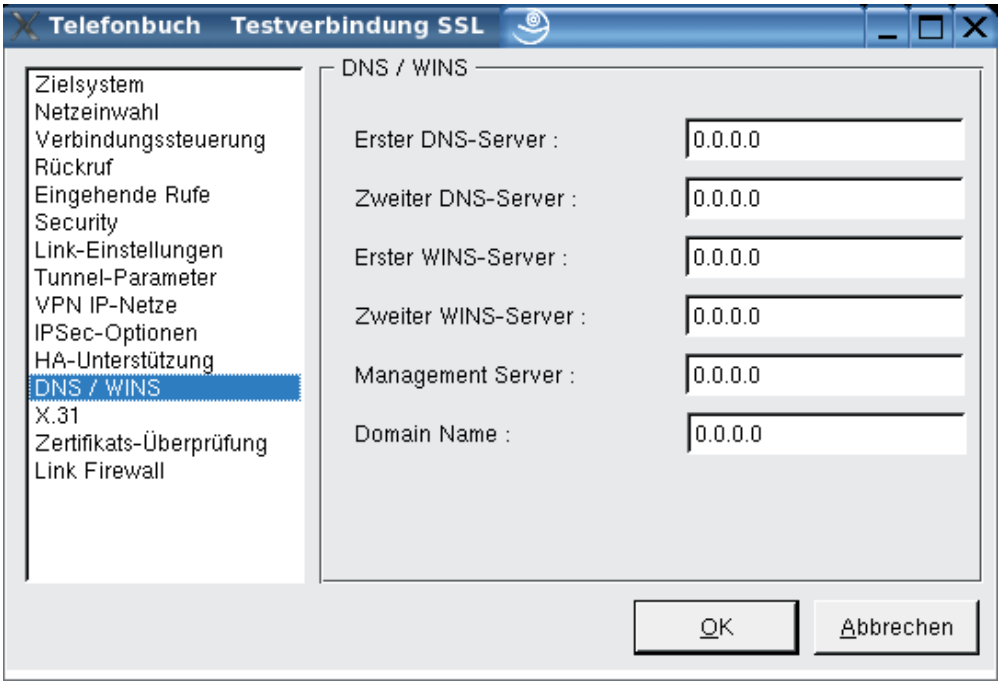
DVE Secret

Hier tragen Sie das Passwort für die Verbindung des DVE-Clients zum Zielsystem (DVE-Server) ein. Sie erhalten es von Ihrem System-Administrator.

Zuletzt zugewiesenes Gateway benutzen

Ist im Gateway die Option “IP-Adressen aus Pool” gewählt und wird ein HA-Server mit Load Balancing verwendet, sollte der Client immer zu dem Gateway verbunden werden, aus dessen IP-Pool er seine IP-Adresse erhalten hat. Um dies zu gewährleisten, aktivieren Sie diese Funktion.

5.1.13 DNS / WINS



In diesem Parameterfenster kann der durch die PPP-Verhandlung automatisch zugewiesene Server durch alternative Server ersetzt werden. Dazu muss in den Netzwerk-Einstellungen des Betriebssystems der DNS-Modus eingestellt sein.

Parameter:

- ☐ DNS-Server
- ☐ WINS-Sever
- ☐ Management Server
- ☐ Domain Name

DNS-Server

erster/zweiter DNS-Server: Der zuerst eingetragene DNS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite DNS-Server dient als Backup-DNS-Server.

WINS-Server

erster/zweiter WINS-Server: Der zuerst eingetragene WINS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite WINS-Server dient als Backup-WINS-Server.

Hinweis: Je nach Anwendung können Sie ein oder zwei DNS- oder WINS-Server eintragen. Genutzt wird immer der jeweils erste. Wird kein alternativer Server eingetragen, wird der Server genutzt, der über PPP zugewiesen wird.

Management Server

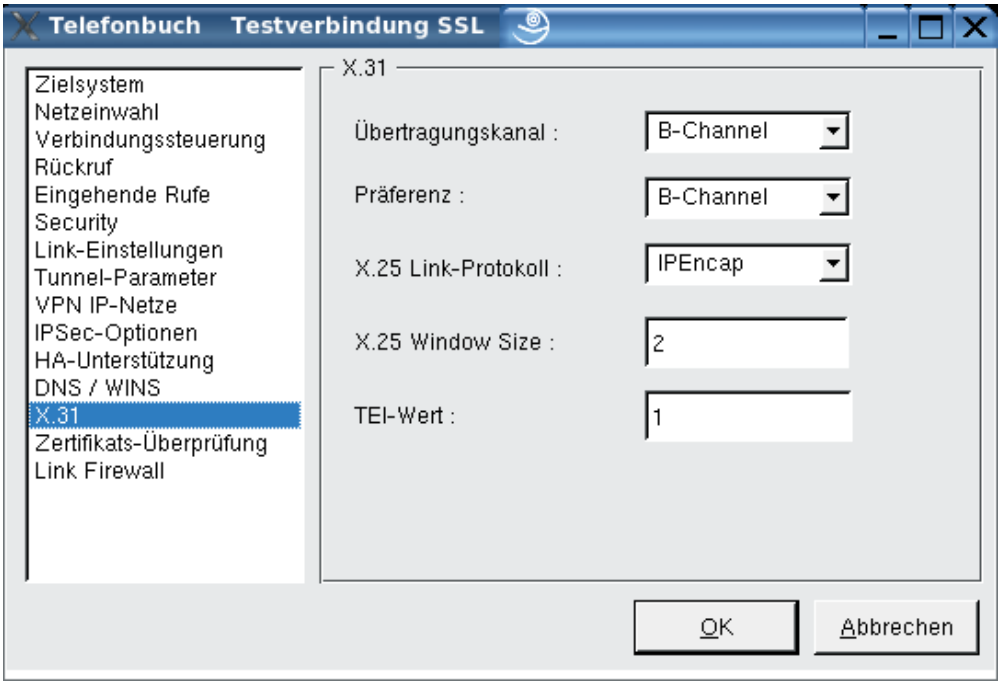
Die IP-Adresse des NCP Management Servers muss hier eingetragen werden, wenn das Gateway der Gegenstelle kein NCP-Gateway ist und somit kein NCP Management-Server automatisch über die PPP-Verhandlung bekannt gegeben werden kann.

Wird die IP-Adresse eines Management Servers eingetragen, obwohl die Gegenstelle ein NCP-Gateway ist, so wird unabhängig von der eingetragenen IP-Adresse der Management-Server des NCP Secure Enterprise Managements genutzt, welcher bei der PPPVerhandlung zwischen NCP-Gateway und NCP Secure Client bekannt gegeben wird. Die eingetragene IP-Adresse wird in diesem Fall ignoriert.

Domain Name

Dies ist der Domain Name der sonst per DHCP dem System in den Netzwerkeinstellungen übergeben wird.

5.1.14 X.31



X.31 ist ein ISDN-Kommunikationsdienst, der auf dem X.25 Protokoll aufsetzt und über den ISDN D-Kanal gehandelt wird. Die maximale Übertragungsrate ist 16 Kbit/s. Der Tarif für X.31 ist wie der für X.25 volumenabhängig. X.31 ist ideal für Dialog-Betrieb mit geringem Datenaufkommen und schnellen Antwortzeiten.

Dieses Parameterfeld erscheint nur, wenn als "verbindungsart" "ISDN" gewählt wurde.

Parameter:

- ☐ Übertragungskanal
- ☐ Präferenz
- ☐ X.25 Link-Protokoll
- ☐ X.25 Window Size
- ☐ TEI-Wert

■ Übertragungskanal

Sie haben hier die Möglichkeit einen von drei Übertragungsmodi zu wählen:

B-Channel (standard) Mit dieser Einstellung verfügen Sie über eine Bandbreite von 64 Kbit/s. Alle Daten werden über den ISDN B-Kanal übertragen

DX25 Diese Einstellung benötigen Sie für X.31 (X.25 im ISDN D-Kanal) und bietet eine Bandbreite von 16 Kbit/s. Alle Daten werden mit X.25-Protokoll über den ISDN D-Kanal übertragen.

Any Mit dieser Einstellung wird je nach Verfügbarkeit sowohl die Übertragung im D-Kanal als auch im B-Kanal unterstützt. Die Voreinstellungen müssen entsprechend gesetzt sein.

Wichtig: Die hier gewählten Übertragungsmodi können nur genutzt werden, wenn der Network Access Server (NAS) des Zielsystems dieselben Modi unterstützt. Die Übertragung im B-Kanal ist für die meisten NAS-Geräte im ISDN der Standard. Die Übertragung im D-Kanal ist nicht in allen Ländern mit einem ISDN möglich, noch wird sie von den meisten NAS-Geräten unterstützt.

■ Präferenz

Dieser Parameter ist nur von Bedeutung, wenn für den Übertragungskanal “ANY” gewählt wurde. Der Client benötigt diesen Parameter, um den bevorzugten Übertragungskanal nutzen zu können. Drei verschiedene Voreinstellungen sind möglich:

B-Channel (standard) Mit dieser Einstellung wählt die Client Software zunächst den B-Kanal bevor sie den D-Kanal als Übertragungskanal probiert.

DX25 Mit dieser Einstellung wählt die Client Software zunächst den D-Kanal bevor sie den B-Kanal als Übertragungskanal probiert.

Any Mit dieser Einstellung wird je nach Verfügbarkeit sowohl die Übertragung im D-Kanal als auch im B-Kanal unterstützt. Beide Übertragungsmodi müssen auch vom Zielsystem unterstützt werden.

Wichtig: Die hier gewählten Übertragungsmodi können nur genutzt werden, wenn der Network Access Server (NAS) des Zielsystems dieselben Modi unterstützt. Die Übertragung im B-Kanal ist für die meisten NAS-Geräte im ISDN der Standard. Die Übertragung im D-Kanal ist nicht in allen Ländern mit einem ISDN möglich, noch wird sie von den meisten NAS-Geräten unterstützt. Das NARAC Enterprise System unterstützt beide Modi.

X.25 Link-Protokoll

Dieser Parameter ist nur von Bedeutung, wenn als Übertragungskanal “DX25" oder ”ANY" gewählt wurde. Die Client Software unterstützt zwei verschiedene X.25 Link Protokolle:

IpEncap	(IP Encapsulation über X.25 RFC konform) Dies ist die Standardeinstellung
PPP	PPP über X.25 RFC konform

Ziehen Sie bei diesem Parameter bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

X.25 Window Size

Dieser Parameter ist nur von Bedeutung, wenn als Übertragungskanal “DX25" oder ”ANY" gewählt wurde. Die X.25 Window Size ist ein Wert, der die mögliche Paketgröße festlegt. Werte von 1 bis 7 sind möglich. Der Standardwert ist “2".

Ziehen Sie bei diesem Parameter bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

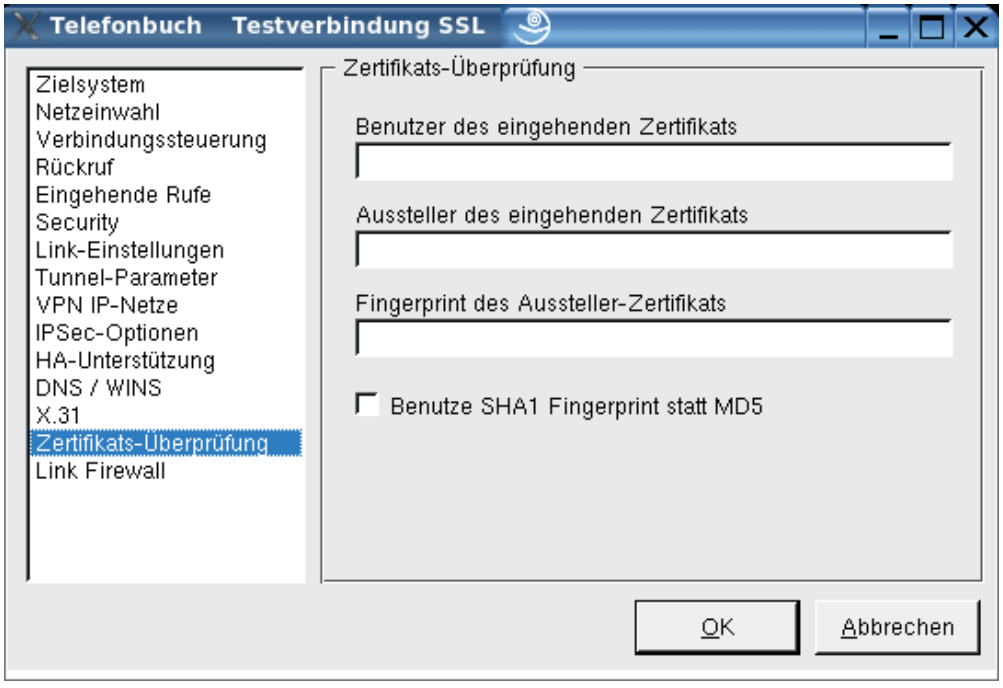
TEI-Wert

Dieser Parameter wird nur in Verbindung mit DX25 (Datenübertragung im D-Kanal) benötigt. Als Übertragungskanal muss “DX25" oder ”ANY" gewählt worden sein.

TEI = Terminal End-Point Identifier.

Der TEI kann Werte von 1 bis 127 annehmen. Standard ist “1".

5.1.15 Zertifikats-Überprüfung



Im Parameterfeld "Zertifikats-Überprüfung" kann pro Zielsystem des Secure Clients vorgegeben werden, welche Einträge in einem Zertifikat der Gegenstelle (Secure Server) vorhanden sein müssen (siehe → Eingehendes Zertifikat anzeigen, Allgemein).

(Siehe auch → Beispiele und Erklärungen, Zertifikats-Überprüfungen)

Parameter:

☐ Benutzer des eingehenden Zertifikats

☐ Aussteller des eingehenden Zertifikats

☐ Fingerprint des Aussteller-Zertifikats

☐ Benutze SHA1 Fingerprint statt MD5

Benutzer des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Benutzers, soweit bekannt - auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu, welche Einträge bei “eingehendes Zertifikat anzeigen” unter Benutzer aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
l      = Location / Stadt, Ort
email  = E-mail
```

Beispiel:

```
cn=VPNGW*, o=NCP, c=de
```

Der Common Name des Security Servers wird hier nur bis zur Wildcard “*” überprüft. Alle nachfolgenden Stellen können beliebig sein, etwa 1 - 5 als Numerierung. Die Organzation Unit muss in diesem Fall immer NCP sein und das Land Deutschland.

Aussteller des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Ausstellers, soweit bekannt - auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu welche Einträge bei “eingehendes Zertifikat anzeigen” unter Aussteller aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
```

```
l      = Location / Stadt, Ort
email  = E-mail
```

Beispiel:

```
cn=NCP engineering GmbH
```

Hier wird nur der Common Name des Ausstellers überprüft.

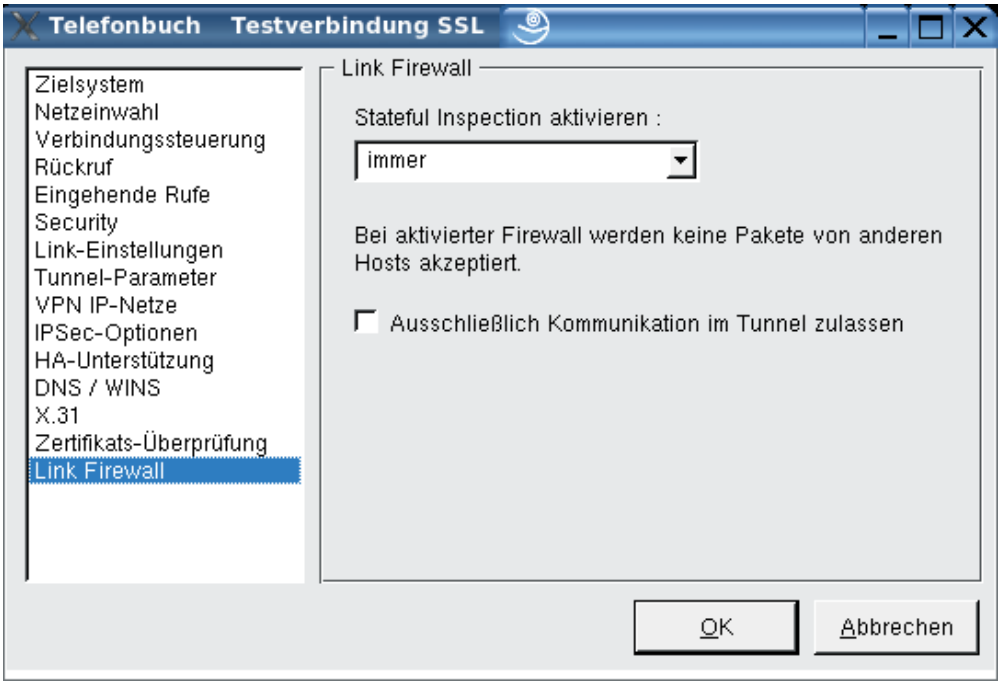
■ Fingerprint des Aussteller-Zertifikats

Um zu verhindern, dass ein Unberechtigter, der die vertrauenswürdige CA imitiert, ein gefälschtes Aussteller-Zertifikat verwenden kann, kann zusätzlich der Fingerprint des Ausstellers, soweit bekannt, eingegeben werden.

■ Benutze SHA1 Fingerprint statt MD5

Der Algorithmus zur Erzeugung des Fingerprints kann MD5 (Message Digit 5) oder SHA1 (Secure Hash Algorithm 1) sein.

5.1.16 Link Firewall



Die Firewall-Einstellungen können für alle Netzwerkadapter wie auch für RAS-Verbindungen genutzt werden. Die aktivierte Firewall wird in der grafischen Oberfläche des Clients als Symbol (Mauer mit Pfeil) dargestellt.

Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ob ein Datenpaket durchgelassen wird oder nicht.

Die hier zu aktivierende Firewall basiert auf dem Paket iptables. Bei Aktivierung der Firewall werden dynamisch Regeln hinzugefügt, sodass nur noch Pakete passieren können, die für die Aufrechterhaltung der VPN-Verbindung nötig sind (verbliebene offene Ports: 1701,/L2TP, 500/IKE, 4500/IKE, ESP Protokoll 50).

Mit Aktivierung der Firewall werden die beiden Scripte ges.st und gdes.sh aktiviert. Sie befinden sich in dem Verzeichnis /etc/ncp/rws/cfg. Sollten bereits Firewall-Scripte auf der Basis von iptables im Einsatz sein, so tragen Sie deren Policies bitte in die oben genannten Scripte ein, da sie ansonsten überschreiben und damit gelöscht werden.

■ Aktivierung (der Firewall)

Bei Aktivierung der Firewall können nur noch Pakete passieren, die für die Aufrechterhaltung der VPN-Verbindung nötig sind. (So ist bei aktivierter Firewall zum Beispiel kein E-Mail-Empfang mehr möglich, wenn dazu nicht die VPN-Verbindung genutzt wird.)

Aktivierung aus: Die Sicherheitsmechanismen der Firewall werden nicht in Anspruch genommen.

Aktivierung immer: Die Sicherheitsmechanismen der Firewall werden immer in Anspruch genommen, d.h. auch wenn keine Verbindung aufgebaut ist, ist der PC vor unberechtigten Zugriffen geschützt.

Aktivierung bei bestehender Verbindung: Der PC ist dann nicht angreifbar, wenn eine Verbindung besteht.

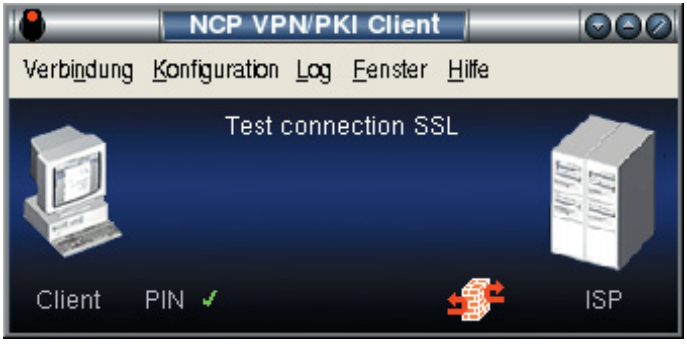


Bild links: Die Firewall ist aktiviert, sodass nur Tunnel-Frames passieren können.

■ Ausschließlich Kommunikation im Tunnel zulassen

Bei aktivierter Firewall kann diese Funktion zusätzlich eingeschaltet werden, um in ein- und ausgehender Richtung ausschließlich VPN-Verbindungen zuzulassen.

.

Frei für Notizen →

© NCP engineering

5.2 IPSec

Die Parameter zu IPSec, einschließlich der zur Konfiguration einer "statischen" Secure Policy Database benötigten, sind in drei Zweige des Konfigurationsbaums unterteilt:

IKE-Richtlinie

IPSec-Richtlinie

SPD Secure Policy Database

Richtlinien | IPSec

Parameterfelder:

1 ***IKE-Richtlinie (Phase-1-Parameter) (5.2.1)***

2 ***IPSec-Richtlinie (Phase-2-Parameter) (5.2.2)***

Die Richtlinien (IKE- / IPSec-Richtlinie) werden in jeder IPSec-Konfiguration benötigt. Das heißt, sie müssen sowohl bei Verwendung einer statischen Secure Policy Database (SPD) als auch bei Verwendung einer dynamischen SPD konfiguriert werden.

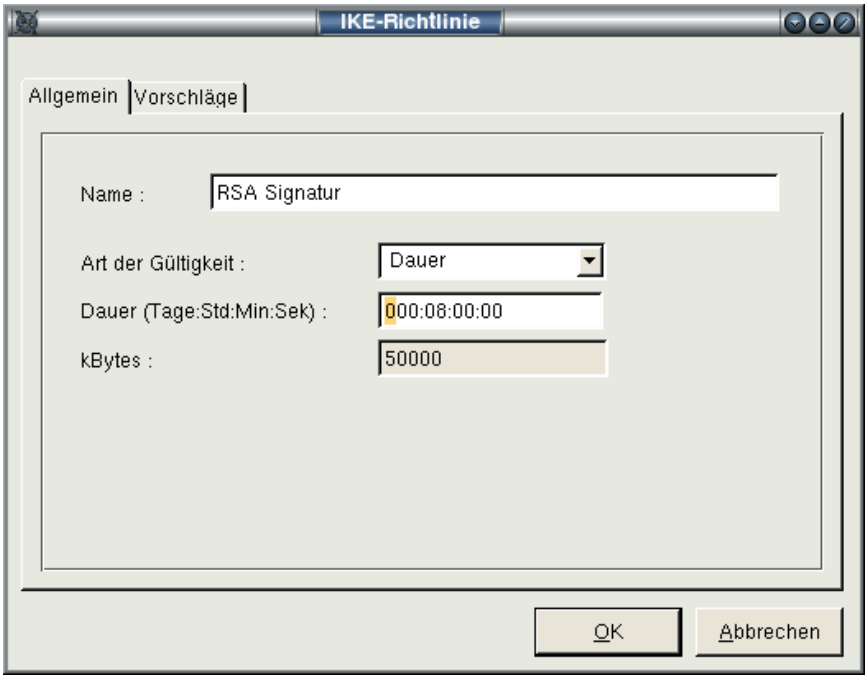
Nach der Maßgabe der IKE-Richtlinie wird die Authentisierungsverhandlung zwischen IPSec-Initiator und Gegenstelle durchgeführt und ein verschlüsselter Kontrollkanal zwischen ihnen hergestellt.

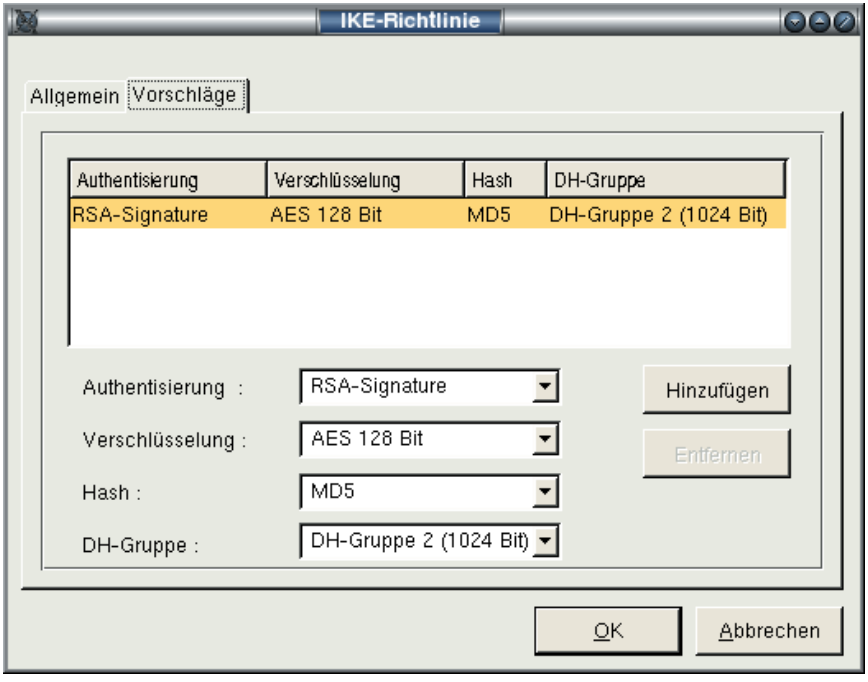
Nach der Maßgabe der IPSec-Richtlinie wird festgelegt, wie die Nutz-Daten gemäß IPSec bearbeitet werden sollen.

Einzelne Parameterfelder oder Parameter, die Sie für Ihre Arbeit mit dem Client nicht benötigen, können von Ihrem Systemadministrator ausgeblendet worden sein.

Bitte beachten Sie zur IPSec-Konfiguration unbedingt die Hinweise im Abschnitt "Beispiele und Erklärungen" unter "Security" in diesem Handbuch.

5.2.1 IKE-Richtlinie (Allgemein / Vorschläge)





Die Parameter in diesen Feldern beziehen sich auf die Phase 1 des Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird (siehe → Beispiele und Erklärungen, IKE-Modi). Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in den Parameterfeldern "Security" im Telefonbuch (für eine dynamische SPD) und unter "Secure Policy Database" (für eine statische SPD.)

Die IKE-Richtlinien, die Sie hier konfigurieren, werden zur Auswahl für die SPD gelistet.

Sofern IPSec für Remote Access eingesetzt wird, ordnen sie eine der IKE-Richtlinien im Parameterfeld "Security" im Telefonbuch für eine dynamisch aufgebaute SPD dem jeweiligen Zielsystem zu.

Die IKE-Richtlinie gilt für eine statische SPD, wenn sie in der Verzweigung der IPSec-Parameter unter "Secure Policy Database" für eine statische SPD im Parameterfeld "Security" selektiert wurde.

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig vorkonfiguriert mit der Software ausgeliefert werden (siehe → Beispiele und Erklärungen, IPSec, IKE-Modi) als "Preshared Key" und "RSA-Signatur".

Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf (siehe → IPSec, IKE-Richtlinie, Authentisierung, Verschlüsselung), d.h. eine Richtlinie kann aus mehreren Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons "Hinzufügen" und "Entfernen" erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Parameter (Allgemein):

☐ Name | IKE-Richtlinie

☐ Art der Gültigkeit | IKE-Richtlinie

☐ Dauer | IKE-Richtlinie

☐ kBytes | IKE-Richtlinie

Parameter (Vorschläge):

☐ Authentisierung |IKE-Richtlinie

☐ Verschlüsselung |IKE-Richtlinie

☐ Hash |IKE-Richtlinie

☐ DH-Gruppe |IKE-Richtlinie

Name | IKE-Richtlinie

Geben Sie dieser Richtlinie einen Namen, über den sie später einer SPD zugeordnet werden kann.

Art der Gültigkeit | IKE-Richtlinie

Bestimmt nach welchen Kriterien die Art der Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach beiden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Dauer | IKE-Richtlinie

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

kBytes | IKE-Richtlinie

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

Authentisierung | IKE-Richtlinie

Bevor der Kontrollkanal für die Phase 1-Verhandlung (IKE Security Association) aufgebaut werden kann, muss beidseitig eine Authentisierung stattgefunden haben.

Werden mehrere Vorschläge mit unterschiedlichen Verschlüsselungen eingetragen, so werden alle Vorschläge der Reihe nach ausgewertet.

Preshared Key = Zur gegenseitigen Authentisierung wird ein (allen) gemeinsamer statischer Schlüssel verwendet. Diesen Schlüssel definieren Sie in den Security-Parameterfeldern (siehe → Telefonbuch, Security bzw. IPSec, Secure Policy Database, Security).

RSA Signature = Zur gegenseitigen Authentisierung wird das Zertifikat verwendet, das Sie für die “Erweiterte Authentisierung” konfiguriert haben (siehe → Verbindung, Benutzer-Zertifikat). Im Main Mode wird das Zertifikat zusätzlich verschlüsselt (siehe → Beispiele und Erklärungen, IKE-Modi). Dies ist nur mit PKI-Unterstützung des Systems möglich (Secure Server).

Verschlüsselung | IKE-Richtlinie

Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal (siehe → Beispiele und Erklärungen, IKE-Modi), sofern der Main Mode (Identity Protection Mode) gefahren wird.

Zur Wahl stehen: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

Hash | IKE-Richtlinie

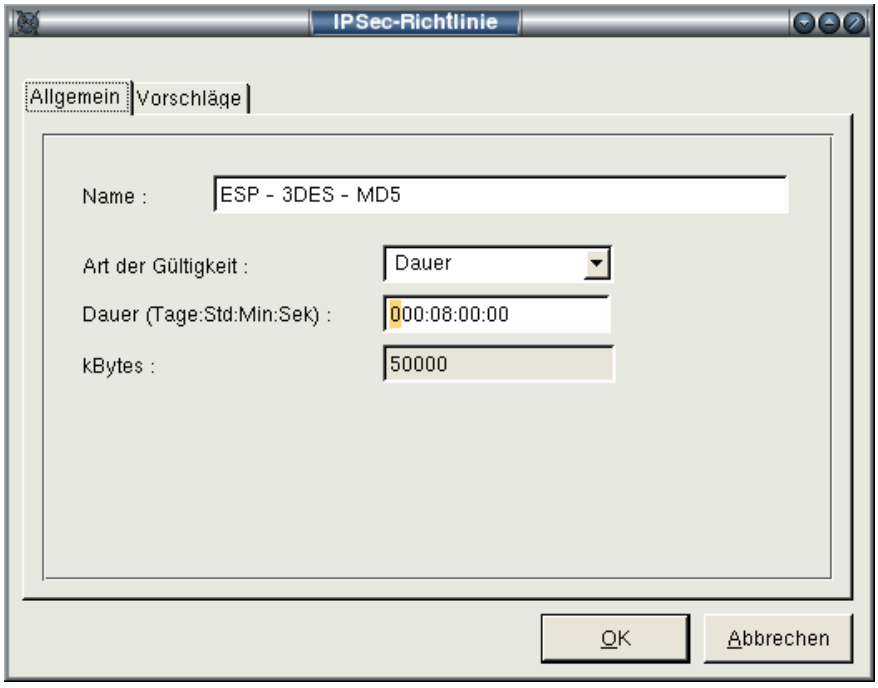
Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird (siehe → Beispiele und Erklärungen, IKE-Modi).

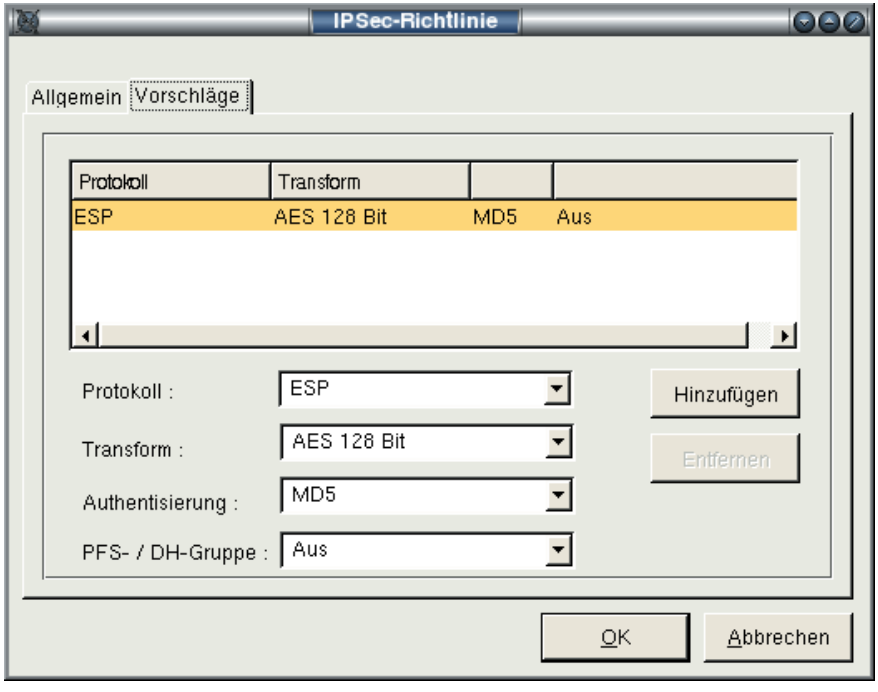
Zur Wahl stehen: MD5 (Message Digest, Version 5) und SHA (Secure Hash Alogrithm).

DH-Gruppe | IKE-Richtlinie

Mit der Wahl einer der angebotenen Diffie-Hellmann-Gruppen wird festgelegt, wie sicher der Key Exchange im Kontrollkanal erfolgen soll, nach dem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH Group desto sicherer ist der Key Exchange.

5.2.2 IPSec-Richtlinie (Allgemein / Vorschläge)





Die IPSec-Richtlinien (Phase-2-Parameter), die Sie hier konfigurieren, werden zur Auswahl für die SPD gelistet.

Sofern IPSec für Remote Access eingesetzt wird, ordnen sie eine der IPSec-Richtlinien im Parameterfeld "Security" im Telefonbuch für eine dynamisch aufgebaute SPD dem jeweiligen Zielsystem zu.

Die IPSec-Richtlinie gilt für eine statische SPD, wenn sie unter den IPSec-Parametern in der Verzweigung "Secure Policy Database" im Parameterfeld "Security" selektiert wurde.

Funktional unterscheiden sich zwei IPSec-Richtlinien nach dem IPSec-Sicherheitsprotokoll AH (Authentication Header) oder ESP (Encapsulating Security Payload). Da der IPSec-Modus mit AH-Sicherung für flexiblen Remote Access völlig ungeeignet ist, wird nur eine IPSec-Richtlinie mit ESP-Protokoll standardmäßig vorkonfiguriert mit der Software ausgeliefert (siehe → Beispiele und Erklärungen, IPSec, AH und ESP).

Inhalt und Name dieser Richtlinie können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPSec-Protokoll und Authentisierung auf, d.h. eine Richtlinie kann aus mehreren Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons "Hinzufügen" und "Entfernen" erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Parameter (Allgemein):

☐ Name |IPSec-Richtlinie

☐ Art der Gültigkeit |IPSec-Richtlinie

☐ Dauer |IPSec-Richtlinie

☐ kBytes |IPSec-Richtlinie

Parameter (Vorschläge):

☐ Protokoll |IPSec-Richtlinie

☐ Transformation (ESP) |IPSec-Richtlinie

☐ Transformation (Comp) |IPSec-Richtlinie

☐ Authentisierung (nur ESP) |IPSec-Richtlinie

☐ DH-Gruppe |IPSec-Richtlinie

Name | IPSec-Richtlinie

Geben Sie dieser Richtlinie einen Namen, über den Sie sie später einer SPD zuordnen können.

Art der Gültigkeit | IPSec-Richtlinie

Bestimmt nach welchen Kriterien die Art der Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach beiden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Dauer | IPSec-Richtlinie

Dauer und kBytes können eigens festgelegt werden.

kBytes | IPSec-Richtlinie

Dauer und kBytes können eigens festgelegt werden.

Protokoll | IPSec-Richtlinie

Die IPSec-Richtlinien sind im Wesentlichen nach den beiden Sicherheitsprotokollen unterschieden, AH oder ESP, die sich im Tunnelmodus gegenseitig ausschließen. Standard ist ESP.

Transformation (ESP) | IPSec-Richtlinie

Wenn das Sicherheitsprotokoll ESP eingestellt wurde, kann hier definiert werden wie mit ESP verschlüsselt werden soll. Zur Wahl stehen die gleichen Verschlüsselungsalgorithmen wie für Layer 2:

DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

Transformation (Comp) | IPSec-Richtlinie

IPSec-Kompression. Die Datenübertragung mit IPSec kann ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache. Nach Selektion des Protokolls “Comp” (Kompression) kann zwischen LZS- und Deflate-Kompression gewählt werden.

Authentisierung (nur ESP) | IPSec-Richtlinie

Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung eigens eingestellt werden.

Zur Wahl stehen: MD5 und SHA.

DH-Gruppe | IPSec-Richtlinie

Mit der Wahl einer der angebotenen Diffie-Hellmann-Gruppen wird festgelegt, dass zusätzlich in Phase 2 mit der SA-Verhandlung ein kompletter Schlüsselaustausch (PFS) stattfinden soll. Standard ist inaktiv.

Secure Policy Database | IPSec

In dieser Verzweigung des Konfigurationsbaums können die statischen SPDs konfiguriert werden. Die Verzweigung ist wie folgt unterteilt.

Parameterfelder:

3 ***Allgemein | SPD (5.2.3)***

4 ***Selektoren | SPD (5.2.4)***

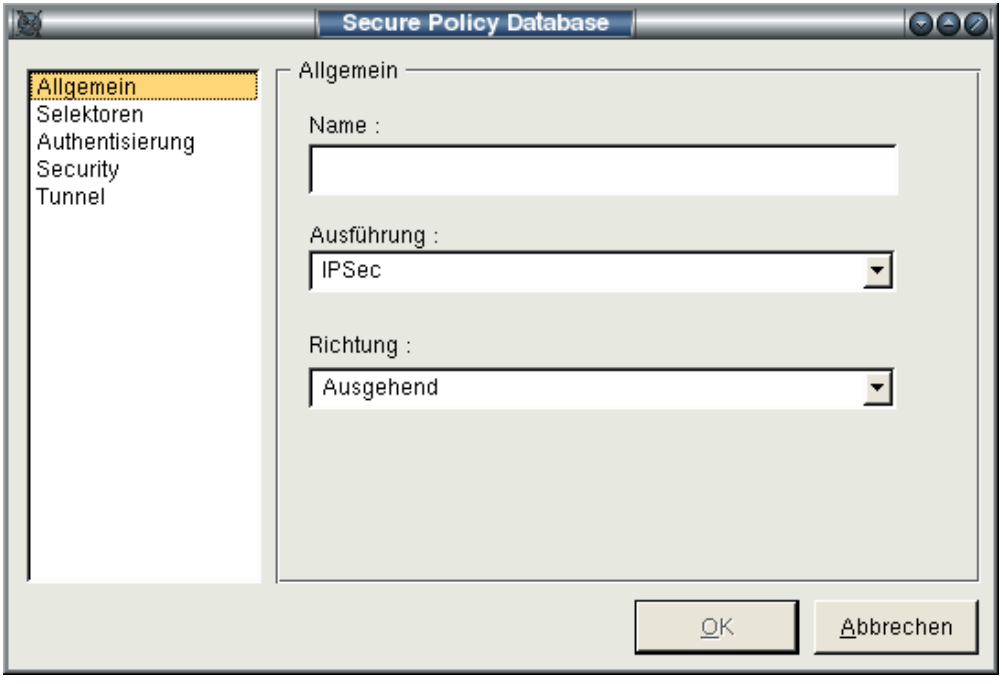
5 ***Authentisierung | SPD (5.2.5)***

6 ***Security | SPD (5.2.6)***

7 ***Tunnel | SPD (5.2.7)***

Bitte beachten Sie zur IPSec-Konfiguration unbedingt die Hinweise im Abschnitt “Beispiele und Erklärungen” unter “Security” in diesem Handbuch.

5.2.3 Allgemein | SPD



In diesem Parameterfeld werden allgemeine Parameter zur Secure Policy Database konfiguriert.

Parameter:

☐ Name |SPD

☐ Ausführung |SPD

☐ Richtung |SPD

Name | SPD

Geben Sie dieser Secure Policy Database einen eindeutigen Namen.

Ausführung | SPD

IPSec (IPSec) → für die IP-Pakete mit Adressen aus dem definierten Bereich werden die IPSec-Sicherheitsdienste angewendet, die SPD-Filtertabelle kommt zum Einsatz

gestatten (permit) → die IP-Pakete mit Adressen aus dem definierten Bereich werden durchgelassen, ohne dass die SPD zum Einsatz kommt

sperren (deny) → alle IP-Pakete mit Adressen aus dem definierten Bereich werden weggeworfen

inaktiv (disabled) → diese SPD wird ausgeschaltet und kommt für IPSec nicht zum Einsatz, ohne dass sie gelöscht werden muss

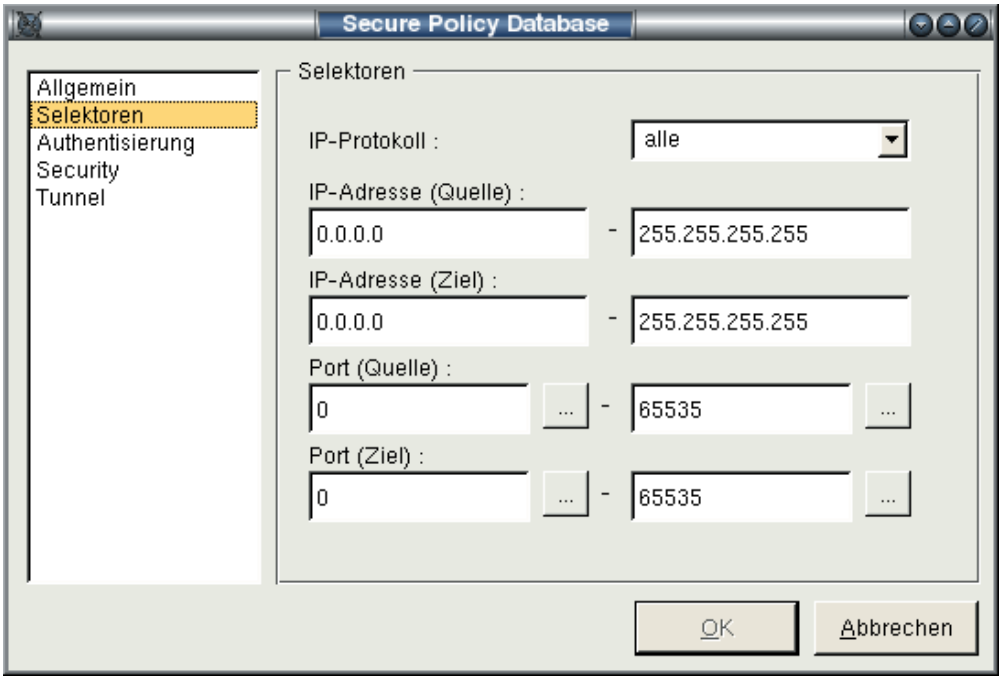
Richtung | SPD

eingehend = Sie stellen auf “eingehend” wenn der Aufbau des Kontrollkanals und die IKE-Verhandlung (siehe → Beispiele und Erklärungen, IKE-Modi) von der Gegenstelle aus eingeleitet wird.

ausgehend = Der Aufbau des Kontrollkanals und die IKE-Verhandlung (siehe → Beispiele und Erklärungen, IKE-Modi) wird von dieser Stelle aus eingeleitet. Auf der Gegenseite muss der Aufbau des Kontrollkanals zugelassen werden, bzw. “eingehend” konfiguriert sein.

Beim Client ist standardmäßig “ausgehend” eingestellt, so dass bei Kommunikation (mit statischer SPD) am Server auf “eingehend” eingestellt werden muss.

5.2.4 Selektoren | SPD



Der Selektor oder Filterteil des SPD-Eintrags besteht aus IP- und Port-Adressen. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird im Status festgelegt, wie mit diesem IP-Paket weiter zu verfahren ist.

Parameter:

☐ IP-Protokoll | SPD

☐ IP-Adresse (Quelle) | SPD

☐ IP-Adresse (Ziel) | SPD

☐ Port (Quelle) | SPD

☐ Port (Ziel) | SPD

- **IP-Protokoll | SPD**

Dies ist das Transportprotokoll (ICMP, TCP oder UDP). Eines der angebotenen Protokolle kann ausgewählt werden oder ein beliebiges (alle / any) wird genutzt.

- **IP-Adresse (Quelle) | SPD**

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Ausgangssysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

- **IP-Adresse (Ziel) | SPD**

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Zielsysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

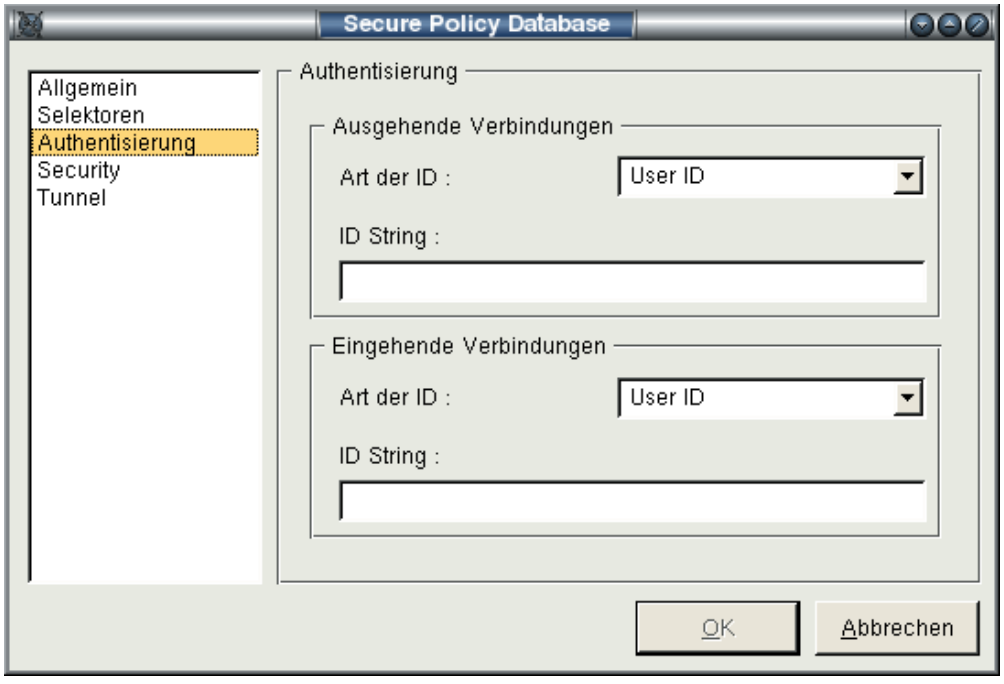
- **Port (Quelle) | SPD**

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

- **Port (Ziel) | SPD**

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton |...].

5.2.5 Authentisierung | SPD



ID, die zum Aufbau des Kontrollkanals (Main Mode Message 5,6 und Aggressive Mode Message 2) benötigt wird (bei statischer SPD).

(Bei dynamischer SPD wird automatisch die gleiche ID verwendet, die auch beim Layer 2-Tunnelaufbau verwendet wird.)

Parameter:

☐ Art der ID (Ausgehende Verbindung / Eingehende Verbindung) | SPD

☐ ID String (Ausgehende Verbindung / Eingehende Verbindung) | SPD

Art der ID (Ausgehende Verbindung / Eingehende Verbindung) | SPD

Bei IPSec wird für eingehende und ausgehende Verbindungen unterschieden.

Was der Sender als ID für ausgehende Verbindung gewählt hat, muss der Empfänger als ID für eingehende Verbindung wählen.

Folgende Arten der ID stehen zur Verfügung:

- ☐ IP Address
- ☐ Domain Name
- ☐ User ID
- ☐ Subnet ID
- ☐ IP Address Range
- ☐ X.500 Distinguished Name
- ☐ X.500 General Name
- ☐ Key ID

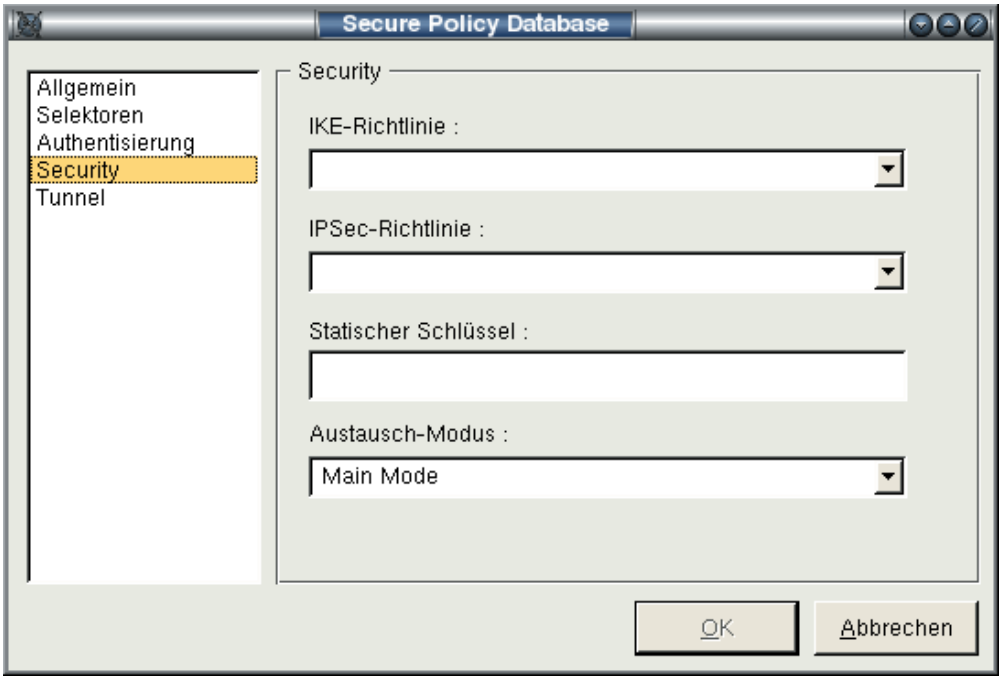
ID String (Ausgehende Verbindung / Eingehende Verbindung) | SPD

Bei IPSec wird für eingehende und ausgehende Verbindungen unterschieden.

Was der Sender als ID für ausgehende Verbindung gewählt hat, muss der Empfänger als ID für eingehende Verbindung wählen.

Je nach gewählter Art der ID, muss in dieses Feld die zugehörige Zeichenfolge bzw. der Adressbereich (mit Minus “-”) eingegeben werden.

5.2.6 Security | SPD



In diesem Feld wählen Sie die vorkonfigurierten Richtlinien aus und setzen die zugehörigen Parameter.

Parameter:

☐ IKE-Richtlinie | SPD

☐ IPSec-Richtlinie | SPD

☐ Statischer Schlüssel | SPD

☐ Austausch-Modus | SPD

IKE-Richtlinie | SPD

Sie wählen aus der Listbox der vorkonfigurierten IKE-Richtlinien diejenige aus, nach der der Kontrollkanal (siehe → IKE-Modi) aufgebaut werden soll.

In der Listbox werden alle IKE-Richtlinien aufgeführt, die Sie im Konfigurationsbaum unter der Verzweigung “IPSec - IKE-Richtlinie” angelegt haben. Die IKE-Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig vorkonfiguriert mit der Software ausgeliefert werden (siehe → Beispiele und Erklärungen, IPSec, IKE-Modi). Sie finden sie im Konfigurationsbaum unter der Verzweigung “IPSec - IKE-Richtlinie” als “Preshared Key” und “RSA-Signatur”.

Die IKE-Richtlinien werden im Konfigurationsbaum unter dem Zweig “IPSec - IKE-Richtlinie” vorkonfiguriert.

IPSec-Richtlinie | SPD

Sie wählen aus der Listbox der vorkonfigurierten IPSec-Richtlinien (siehe → IPSec, IPSec-Richtlinie) diejenige aus, nach der in der Phase 2 die Datenverschlüsselung erfolgen soll.

In der Listbox werden die IPSec-Richtlinien aufgeführt. Sie erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Funktional unterscheiden sich zwei IPSec-Richtlinien nach dem IPSec-Sicherheitsprotokoll AH (Authentication Header) oder ESP (Encapsulating Security Payload). Da der IPSec-Modus mit AH-Sicherung für flexiblen Remote Access völlig ungeeignet ist, wird nur eine IPSec-Richtlinie mit ESP-Protokoll standardmäßig vorkonfiguriert mit der Software ausgeliefert (siehe → Beispiele und Erklärungen, IPSec, AH und ESP).

Die IPSec-Richtlinien werden im Konfigurationsbaum unter dem Zweig “IPSec - IPSec-Richtlinie” vorkonfiguriert.

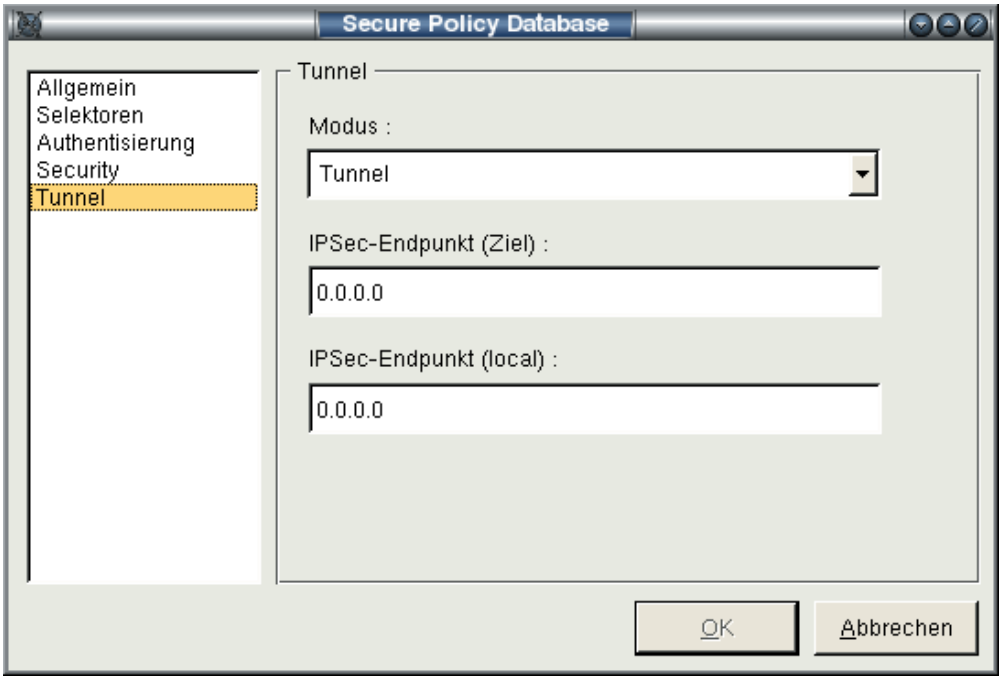
Statischer Schlüssel | SPD

Ein statischer Schlüssel kann zur Authentisierung in der IKE-Verhandlung verwendet werden (siehe → IKE-Richtlinie, Authentisierung, Preshared Key). An beiden Endpunkten der Kommunikation muss der gleiche statische Schlüssel verwendet werden. (Der statische Schlüssel für eine dynamische SPD wird unter “Telefonbuch, Security, Statischer Schlüssel” eingegeben.)

Austausch-Modus | SPD

Der Internet Key Exchange kann in zwei unterschiedlichen Modi ausgeführt werden, dem Main Mode, auch Identity Protection Mode, oder dem Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch die Verschlüsselung (siehe → Beispiele und Erklärungen, IKE-Modi).

5.2.7 Tunnel | SPD



In diesem Parameterfeld werden die Betriebsart und die IP-Adressen der Endpunkte der IP-Sec-Kommunikation festgelegt.

Parameter:

☐ Modus | SPD

☐ IPSec-Endpunkt (Ziel) | SPD

☐ IPSec-Endpunkt (lokal) | SPD

■ Modus | SPD

Hier bestimmen Sie den IPSec-Betriebsmodus (siehe auch → Erklärungen und Beispiele, AH und ESP im Transport- und Tunnelmodus).

Transport	=	Der Transportmodus eignet sich nur für eine direkte Kommunikation zwischen zwei Hosts mit festen IP-Adressen oder zwischen Arbeitsplatzrechnern im LAN. (Dieser Modus ist für Remote Access ungeeignet.)
Tunnel	=	Im Tunnelmodus wird das gesamte IP-Paket mit einem neuen IP Header versehen. Das IP-Paket wird auf diese Weise durch einen Layer 3-Tunnel geschickt. Der innere IP Header mit Original-Adressen ist dabei versteckt und kann nicht eingesehen werden - nur die (Layer 3-) Tunnelendpunkte sind erkennbar. Rechner in Netzen hinter Firewalls oder Routern mit IPSec können in diesem Modus sicher miteinander kommunizieren.

■ IPSec-Endpunkt (Ziel) | SPD

Hier geben Sie die IP-Adresse des Endpunkts der IPSec-Kommunikation ein. Der “IPSec-Endpunkt (Ziel)” muss der lokalen IP-Adresse der Gegenstelle entsprechen und umgekehrt.

■ IPSec-Endpunkt (lokal) | SPD

Hier geben Sie die IP-Adresse des Endpunkts der IPSec-Kommunikation ein. Der “IPSec-Endpunkt (Ziel)” muss der lokalen IP-Adresse der Gegenstelle entsprechen und umgekehrt.

Frei für Notizen →

6. Eine Verbindung herstellen

■ Verbindungsaufbau zum Zielsystem

Die Client Software gestattet die Definition verschiedenster Zielsysteme, die je nach Anforderung benannt und konfiguriert werden können.

Um ein Zielsystem zu definieren, klicken Sie in der Menüleiste auf “Konfigurieren – Telefonbuch“. Das Fenster des Telefonbuchs öffnet sich nun und zeigt die bereits definierten Ziele.

Sobald die Software installiert und die Zielparameter korrekt konfiguriert wurden, kann die Anwahl an das Zielsystem stattfinden. Dabei ist auch die Art der Anwahl Bestandteil der Konfiguration eines Zielsystems. Sie können aus drei Anwahl-Modi für den Verbindungsaufbeu wählen: automatisch, manuell und wechselnd. Sie definieren den Modus des Verbindungsaufbaus für ein Zielsystem im Telefonbuch unter (→) “Verbindungssteuerung – Verbindungsaufbau”.

Automatischer Verbindungsaufbau:

Im Unterschied zu Microsoft RAS, bei dem jedes Ziel manuell angewählt werden muss, arbeitet die Client Software nach dem Prinzip der LAN-Emulation. Dabei ist es lediglich erforderlich, die entsprechende Applikations-Software zu starten (Email, Internet Browser, Terminal Emulation, etc.). Die Verbindung wird dann, entsprechend den Parametern des Zielsystems, automatisch aufgebaut und gehalten.

Manueller Verbindungsaufbau:

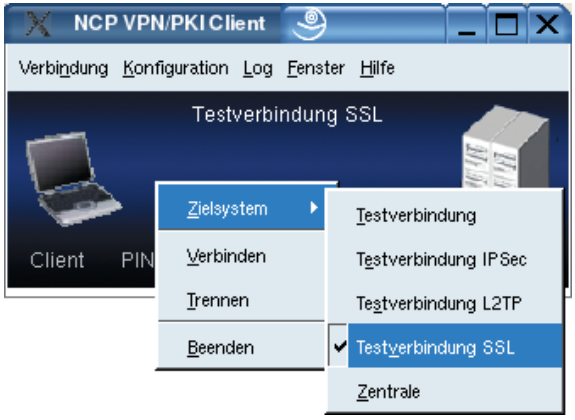
Daneben ist es auch möglich manuell die Verbindung zu einem ausgewählten Ziel herzustellen, indem Sie im Monitor “Verbindung” anklicken und “Verbinden” wählen.

Wechselnder Verbindungsaufbau:

Wird dieser Modus gewählt, muss zunächst die Verbindung “manuell” aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau wie folgt:
– Wird die Verbindung mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung “automatisch” hergestellt,
– wird die Verbindung “manuell” abgebaut, muss sie auch wieder “manuell” aufgebaut werden.

■ Verbinden

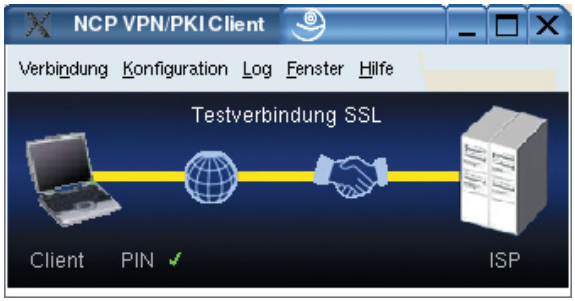
Gleich wie die Verbindung aufgebaut wird, der Monitor, sofern er im Vordergrund sichtbar ist, zeigt immer den Status des Verbindungsaufbaus wie in folgendem Beispiel an:



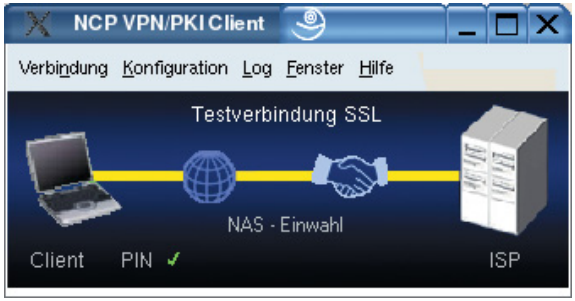
Zunächst wird das Zielsystem ausgewählt – hier über das Menü, das nach einem rechten Mausklick erscheint.

Danach wird die Verbindung hergestellt – hier manuell über das Menü, das nach dem rechten Mausklick erscheint.

Wurde die Verwendung eines (Soft-)Zertifikats konfiguriert – wie bei der Testverbindung mit SSL – so muss zunächst die PIN eingegeben werden.



Anschließend wird eine Verbindung zum Internet Service Provider (ISP) hergestellt (gelbe Linie). Die Einwahl dorthin wird nun mit einem Globus, die Authentisierung beim ISP als Händeschütteln dargestellt. Dabei wechseln die Farben der Symbole je nach aktuellem Status:

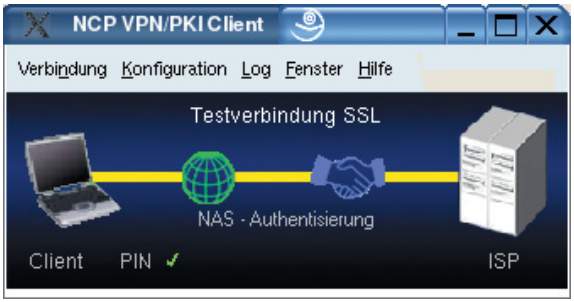


hellblau = Station des Verbindungsaufbaus

dunkelblau = Station wird gerade durchlaufen

grün = Station erfolgreich durchlaufen

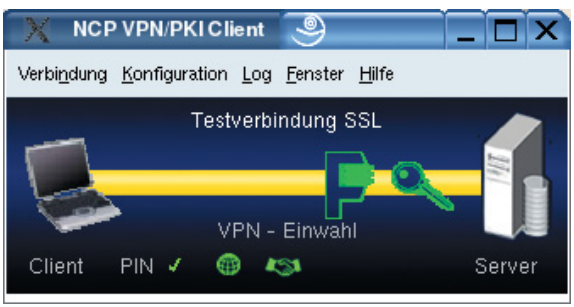
© NCP engineering GmbH



Die erfolgreich durchlaufenen Stationen werden als verkleinerte Symbole dargestellt.

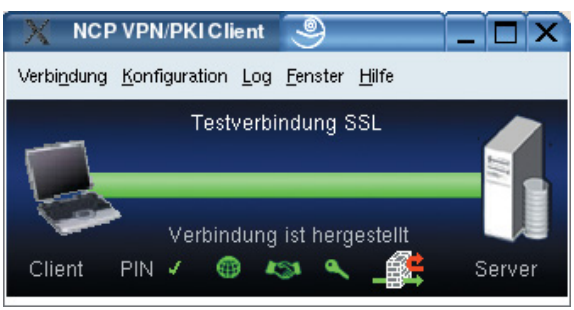
Nach der Verbindung zum ISP (grüne Linie) und der Authentisierung am Network Access Server (grünes Händeschütteln) ...

... wird der Tunnel aufgebaut (gelbe, dicke Linie) und die Einwahl am VPN Gateway beginnt. Auch hier muss eine Authentisierung stattfinden. Zusätzlich ist bei der SSL-Testverbindung aber noch eine Verschlüsselung (Schlüssel) konfiguriert.



Wenn die Konfiguration der Gegenstelle darauf eingestellt ist, kann auch Kompression konfiguriert werden.

Ist die letzte Station des Verbindungsaufbaus (hier die Verschlüsselung, bzw. Entschlüsselung) durchlaufen, schaltet das Ampellicht auf grün ...



... wie auch anschließend die Tunnelverbindung. Die Verbindung ist damit hergestellt!

Passwörter und Benutzernamen

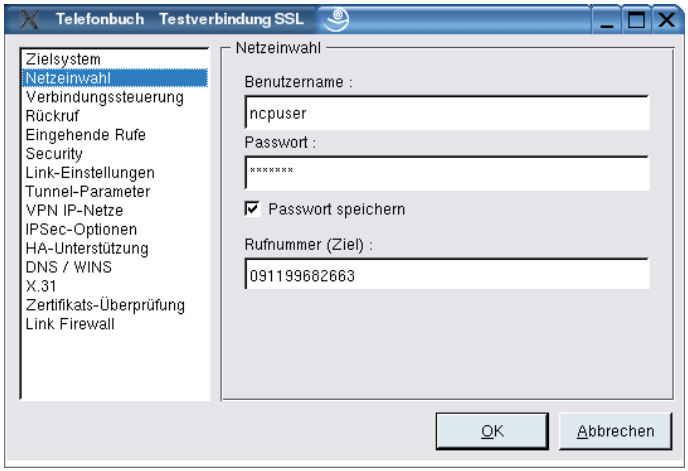
Das Passwort (siehe → Netzeinwahl, Passwort) benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 256 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Auch wenn Sie für den Verbindungsaufbau “automatisch“ gewählt haben (siehe oben → Verbindungsaufbau zum Zielsystem), müssen Sie die Verbindung beim ersten Mal manuell aufbauen und das Passwort eingeben. Für jeden weiteren automatischen Verbindungsaufbau wird das Passwort selbständig übernommen, bis der PC erneut gebootet oder das Zielsystem gewechselt wird. D.h. für eine Reihe von “automatischen” Verbindungsaufbaus wird das Passwort nach der ersten Eingabe und dem ersten Verbindungsaufbau selbständig übernommen, auch wenn die Funktion “Passwort speichern” (siehe → Netzeinwahl) nicht aktiviert wurde. Erst ein Boot-Vorgang löscht das einmal eingegebene Passwort. (Beachten Sie zu Windows auch → Logon Optionen).

Soll das Passwort mit dem Booten nicht gelöscht werden, so muss die Funktion “Passwort speichern” aktiviert werden (siehe → Netzeinwahl). Bitte beachten Sie dabei, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

Benutzername für NAS-Einwahl



Der “Benutzername” für die Netzeinwahl muss immer in der Konfiguration für das Ziel eingegeben werden. Ohne diesen Benutzernamen kann keine Einwahl an den NAS erfolgen.
(Siehe → Netzeinwahl)

Benutzername und Passwort für VPN-Einwahl

Benutzernamen und Passwörter für die Einwahl zum VPN Gateway (siehe → Tunnel-Parameter) können in der Konfiguration des Zielsystems vollständig eingegeben werden. Sie bleiben über einen Boot-Vorgang hinaus für die VPN-Einwahl erhalten. Werden sie nicht eingegeben, so werden sie bei der VPN-Einwahl in einem Dialog abgefragt.

Passwort für OTP-Token

Ein Einmal-Passwort, sofern ein OTP-Token verwendet wird (siehe → Verbindungssteuerung), sowie die zugehörige PIN werden immer abgefragt. Je nachdem ob das OTP-Token für die NAS- oder die VPN-Einwahl verwendet wird, erscheint der entsprechende Dialog.

Verbindungsabruch und Fehler

Ereignet sich ein Fehler, so wird die Verbindung nicht hergestellt und die Fehlerursache im Monitor angezeigt (beachten Sie dazu den Abschnitt “Fehler- und ISDN-Meldungen”).

Trennen

Mit der Funktion “Trennen“ wird der Abbau der aktuell bestehenden Verbindung manuell durchgeführt. Wenn Sie die Möglichkeit behalten wollen, jederzeit die Verbindung manuell abbauen zu können, setzen Sie den Verbindungsaufbau auf “manuell” und deaktivieren den automatischen Timeout, indem Sie ihn auf Null (0) setzen (→ Verbindungsaufbau).

Wenn die Verbindung abgebaut wird, wechselt die farbliche Darstellung der Verbindungslinie bis sie verschwindet.

© NCP engineering GmbH

7. Beispiele und Erklärungen

In diesem Abschnitt des Handbuchs werden einige wesentliche Grundbegriffe des Routings erklärt. Anhand von Beispielen wird die Konfiguration des Secure Clients für bestimmte Funktionalitäten dargestellt.

7.1 IP-Funktionen

Um ein IP-Netzwerk korrekt zu konfigurieren, müssen die Regeln der IP-Adressierung eingehalten werden. Untenstehend sind einige Richtlinien und Terminologien aufgeführt. Zu weiteren Informationen über IP-Netzwerke wird entsprechende Fachliteratur empfohlen.

7.1.1 Geräte eines IP-Netzwerks

IP-Adressen werden den Schnittstellen der Geräte eines IP-Netzwerks zugewiesen. Diese Geräte werden auch als Hosts oder Rechner bezeichnet. Mehrfach vernetzten Geräten (z.B. Router) können auch mehrere Adressen zugeordnet werden. Der Begriff Host-Adresse bezeichnet die IP-Adresse des Rechners eines IP-Prozesses, unabhängig von der tatsächlichen physikalischen Struktur des Geräts oder der Schnittstellen.

7.1.2 IP-Adress-Struktur

IP-Adressen haben eine Länge von vier Oktetten, 32 Bits (4 Bytes), und werden in dezimaler oder hexadezimaler Schreibweise mit Punkt "." getrennt notiert. Zum Beispiel:

```
198.10.6.27 oder
C6.0A.06.1B oder
0xC6.0x0A.0x06.0x1B
```

Die Adressen werden getrennt in einen Netzwerk-Abschnitt, der das zugehörige Netz adressiert, und eine lokale Adresse, dem sogenannten "Restfeld" (auch Host-Abschnitt), der das jeweilige Gerät innerhalb des Netzwerks adressiert. Alle Geräte innerhalb eines einzelnen Netzwerks haben denselben Netzwerk-Abschnitt gemeinsam. Jedes Gerät (Host) hat dabei sein eigenes Restfeld.

Es gibt drei Klassen von Internet-Adressen, je nachdem wieviele Bytes der IP-Adresse für Netzwerk-Abschnitt und Restfeld verwendet werden.

Klasse (Class) A, große Netzwerke: Netzwerknummern 1 - 127

Bei Adressen der Klasse A ist das höchste Bit gleich Null, die nächsten sieben Bits entsprechen dem Netzwerk und die verbleibenden 24 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 1 Byte (max. 126 unterschiedliche Netzwerke)

Restfeld beansprucht 3 Bytes (max. 2 hoch 24 = 16.777.216 verschiedene Geräte)

Damit können max. 127 unterschiedliche Netzwerke, jedes mit max. 16.777.216 verschiedenen Geräten, adressiert werden.

Klasse (Class) B, mittlere Netzwerke: Netzwerknummern 128 - 191

Bei Adressen der Klasse B haben die beiden höchsten Bits die Werte 1 und 0, die nächsten 14 Bits entsprechen dem Netzwerk und die verbleibenden 16 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 2 Byte (max. 16.384 unterschiedliche Netzwerke)

Restfeld beansprucht 2 Bytes (max. 2 hoch 16 = 65.536 verschiedene Geräte)

Damit können max. 16.384 unterschiedliche Netzwerke, jedes mit max. 65.526 verschiedenen Geräten, adressiert werden.

Klasse (Class) C, kleine Netzwerke: Netzwerknummern 192 - 223

Bei Adressen der Klasse C haben die drei höchsten Bits die Werte 1, 1 und 0, die folgenden 21 Bits entsprechen dem Netzwerk und die letzten 8 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 3 Bytes (max. 2.097.152 unterschiedliche Netzwerke)

Restfeld beansprucht 1 Byte (max. 256 verschiedene Geräte)

Damit können max. 2.097.152 unterschiedliche Netzwerke, jedes mit max. 256 verschiedenen Geräten, adressiert werden.

Beispiel:

```
           Netz    Host
Klasse A: 122. | 087.    156.    045
Klasse B: 162.   143. | 085.    132
Klasse C: 195.   076.   212. | 024
```

Bitte beachten Sie bei der Adressvergabe, dass für einen einzelnen physikalischen Rechner mehrere IP-Adressen verwendbar sein müssen. Eine Workstation kann mit einer IP-Adresse auskommen. Ein Router benötigt für jede seiner Schnittstellen eine IP-Adresse, mindestens jedoch zwei – eine für den Anschluss zum lokalen Netz (LAN IP-Adresse), eine für den Anschluss zur WAN-Seite.

7.1.3 Netzmasken (Subnet Masks)

In einem Wide Area Network können verschiedene, physikalisch getrennte Netze (LANs) dem gleichen Netzwerk (WAN) mit der gleichen Netzwerknummer angehören. Anhand dieser Netzwerknummer allein kann kein Router entscheiden, ob er bei einer IP-Kommunikation eine Verbindung zu einem physikalisch anderen Netz innerhalb des WANs aufbauen soll. Das Netzwerk (WAN) muss daher in kleinere Abschnitte (LANs) unterteilt werden, die einen eigenen Adressblock erhalten. Jeder Adressblock der einzelnen physikalischen Netze wird als Subnet bezeichnet. Durch diese Unterteilung eines Netzwerks in Subnets wird die Hierarchie aus Netzwerk und Rechner zu einer Hierarchie erweitert aus Netzwerk, Subnet und Rechner.

Diese erweiterte Hierarchie erleichtert zum einen das Auffinden eines Rechners im Gesamtnetz (WAN). Man kann sich dies vorstellen analog zur Nomenklatur im Telefonnetz, wo zum Beispiel die Ortsvorwahl aussagt in welchem Bereich sich ein Anschluss befindet. Diese Hierarchie gewährt auch eine gewisse Zugriffssicherheit. So kann in einem Firmennetz zum Beispiel der Rechner eines Subnets nicht ohne weiteres auf Ressourcen eines anderen Subnets zugreifen – etwa ein Mitarbeiter aus der Fertigungsabteilung auf Datenbestände aus der Personalabteilung – wenn die Netz-Masken nach Firmenabteilungen entsprechend gewählt sind.

Die Netz-Maske (Subnet Mask) gibt den Standort des Subnet-Felds in einer IP-Adresse an. Die Netz-Maske ist eine binäre 32-Bit-Zahl wie eine IP-Adresse. Sie hat eine “1” an allen Stellen des Netzwerk-Abschnitts der IP-Adresse (je nach Netzwerk-Klasse innerhalb des ersten bis dritten Oktetts). Das darauf folgende Oktett gibt die Position des Subnet-Feldes an. Die im Subnet-Feld an den Netzwerk-Abschnitt aufschließenden Einsen geben die Subnet-Bits an. Alle übrigen Stellen mit ”0” verbleiben für den Host-Abschnitt.

■ Beispiele

Beispiel 1:

Die Netzmaske dient der Interpretation der IP-Adresse. So kann eine Adresse 135.96.7.230 mit der Maske 255.255.255.0 so interpretiert werden: Das Netzwerk hat die Adresse 135.96.0.0, das Subnet hat die Nummer 7, der Rechner Nummer 230. Eine IP-Adresse mit 135.96.4.190 gehört dem gleichen Netzwerk aber einem anderen Subnet (4) an.

Binäre Darstellung:

```
135.96.7.230     = 10000111 11000000 | 00000111 | 11100110
135.96.4.190     = 10100000 10010101 | 00000100 | 10111110
255.255.255.0    = 11111111 11111111 | 11111111 | 00000000
                   Netzwerk          | Subnet   |
255.255.248.0    = 11111111 11111111 | 11111|000  00000000
```

Hätte die Netz-Maske in obigem Beispiel nicht den Standardwert 255.255.255.0, sondern 255.255.248.0, befänden sich die IP-Adressen im gleichen Subnet – und Routing würde nicht stattfinden.

Beispiel 2:

Zwei IP-Adressen mit 160.149.115.8 und 160.149.117.201 und der Netz-Maske 255.255.252.0 befinden sich im gleichen Netzwerk 160.149, gehören aber unterschiedlichen Subnets an.

Binäre Darstellung:

```
160.149.115.8    = 10100000 10010101 | 011100|11 00001000
160.149.117.201  = 10100000 10010101 | 011101|01 11001001
255.255.252.0    = 11111111 11111111 | 111111|00 00000000
                     Netzwerk        | Subnet|
```

Die Wahl einer geeigneten Netzmaske hängt von der Netzwerk-Klasse, der Beschaffenheit der möglichen Subnets, ihrer Anzahl und ihrem Wachstum ab. Ziehen Sie zur Planung einschlägige Tabellen oder einen Subnet-Taschenrechner zu Rate.

Subnet-Tabelle Klasse C:

Subnet-Bits	Host-Bits	Netz-Maske	Subnets	Rechner
2	6	255.255.255.192	2	62
3	5	255.255.255.224	6	30
4	4	255.255.255.240	14	14
5	3	255.255.255.248	30	6
6	2	255.255.255.252	62	2

(Berechnung: 2 hoch n minus 2 = Anzahl der Subnets/Rechner
n: Anzahl der Subnet/Host-Bits)

Mit einer Netz-Maske 255.255.255.240 wird ein Netz der Klasse C in Subnets geteilt. Mit dieser Netz-Maske sind insgesamt 14 Subnets mit jeweils max. 14 Rechnern möglich.

```
255.255.255.240  11111111 11111111 11111111 | 1111 | 0000
199.  9. 99.130  11000111 00001001 01100011 | 1000 | 0010  Subnet-Nummer 8
199.  9. 99.146  11000111 00001001 01100011 | 1001 | 0010  Subnet-Nummer 9
                 Netzwerk                   |Subnet| Host
```

■ Standard-Masken

Netzmaske für Klasse A: 255. 0. 0. 0

Netzmaske für Klasse B: 255. 255. 0. 0

Netzmaske für Klasse C: 255. 255. 255. 0

Reservierte Adressen

Einige IP-Adressen dürfen Geräten eines Netzwerks nicht zugeordnet werden. Dazu gehören die Netzwerk- oder Subnet-Adresse und die Rundsendungsadresse für Netzwerke bzw. Subnets. Netzwerk-Adressen bestehen aus der Netzwerknummer und dem Host-Feld, das mit binären Nullen gefüllt ist (z.B. 200.1.2.0, 162.66.0.0., 10.0.0.0) – auch Loop Back, es findet keine Übertragung ins Netzwerk statt. Die Rundsendungsadresse eines Netzwerks besteht aus der Netzwerknummer und dem Host-Feld mit binären Einsen (z.B. 200.1.2.255, 162.66.255.255., 10.255.255.255) – daher auch "All One Broadcast", alle Stationen eines Netzwerks werden adressiert.

Beispiel:

198.10.2.255	adressiert alle Stationen im Netz 198.10.2.
255.255.255.255	adressiert alle Stationen in allen angeschlossenen Netzen
0.0.0.0	All Zero Broadcast: Ungültige Adresse.

Bitte beachten Sie, dass diese Adresse oft für Standard-Einstellungen benutzt wird.

7.1.4 Zum Umgang mit IP-Adressen

- ☐ Jede IP-Adresse im unternehmensweiten Netz sollte nur einmalig vorhanden sein. Beachten Sie dies bei Internet-Anschluss und Anschluss neuer Netze.
- ☐ Benutzen Sie ein nachvollziehbar logisches Schema bei der Adress-Vergabe, z.B. Verwaltungseinheiten, Gebäude, Abteilungen etc.
- ☐ Für den Anschluss ans Internet benötigen Sie eine offizielle einmalige Internet-Adresse.
- ☐ Vergeben Sie, wenn möglich, keine IP-Adresse, deren Netzwerk- oder Host-Abschnitt mit "0" endet. Dies könnte zu Fehlinterpretationen und undefinierbaren Fehlern im Netz führen.
- ☐ Netzmasken werden vom Internet-Protokoll nur ausgewertet, wenn die Netzwerknummern der Kommunikationspartner gleich sind.
- ☐ Wie die Adress-Klassen haben auch die Netz-Masken unterschiedlich lange Netzwerk-Abschnitte.

7.2 Security

Dieser Abschnitt beschreibt die Besonderheiten der Security-Verfahren L2Sec und IPSec und dient der grundlegenden Erläuterung der Konfigurationsparameter zu diesen beiden Verfahren.

Im Parameterfeld “Security” des Telefonbuchs sind die Konfigurationsparameter zu L2Sec und IPSec für den Einsatz in Remote Access-Umgebungen gesammelt. Sofern IPSec für Remote Access eingesetzt wird, wird die Secure Policy Database (SPD) dynamisch nach Vorgabe der Parameter im Feld “Security” aufgebaut (siehe unten → IPSec für Remote Access, IPSec over L2TP). In diesem Fall wird eine statische SPD-Konfiguration nicht benötigt!

Bei ausgehendem IP-Verkehr mit IPSec werden vom Secure Client zuerst die statischen SPDs abgearbeitet, die im Konfigurationsbaum im Zweig “IPSec” unter der Rubrik “Secure Policy Database” angelegt wurden. Nur wenn keine dieser statischen SPDs zum Einsatz kommt, wird eine dynamische SPD aufgebaut.

Statische SPDs werden nur für IP-Verbindungen zu anderen Access Servern benötigt, die nicht L2Sec unterstützen. Ansonsten kann ihr Status auf “inaktiv” gesetzt werden (siehe unten → Sicherheits-Richtlinien von IPSec).

7.2.1 Verschlüsselungsart L2Sec nach RFC 2716

Die Praxis zeigt, dass es in VPN-Projekten gilt, einerseits eine sehr große Anzahl von verteilten PC-Arbeitsplätzen an die Firmenzentrale anzubinden und andererseits neben IP- auch IPX-, SNA- und NetBios-Datenpakete (native) zu übertragen sind.

Wichtig für die Sicherheit einzurichtender Kommunikationsnetze ist in besonderem Maße eine angemessene Authentisierung der Kommunikationsteilnehmer – bereits während des Verbindungsaufbaus. Dies ist umso vorrangiger, je mehr sich Mitarbeiter vom Telearbeitsplatz oder vom mobilen Büro über das Internet oder andere öffentliche Netze in das Datennetz des Unternehmens einwählen.

Ohne Zweifel hat IPSec seine Berechtigung, aber der aktuelle Entwicklungsstand hat sogar einige seiner Initiatoren gezwungen, proprietäre Derivate zu implementieren, um einige seiner immanenten Schwächen zu überwinden (siehe unten → IPSec für Remote Access). So wird bei IPSec etwa vorausgesetzt, dass die Verbindung bereits steht, bevor die Sicherheits-Verhandlung beginnt.

NCP hat L2Sec (siehe → Konfiguration,Telefonbuch, Security, Verschlüsselungsart (L2Sec)) implementiert, um die Schwächen von IPSec auszuschalten und gleichzeitig den Anforderungen der Unternehmen hinsichtlich offener Standards nachzukommen. L2Sec gilt sowohl vom Standpunkt der Sicherheit als auch der Kommunikation als einzige echte Alternative zu IPSec. L2Sec vereint die Vorteile von L2TP mit Authentisierung und Verschlüsselung nach SSL (TLS). Dieses Verfahren ist im RFC 2716 (Microsoft) niedergelegt. NCP war nicht nur der erste Hersteller, der L2Sec implementiert hatte, lange bevor der RFC veröffentlicht wurde, sondern hat heute bereits auf die Bedürfnisse zahlreicher Großunternehmen, Organisationen und Behörden, die über die Unzulänglichkeiten von IPSec desillusioniert waren, erfolgreich reagiert.

L2Sec – Funktionsbeschreibung

Die PPP-Sicherheits-Verhandlungen erfolgen bei L2Sec, einer Layer 2-Verbindungen mit Security, sobald ein Kanal zum Zentralsystem aufgebaut ist. Layer 2-Kanäle können sein: ISDN B-Kanal, Modem-Verbindung, Tunnel (L2TP). Bei der NCP VPN-Tunneling-Lösung erfolgen alle Verhandlungsschritte verschlüsselt und sicher in einem End to End-Tunnel zwischen Client und VPN Gateway.

Dabei gewährleistet die Datenkommunikation über den End to End-Tunnel im virtuellen privaten Netz völlige Unabhängigkeit von der Kommunikationsumgebung. Der hierbei aufgebaute Tunnel, Geheimgang der Teilnehmer durch ein öffentliches Wählleitungsnetz, verläuft zwischen entferntem VPN Client und zentralem VPN Gateway.

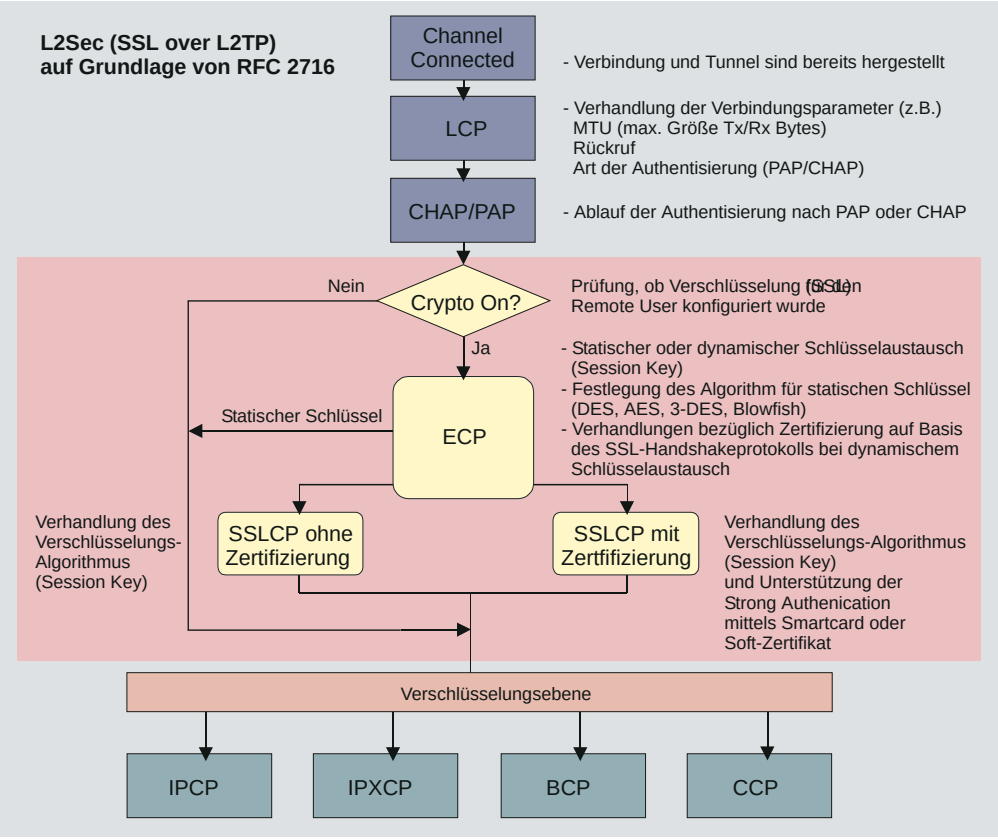
Das komplette IP-Datenpaket, bestehend aus Nutzdaten und IP-Header, wird für die Übertragung verschlüsselt und mit einem neuen Header versehen. Mit anderem Worten: Auch die ursprünglichen IP-Quell- und Zieladressen unterliegen der Kryptierung – ein enormes Sicherheitsplus.

Zwischen dem VPN-Client und dem VPN-Gateway können auf der Wegstrecke des NCP End-to-End-Tunnels beliebig viele IP-Router unterschiedlicher Hersteller installiert sein. Diese müssen weder über Funktionalitäten zur Datenkompression und -Verschlüsselung noch über Tunneling-Protokolle verfügen.

Dies bedeutet Investitionsschutz und Offenheit pur, denn: In das Virtuelle Private Netz können somit sowohl Network Access Server von Internet Service Providern als auch bereits vorhandene eigene bzw. bei Geschäftspartnern installierte IP-Router integriert werden.

Auf diese Weise bildet die NCP Secure Software eine universelle Sicherheits-Infrastruktur, in die sich beliebige Business-Applikationen auf einfache Weise integrieren lassen. Ein zuverlässiges Schlüsselmanagement ist ebenso sichergestellt wie die Einbindung von Certificate Authorities (CAs).

L2Sec – Funktionsskizze



LCP	*Link Control Protocol*
IPCP	*Internet Protocol Control Protocol*
CHAP	*Challenge Authentication Protocol*
IPXCP	*Internetwork Packet Exchange Control Protocol*
PAP	*Password Authentication Protocol*
ECP	*Encryption Control Protocol*
BCP	*Bridge Control Protocol*
SSLCP	*Secure Socket Layer Control Protocol*
CCP	*Compression Control Protocol*
L2Sec	*Layer 2 Security ist funktionell im RFC 2716 beschrieben*

7.2.2 IPSec – Übersicht

IPSec ist ein Standard mit ausgezeichneten Sicherheitsmechanismen, der in bestimmten VPN-Szenarien funktioniert, in denen mit festen IP-Adressen gearbeitet wird (z.B. B2B, Extranet). In diesen Fällen lassen sich auch VPN Gateways verschiedener Hersteller einsetzen. Hier sind feine, bis auf Port-Ebene reichende Sicherheitseinstellungen möglich. Allerdings kann IPSec nur für IP-Datenverkehr eingesetzt werden.

Die IPSec-Spezifikation umfasst nicht nur das (Layer 3-) Tunneling, sondern auch alle notwendigen Sicherheitsmechanismen, wie starke Authentisierung, Schlüsselaustausch und Verschlüsselung.

Mit den IPSec RFCs (2401 - 2409) lässt sich ein VPN mit vorgegebener Security für IP realisieren. Tunneling und Security sind für IPSec vollständig beschrieben, so dass ein komplettes Rahmenwerk für das VPN zur Verfügung steht. Prinzipiell ist es möglich, herstellerunabhängige veschiedene Komponenten zu nutzen. In Site to Site VPNs etwa könnten die VPN Gateways von veschiedenen Herstellern stammen, in End to Site VPNs könnten die Clients von einem anderen Hersteller als die Gateways sein.

Der Verbindungsaufbau zum IPSec-Verkehr erfolgt auf Basis des Internet Key Exchange-Protokolls (IKE).

IPSec – Funktionsbeschreibung

In jedem IP-Host (Client oder Gateway) der IPSec unterstüzt, gibt es ein IPSec-Modul, bzw. eine IPSec-Maschine. Dieses Modul untersucht jedes IP-Paket nach bestimmten Eigenschaften, um die jeweils entsprechende Security-Behandlung darauf anzuwenden.

Die Prüfung der vom IP Stack ausgehenden IP-Pakete erfolgt bezüglich einer Secure Policy Database (SPD). Dabei werden alle konfigurierten SPDs abgearbeitet. (Zunächst die statischen SPDs, die im Konfigurationsbaum unter dem Zweig “IPSec, Secure Policy Database” gelistet sind, erst danach, sofern keine Übereinstimmung gefunden wurde, die dynamische SPD.)

Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil oder Selektor eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist. Das Paket kann einfach durchgelassen werden (permit), es kann abgelehnt bzw. weggeworfen werden (deny) oder bestimmte Security-Richtlinien des IPSec-Prozesses kommen an ihm zur Anwendung. Diese Security-Richtlinien stehen auch im SPD-Eintrag beschrieben.

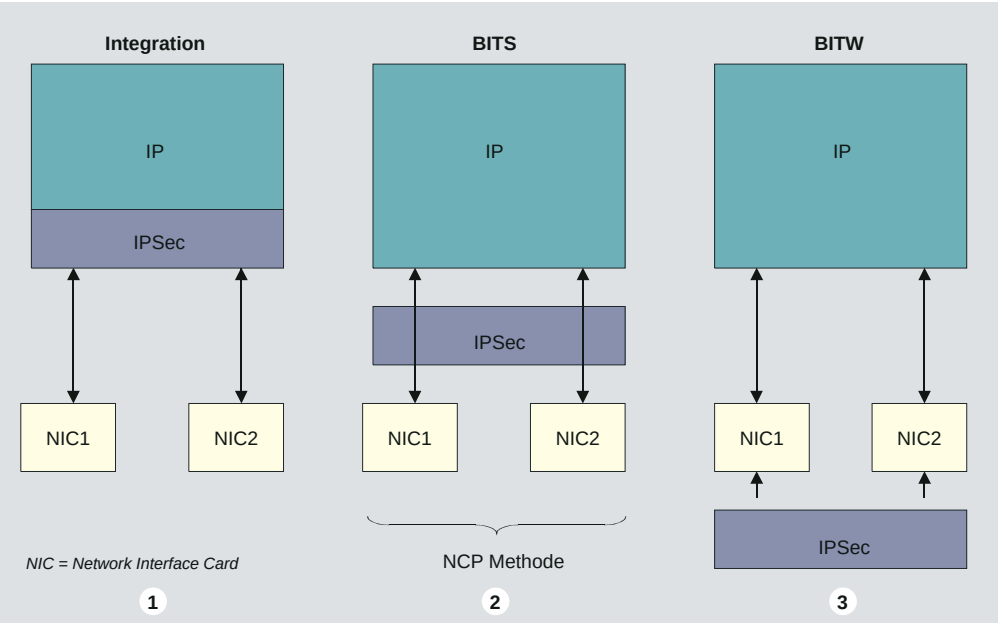
Wird auf diese Weise festgestellt, dass ein IP-Paket mit einem SPD-Eintrag verknüpft ist, der einen IPSec-Prozess einleitet, so wird überprüft, ob bereits eine Sicherheits-Verknüpfung (Security Association, SA) für diesen SPD-Eintrag existiert. Existiert noch keine SA, wird vor dem Aushandeln einer SA zunächst eine Authentisierung und ein Schlüsselaustausch (siehe unten → IPSec-Verhandlung Phase 1) vorgenommen.

Nach der SA-Verhandlung erfolgen in einem weiteren Schritt (siehe unten → IPSec-Verhandlung Phase 2) die Verhandlungen für eine Verschlüsselung (ESP) und/oder Authentisierung (AH) der Datenpakete und ob im Tunnel- oder Transportmodus übertragen werden soll (siehe unten → Transport- und Tunnelmodus).

Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll (ESP oder AH). ESP (Encapsulating Security Payload) unterstützt die Verschlüsselung und die Authentisierung von IP-Paketen , AH (Authentication Header) unterstüzt nur die Authentisierung von IP-Paketen. Die SA beschreibt auch, in welcher Betriebsart das Sicherheitsprotokoll benutzt werden soll (Tunnel- oder Transportmodus). Im Tunnelmodus wird ein IP Header hinzugefügt, im Transportmodus wird der Original-Header verwendet. Weiter beschreibt die SA, welcher Algorithmus zur Authentisierung verwendet werden soll, welche Verschlüsselungsmethode (bei ESP) und welcher Schlüssel zur Anwendungen kommen sollen. Die Gegenstelle muss selbstverständlich nach der gleichen SA arbeiten.

Ist die SA ausgehandelt, wird jedes Datenpaket gemäß Betriebsmodus (Tunnel oder Transport) und Protokoll (ESP oder AH) bearbeitet.

Die Implementierung von IPSec



Die Implementierung von IPSec kann auf drei verschiedene Arten erfolgen:

1. Intergration: Dabei wird IPSec vollständig in den IP Stack integriert. Dies ist jedoch nur möglich, wenn der IP Stack vom gleichen Hersteller entwickelt wird wie IPSec.

2. BITS (Bump in the Stack): In diesem Fall wird IPSec durch zusätzliche Treiber zwischen Layer 2 und dem Netzwerkadapter implementiert. Dies ist die am weitesten verbreitete und auch von NCP angewendete Methode. Dabei stellt sich das IPSec-Modul von NCP als ein LAN-Adapter und Intermediate-Treiber für IPSec und Tunneling (siehe → unten) dar. Die IPSec-Implementierung von NCP ist RFC-konform und vollständig kompatibel zu Drittherstellern.

3. BITW (Bump in the Wire): Hierbei wird IPSec in die Hardware integriert.

IPSec-Dienste

IPSec bietet durch die Wahlmöglichkeit alternativer Sicherheitsprotokolle und Verschlüsselungsalgorithmen verschiedene Sicherheitsdienste. Bei den Sicherheitsprotokollen handelt es sich um ein Authentisierungsprotokoll, festgelegt durch den Header (Authentisierungs-Header / AH), und ein kombiniertes Verschlüsselungs- und Authentisierungsprotokoll, festgelegt durch das Format (Encapsulating Security Payload / ESP). Folgende Sicherheitsdienste werden durch IPSec bereitgestellt:

- ☐ Zugriffskontrolle (Access Control)
- ☐ Integrität (Integrity, AH/ESP)
- ☐ Authentisierung der Datenherkunft (Data origin Authentication, AH/ESP)
- ☐ Vertraulichkeit (Confidentiality, ESP)

IPSec-Richtlinien / IPSec Policy

Die IPSec-Richtlinien sind im Wesentlichen nach den beiden Sicherheitsprotokollen unterschieden, AH oder ESP, die sich im Tunnelmodus gegenseitig ausschließen. Desweiteren legen Sie fest:

- ☐ wie mit ESP verschlüsselt oder mit AH der Hash-Wert zur Authentisierung gebildet werden soll (Transform / Authentisierung)
- ☐ ob zusätzlich in Phase 2 mit der SA-Verhandlung ein kompletter Schlüsselaustausch (PFS) nach Diffie-Hellmann (DH-Gruppe) stattfinden soll
- ☐ und nach welchen Kriterien die Dauer der Schlüsselgültigkeit bemessen wird (Dauer / Gültigkeit)

Im Konfigurationsbaum unter “IPSec” ist eine IPSec-Richtlinie vorkonfiguriert. Sie ist für das Sicherheitsprotokoll ESP eingerichtet.

AH und ESP im Transport- und Tunnelmodus

Beachten Sie zur folgenden Beschreibung bitte die Abbildung auf der gegenüberliegenden Seite.

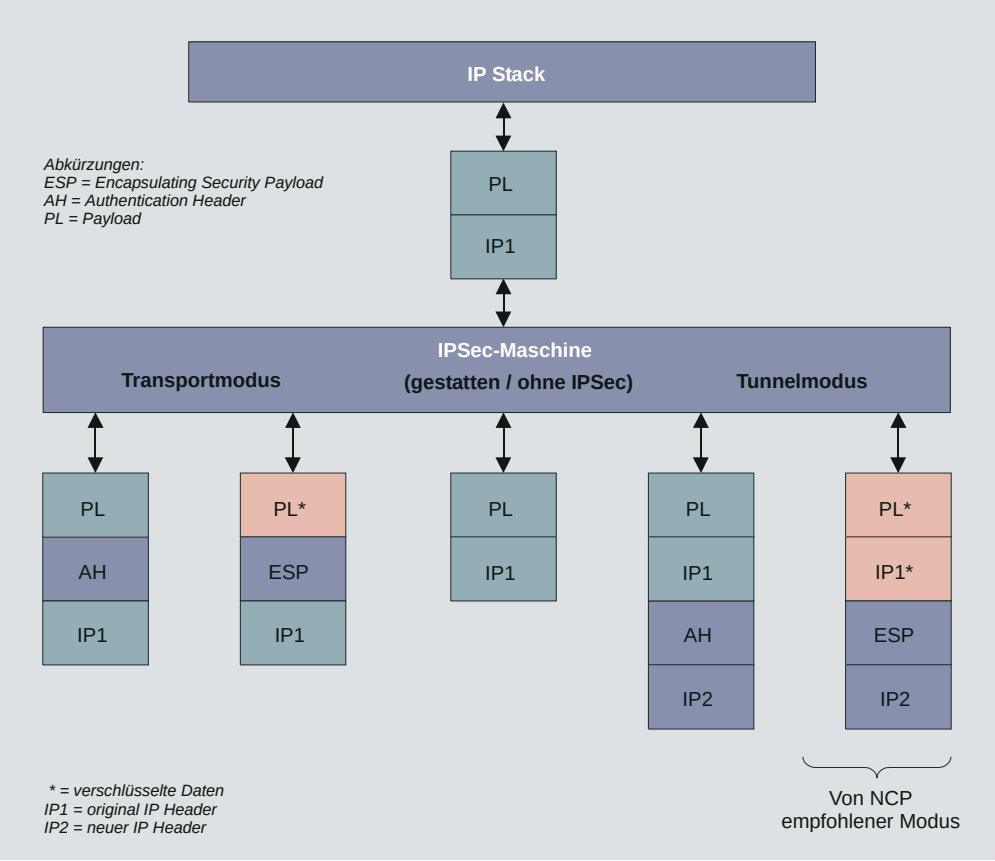
Beide IPSec-Sicherheitsprotokolle (AH und ESP) unterstützen zwei verschiedene Betriebsarten, den Transport- und den Tunnelmodus.

AH im Transportmodus authentifiziert die Nutzdaten des IP-Pakets (Payload) und ausgewählte Teile des IP Headers (IP1). ESP im Transportmodus verschlüsselt (und authentifiziert) die Nutzdaten (Payload) des IP-Pakets, nicht aber den IP Header (IP1). Im Transportmodus werden Ziel- und Quelladressen mit dem IP Header unverschlüsselt übertragen – Quell- und Zieladresse bleiben ungeschützt. Der Transportmodus eignet sich daher nur für eine direkte Kommunikation zwischen zwei Hosts mit festen IP-Adressen oder zwischen Arbeitsplatzrechnern im LAN. (Dieser Modus ist für flexiblen Remote Access völlig ungeeignet.)

Im Tunnelmodus wird das gesamte IP-Paket, einschließlich des hinzugefügten AH- oder ESP-Feldes, eingekapselt und mit einem neuen IP Header (IP2) versehen. Das IP-Paket wird auf diese Weise durch einen Layer 3-Tunnel geschickt. Der innere IP Header mit Original-Adressen ist dabei versteckt und kann nicht eingesehen werden – nur die (Layer 3-) Tunnelendpunkte sind erkennbar. Rechner in Netzen hinter Firewalls oder Routern mit IPSec können in diesem Modus sicher miteinander kommunizieren. Der neue IP Header (IP2) kann völlig andere Quell- und Zieladressen beinhalten als der Original-Header aber er muss Informationen für die Gegenstelle bereithalten, die nötig sind, um das eingekapselte IP-Paket nach den Richtlinien der Sicherheitsverknüpfung (SA) anzunehmen und weiterzuleiten. (Dieser Modus ist für den Secure Server Standard-Einstellung.)

Welches IPSec-Sicherheitsprotokoll mit welchem Verschlüsselungsalgorithmus und welcher Art der Authentisierung kombiniert wird, wird in den IPSec-Richtilinien (IPSec Policy) festgelegt. In der SPD wird auf diese IPSec-Richtlinie, d.h. das Sicherheitsprotokoll, wie auch auf den Betriebsmodus, d.h. Tunnel- oder Transportmodus, verwiesen (siehe → Secure Policy Database, Tunnel).

Funktion der IPSec-Maschine



Die Abbildung (oben) zeigt wie ein IP-Datenpaket vom IP Stack zum IPSec-Modul gesendet wird. Der originale IP Header (IP1) mit seinem Payload (PL-Nutzdaten) wird bearbeitet. Der untere Teil des Bildes zeigt das Ergebnis des IPSec Prozesses.

Der Transportmodus ist nur für Host-zu-Host Kommunikation geeignet, der Tunnelmodus dagegen ermöglicht auch den Betrieb über ein VPN Gateway. Mit dem IP2 Header ist der Transfer von einem Client über das Internet zu einem Gateway möglich. Das VPN Gateway entfernt den IP2 Header, entschlüsselt und sendet das Paket weiter ins lokale LAN. Für Remote Access und End to Site VPN kommt generell nur der ESP-Tunnelmodus in Frage!

7.2.3 Anwendungen

In beiden Betriebsmodi von IPSec erfolgen Authentisierung und Verschlüsselung IP-Adressen-orientiert (auf Layer 3). Daher kommt IPSec insbesondere dann zum Einsatz, wenn beide Kommunikationsendpunkte durch offizielle IP-Adressen gekennzeichnet sind, bzw. die Verbindung vordefiniert ist:

- So lässt sich mit IPSec eine sichere Kommunikation zwischen Zweigstellen eines Unternehmens herstellen. Die Sicherheit dieser LAN-LAN-Kommunikation über ein öffentliches Netz kann auch ohne gemietete Standleitung gewährleistet werden. Ein Unternehmen kann zu diesem Zweck das Internet nutzen. Voraussetzung ist, dass eine Firewall oder ein Router mit IPSec-Funktionalität am Einwahlpunkt des jeweiligen LANs über eine feste offizielle IP-Adresse verfügt.

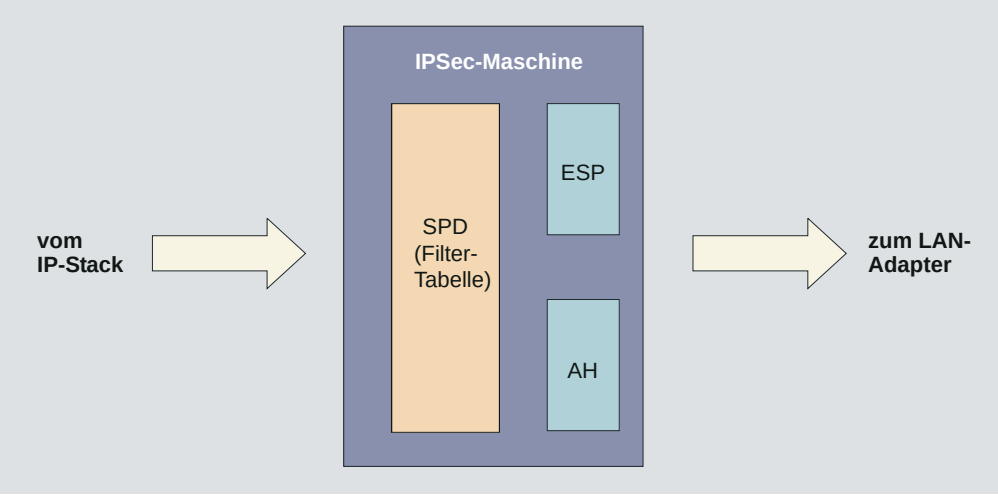
- Ebenso lassen sich mit IPSec Extranet- und Internet-Verbindungen zu Partnern schützen, indem Authentisierung und Vertraulichkeit sichergestellt werden und ein Mechanismus für den Austausch von Schlüsseln festgelegt wird.

- Weitaus schwieriger und nur mit Einschränkungen lassen sich Remote-Anbindungen mehrerer Telearbeiter an das zentrale Firmennetz ausschließlich mit IPSec sichern. Dies liegt daran, dass sich der Client am VPN/GW durch seine IP-Adresse eindeutig identifizieren muss. Ein Client, der sich beim Provider einwählt, ist jedoch nicht durch die IP-Adresse zu erkennen, da er bei jeder Provider-Anwahl eine neue zugewiesen bekommt. Die IP-Adresse, die IPSec zur Authentisierung benötigt (siehe → Bild oben IP1), steht nicht mehr zur Verfügung.

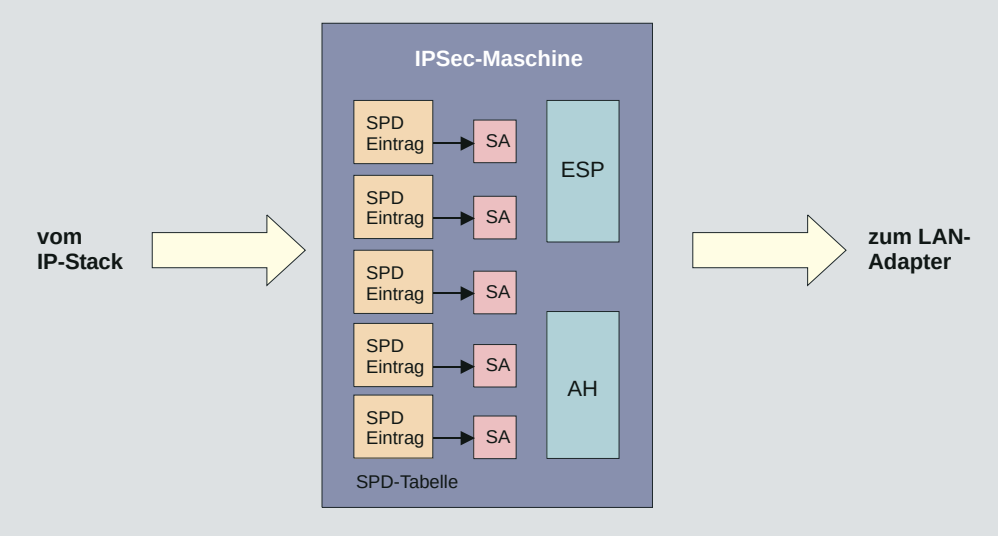
- IPSec kann in diesem Fall nur im Tunnelmodus zum Einsatz kommen. Zudem muss jeder Remote Client über eine eigene private IP-Adresse (eingetragen im Microsoft IP Stack) verfügen, die dem Ziel-Gateway bekannt ist – und für alle Remote Clients muss ein einziger Preshared Key gelten, was die Sicherheit für Remote Access-Anbindungen einschränkt.

7.2.4 Secure Policy Database – Datenbank der Sicherheits-Richtlinien

Ein wesentlicher Bestandteil von IPSec, bzw. der IPSec-Maschine, ist eine Datenbank, in der die Sicherheits-Richtlinien festgehalten sind, die Secure Policy Database (SPD). Siehe Abbildung unten.



Jeder der Einträge der SPD, die wie eine Filtertabelle aufgebaut ist, definiert einen Teil des IP-Verkehrs, sowie die Punkte einer Security Association (SA) dieses Verkehrs. Siehe Abbildung unten.



Zunächst entscheiden drei verschiedene Stati der SPD über den weiteren Umgang mit den IP-Paketen (siehe → Selektoren, Status). Da in der IPSec-Maschine immer die Pakete definierter IP-Adressen bearbeitet werden, beziehen sich die Stati der SPD immer auch nur auf die in den Selektoren angegebenen Adressen oder Adressbereiche:

- ☐ IPSec (IPSec) → für die IP-Pakete mit Adressen aus dem definierten Bereich werden die IPSec-Sicherheitsdienste angewendet, die SPD-Filtertabelle kommt zum Einsatz
- ☐ gestatten (permit) → die IP-Pakete mit Adressen aus dem definierten Bereich werden durchgelassen, ohne dass die SPD zum Einsatz kommt
- ☐ sperren (deny) → alle IP-Pakete mit Adressen aus dem definierten Bereich werden weggeworfen
- ☐ inaktiv (disabled) → diese SPD wird ausgeschaltet und kommt für IPSec nicht zum Einsatz, ohne dass sie gelöscht werden muss

■ Sicherheits-Verknüpfung (Security Association / SA)

Die Security Association bezeichnet eine Einwegbeziehung zwischen Sender und Empfänger von Daten, die die Sicherheitsdienste für den Datenaustausch definiert (und bereitstellt). Für sicheren Datenaustausch in einer bidirektionalen Peer-to-Peer-Verbindung sind zwei SAs erforderlich. Mit Hilfe der SPD wird dem IP-Verkehr eine bestimmte Sicherheitsverknüpfung (SA) zugeordnet. (Vergleiche Abbildung und Bildbeschreibung auf der folgenden Seite.)

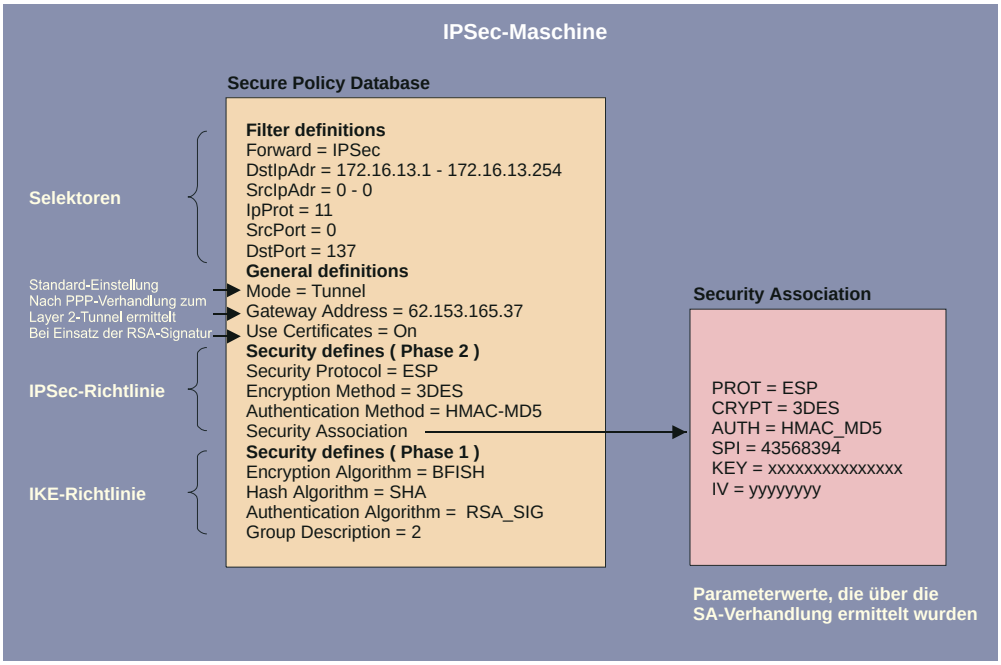
Jeder SPD-Eintrag wird durch eine Gruppe von IP- und Oberschichtprotokoll-Parametern definiert, den Selektoren. Mit ihnen wird der ausgehende Verkehr so gefiltert, dass er zu einer bestimmten SA passt.

Dabei wird jedes einzelne IP-Paket nach folgenden Kriterien untersucht:

1. Vergleiche die Selektorenfelder des IP-Pakets mit der SPD, um einen Eintrag zu finden, der auf eine SA verweist
2. Selektiere eine passende SA nach dem Security Parameter Index (SPI)* im IP-Paket
3. Führe die entsprechenden IPSec-Anweisungen aus (z.B. AH oder ESP)

** Der SPI (Security Parameters Index) ist ein Bitstring und wird in den AH- oder ESP-Header des IP-Pakets eingetragen, damit die Gegenstelle die zugehörige SA erkennen kann.*

Beispiel einer Secure Policy Database von NCP



Bildbeschreibung zu obiger Abbildung:

Die Prüfung der vom IP Stack ausgehenden IP-Pakete erfolgt bezüglich einer Secure Policy Database (SPD). Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil oder Selektor eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderen IP Header-spezifischen Einträgen. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist. Das Paket kann einfach durchgelassen werden (permit), es kann abgelehnt bzw. weggeworfen werden (deny) oder bestimmte Security-Richtlinien des IPSec-Prozesses kommen an ihm zur Anwendung (IPSec). Diese Security-Richtlinien stehen auch im SPD-Eintrag beschrieben.

Wird auf diese Weise festgestellt, dass ein IP-Paket mit einem SPD-Eintrag verknüpft ist, der einen IPSec-Prozess einleitet, so wird überprüft, ob bereits eine Sicherheits-Verhandlung (Security Association, SA) für diesen SPD-Eintrag existiert. Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll (ESP oder AH). ESP, Encapsulating Security Payload, unterstützt die Verschlüsselung und die Authentisierung von IP-Paketen, AH, Authentication Header, unterstüzt nur die Authentisierung von IP-Paketen. Die SA beschreibt auch, in welcher Betriebsart das Sicherheitsprotokoll benutzt werden soll (Tunnel- oder Transportmodus). Im Tunnelmodus wird ein IP Header hinzugefügt, im Transportmodus wird der Original-Header verwendet. Weiter beschreibt die SA, welcher Algorithmus zur Authentisierung verwendet werden soll, welche Verschlüsselungsmethode (bei ESP) und welcher Schlüssel zur Anwendungen kommen sollen. Die Gegenstelle muss selbstverständlich nach der gleichen SA arbeiten.

■ Selektoren (der statischen SPD)

Der Selektor oder Filterteil eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist.

Im folgenden die Selektoreneinträge zur Konfiguration im Secure Client von NCP:

☐ Status / State (siehe oben)

IPSec (IPSec), gestatten (permit), sperren (deny), inaktiv (disabled)

☐ IP-Protokoll / IP Protocol

Dies ist das Transportprotokoll (ICMP, TCP oder UDP). Eines der angebotenen Protokolle kann ausgewählt werden oder ein beliebiges (alle / any) wird genutzt.

☐ IP-Adresse (Quelle) / Source IP Address

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Ausgangssysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

☐ IP-Adresse (Ziel) / Destination IP Address

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Zielsysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

☐ Port (Quelle) / Source Port

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

☐ Port (Ziel) / Destination Port

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

7.2.5 SA-Verhandlung und Richtlinien / Policies

Damit der IPSec-(Filter-)Prozess in Gang kommen kann, muss vorher die SA verhandelt worden sein. Diese SA-Verhandlung findet pro SPD – die für verschiedene Ports, Adressen und Protokolle angelegt sein können (siehe → Selektoren) – einmal statt. Für diese SA-Verhandlung wird ein Kontrollkanal benötigt.

- **Phase 1 (Parameter der IKE-Richtlinie / IKE Policy):**

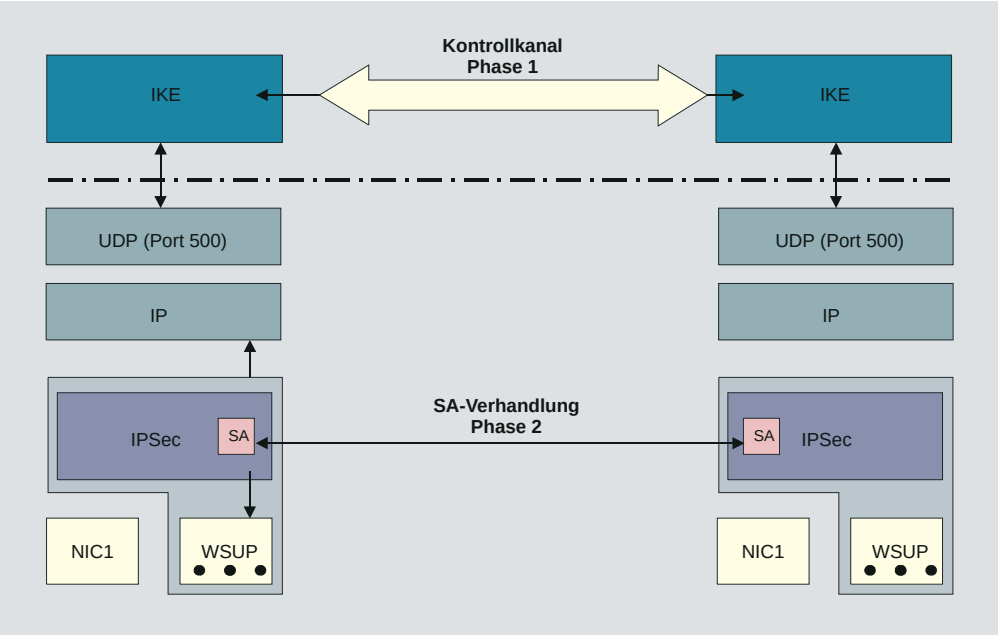
Der Kontrollkanal wird im Tunnelmodus von IPSec über das IKE-Protokoll zur IP-Adresse des Secure Gateways aufgebaut, im Transportmodus direkt zur IP-Adresse der Gegenstelle. (Tunnel- oder Transportmodus wird gesetzt unter “Secure Policy Database, Tunnel”).

Parameter zur Festlegung von Verschlüsselungs- und Authentisierungsart über das IKE-Protokoll definieren Sie in den IKE-Richtlinien. Dabei kann die Authentisierung über einen Preshared Key oder eine RSA Signatur erfolgen. (In der Secure Policy Database wird unter Security auf diese IKE-Richtlinie verwiesen.)

- **Phase 2 (Parameter der IPSec-Richtlinie / IPSec Policy):**

Die SA-Verhandlung wird über den Kontrollkanal abgewickelt. Von der IPSec-Maschine wird die SA an das IKE-Protokoll übergeben, das sie über den Kontrollkanal zur IP-Sec-Maschine der Gegenstelle überträgt.

Kontrollkanal und SA-Verhandlung



Bildbeschreibung:

Damit der IPSec-Prozess in Gang kommen kann, muss vorher die SA verhandelt worden sein. Diese SA-Verhandlung findet pro SPD – die für verschiedene Ports, Adressen und Protokolle angelegt sein können – einmal statt. Für diese SA-Verhandlung wird ein Kontrollkanal benötigt.

Im Client muss nun zunächst eine Layer 2-(PPP)-Verbindung zum Provider hergestellt werden. Dabei bekommt er (bei jeder Einwahl) eine neue IP-Adresse. Das IPSec-Modul im Client bekommt ein IP-Paket mit der Zieladresse der Firmenzentrale. Ein SPD-Eintrag für dieses IP-Paket wird gefunden aber es existiert noch keine SA. Das IPSec-Modul stellt die Anforderung an das IKE-Modul, eine SA auszuhandeln. Dabei werden auch die angeforderten Sicherheits-Richtlinien, wie sie im SPD-Eintrag vorhanden sind, an das IKE-Modul übergeben. Eine IPSec-SA auszuhandeln wird als Phase-2-Verhandlung bezeichnet. Bevor jedoch eine IPSec-SA mit der Gegenstelle (Secure Server) ausgehandelt werden kann, muss eine Art Kontrollkanal vom Client zum Secure Server existieren. Dieser Kontrollkanal wird über die Phase-1-Verhandlung hergestellt, deren Ergebnis eine IKE-SA ist. Die Phase-1-Verhandlung übernimmt somit die komplette Authentisierung vom Client gegenüber dem Secure Server (VPN Gateway) und erzeugt einen verschlüsselten Kontrollkanal. Über diesen Kontrollkanal kann dann rasch die Phase 2 (IPSec SA) durchgeführt werden. Die Phase-1-Verhandlung ist ein Handshake, über den auch der Austausch von Zertifikaten möglich ist und die den Schlüsselaustausch für den Kontrollkanal beinhaltet.

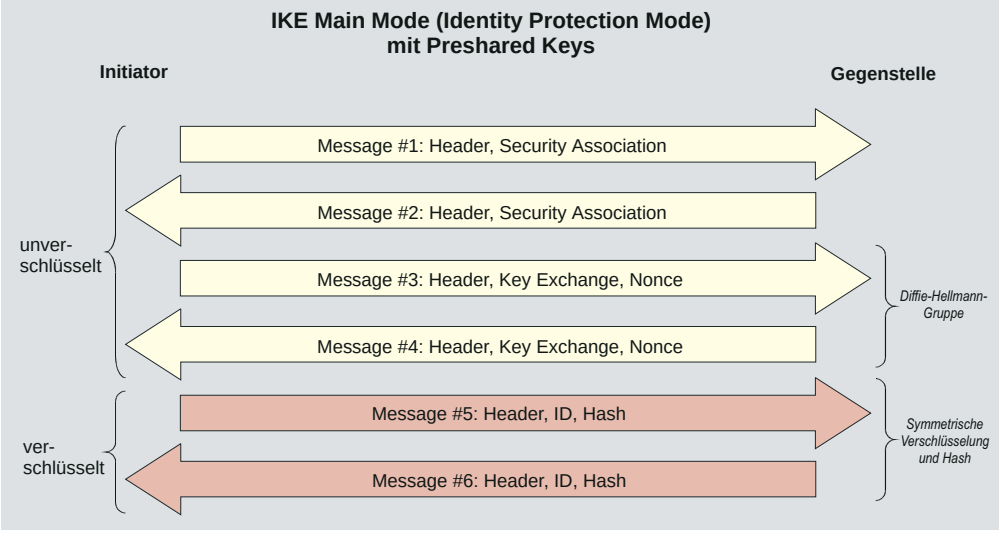
IKE-Modi

Im wesentlichen können zwei Arten der IKE-Richtlinien konfiguriert werden. Sie unterscheiden sich durch die Art der Authentisierung, entweder über Preshared Key oder über RSA-Signatur. Beide Arten des Internet Key Exchanges können in zwei unterschiedlichen Modi ausgeführt werden, dem Main Mode, auch Identity Protection Mode, oder dem Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch die Verschlüsselung.

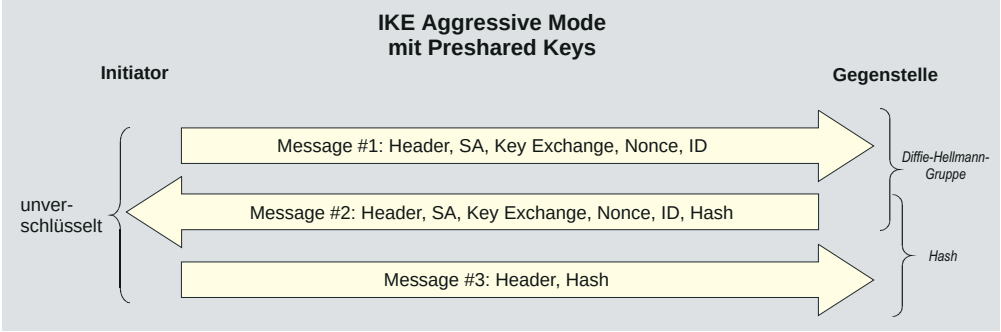
Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

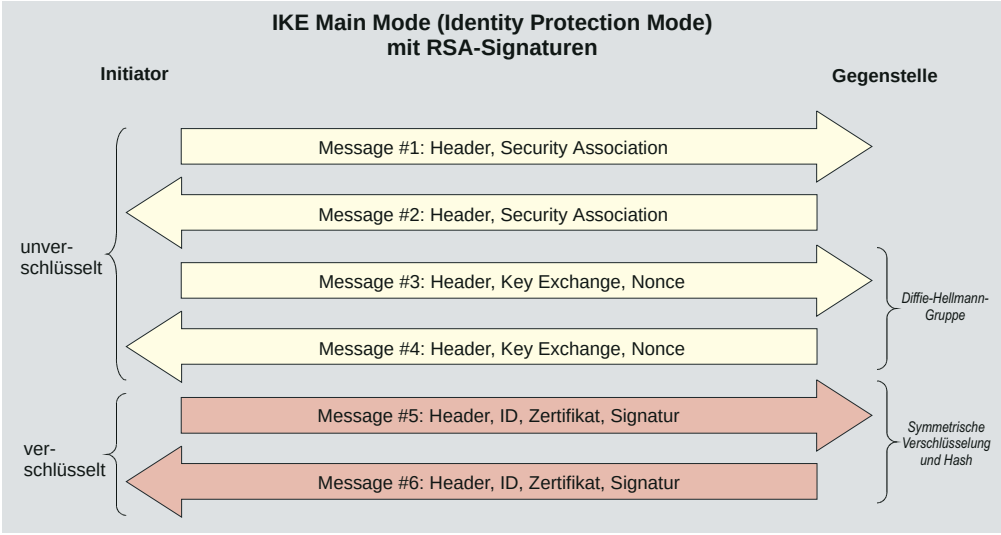
Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in den Parameterfeldern “Security” des Telefonbuchs (für eine dynamische SPD) und unter “IPSec, Secure Policy Database” (für eine statische SPD). (Siehe auch → Austausch-Modus / Exchange Mode)



Wird die Preshared Key-Methode im Main Mode genutzt (Bild oben), so muss der Client am VPN/GW durch seine IP-Adresse eindeutig identifizierbar sein, da der Preshared Key mit in die symmetrische Schlüsselberechnung einbezogen und verschlüsselt wird, bevor sonstige Informationen übertragen werden, die den Client identifizieren könnten. Ein Client, der sich beim Provider einwählt, ist jedoch nicht durch die IP-Adresse zu erkennen, da er bei jeder Provider-Anwahl eine neue zugewiesen bekommt. Letztlich kann im Main Mode an alle Clients nur derselbe Preshared Key vergeben werden, was allerdings die Authentisierung abschwächt.



Eine Möglichkeit, einen allgmeinen Preshared Key zu vermeiden, wäre, den Aggressive Mode zu nutzen (Bild oben), doch wird dabei die ID des Clients nicht verschlüsselt.



Werden RSA-Signaturen eingesetzt (Bild oben und unten), so bedeutet dies, dass Zertfikate zum Einsatz kommen, womit die Vorkonfiguration jedweder "Secrets" überflüssig wird.

7.3 IPSec für Remote Access – IPSec over L2TP

Wie lässt sich IPSec in uneingeschränktem Funktionsumfang für Remote Access nutzen, ohne dass Sicherheitslücken entstehen, d.h. wie kann trotz sich ändernder IP-Adressen das Prinzip der IP-Adressen-Orientierung von IPSec beibehalten werden, ohne dass die oben beschriebenen Einschränkungen vorgenommen werden müssen?

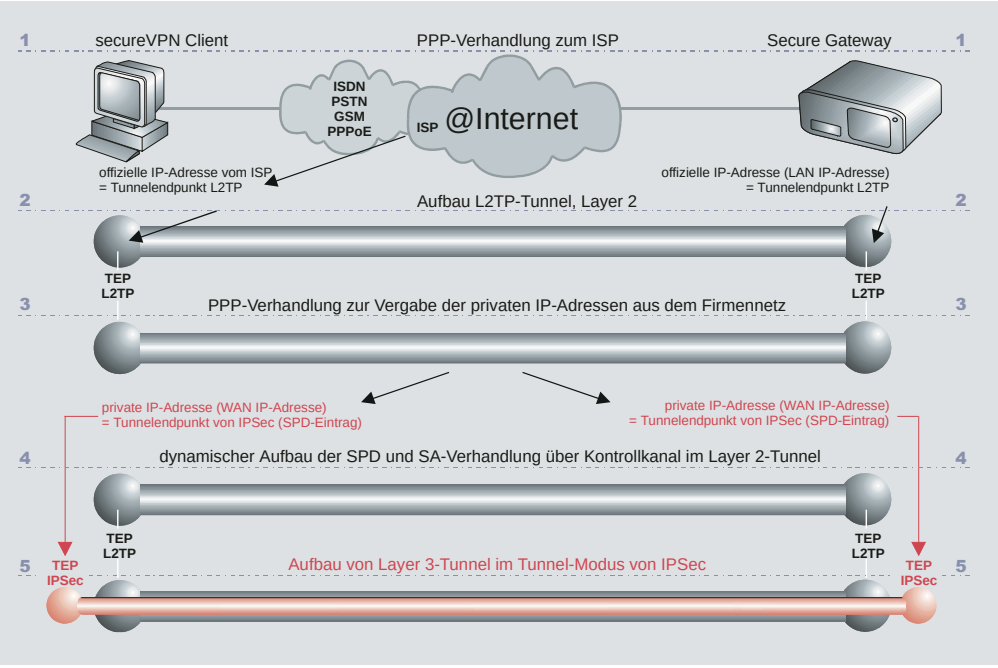
Wie in RFC 2888 beschrieben und von verschiedenen IPSec-Experten empfohlen, kann dies bewerkstelligt werden, indem zunächst ein Layer 2-Tunnel über das Internet zwischen Remote Access Client und Zentralsystem aufgebaut wird, so dass die anschließende IPSec-Verhandlung bereits in einem VPN (Virtual Private Network) getunnelt stattfindet.

Der Tunnelaufbau wird durch eine Benutzer-orientierte Authentisierung (Layer 2) gesichert. Danach kann eine IP-Adresse aus dem Firmennetz vergeben werden, die für den daraufhin einsetzenden IPSec-Prozess verwendet werden kann.

Mit IPSec over L2TP werden alle Nachteile von IPSec im Remote Access-Bereich wett gemacht. Jeder handelsübliche Router, der IP Network Address Translation unterstützt, kann eingebunden werden. Zudem besteht die Möglichkeit, über standardisierte Schnittstellen zusätzliche Sicherheitsmechanismen einer Public Key Infrastucture zu nutzen. Um die Sicherheit von IPSec over L2TP auf ganzer Strecke gewährleisten zu können, empfiehlt NCP das Secure Gateway hinter dem Access Server und der Firewall in der Demilitarisierten Zone (DMZ) zu installieren. Damit befinden sich alle Parameter der sicheren Datenübertragung im Einflussbereich des Unternehmens:

- ☑ Endpunkte des Layer 2-Tunnels (Secure Server, VPN Gateway, Remote Client)
- ☑ Tunnelingverfahren
- ☑ Schlüsselalgorithmus
- ☑ Netzwerkprotokoll
- ☑ Datenkompression
- ☑ Übertragungsmedium
- ☑ IP-Adresse aus dem Firmennetz
- ☑ IPSec-Parameter

IPSec over L2TP mit dynamischer SPD



1. Standard-PPP-Verhandlung über Benutzer / Passwort (User ID / Password) und Authentisierung vom Client gegenüber Internet Service Provider (ISP), wonach der Client eine offizielle IP-Adresse vom ISP erhält. Anschließend baut der Client eine Verbindung zum Secure Server via Internet auf. Die dazu nötigen Parameter befinden sich im Telefonbuch des Clients unter "Zielsystem" und "Netzeinwahl". Die "Tunnel IP-Adresse (Ziel)", eingetragen im Telefonbuch unter "Tunnelparameter", entspricht der offiziellen IP-Adresse des Secure Servers.
2. Nach Prüfung des "Tunnelsecret" werden die Tunnel-Parameter verhandelt und der L2TP-Tunnel im Layer 2 aufgebaut. Tunnelendpunkte sind die offizielle IP-Adresse, die der Client vom ISP erhalten hat und die offizielle IP-Adresse des Secure Servers, die im Telefonbuch des Clients als "Tunnel IP-Adresse (Ziel)" eingetragen ist.(1 (*2*
3. Nach einer weiteren PPP-Verhandlung und Prüfung von "Benutzer" und "Passwort", erfolgt die Vergabe der privaten IP-Adressen aus dem Firmennetz. Diese Adressen können aus einem Pool des Secure Servers stammen (siehe → Routing Interfaces, Pools). Der Remote Client ist damit – unabhängig von seinem Standort – immer eindeutig anhand seiner IP-Adresse identifizierbar.
4. Über den Kontrollkanal im Layer 2-Tunnel findet die SA-Verhandlung statt. Die Strong Authentication erfolgt gemäß der IKE-Richtlinien (IKE Policy), die für dieses Link-Profil festgelegt wurden (siehe → Telefonbuch, Security).
5. Der Layer 3-Tunnel wird nach Vorgabe des IPSec-Betriebsmodus (siehe → Telefonbuch, Security, IPSec-Richtlinie) aufgebaut. Tunnelendpunkte sind die IP-Adressen aus dem Firmennetz.

*(*1 Nach IETF muss das Tunnelende immer im geschützten privaten Bereich des VPN-Betreibers, hinter der Firewall in der DMZ liegen.*
*(*2 Bei L2Sec erfolgt hier die SSL-Verhandlung.*

7.4 Verbindungen über das Tunnelprotokoll “IPSec Tunneling”

Im Telefonbuch des Clients unter “Tunnel-Parameter” kann zwischen den VPN-Protokollen “L2TP” (Layer 2) und “IPSec Tunneling” (Layer 3) gewählt werden. Wird das VPN-Protokoll “IPSec Tunneling” gewählt, so wird die IPSec-Verbindung ohne einen Layer 2-Tunnel (L2TP) hergestellt. Diese Art des IPSec Tunnelings entspricht dem standardmäßigen Einsatz von IPSec (IPSec native), das auf diese Weise auch gegenüber IPSec-Gateways zum Einsatz kommen kann, die von anderen Herstellern als NCP stammen.

Die Kompatibilität mit den IPSec-Modi der anderen Hersteller beruht auf der Konformität mit folgenden RFCs und Drafts zu IPSec:

RFC 2104 - Keyed-Hashing for Message Authentication
RFC 2401 - Security Architecture for the Internet Protocol
RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2406 - IP Encapsulating Security Payload (ESP)
RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 - The Internet Key Exchange (IKE)
DRAFT - draft-beaulieu-ike-xauth-05 (XAUTH)
DRAFT - draft-dukes-ike-mode-cfg-02 (IKECFG)
DRAFT - draft-ietf-ipsec-dpd-01 (DPD)
DRAFT - draft-ietf-ipsec-nat-t-ike-01 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-02 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-03 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-05 (NAT-T)
DRAFT - draft-ietf-ipsec-udp-encaps-06 (UDP-ENCAP)

- **Implementierte Algorithmen für Phase 1 und 2:**

Unterstützte Authentisierung für Phase 1 (IKE-Richtlinie)

– RSA-Signatur

– PSK (Preshared Key)

Unterstützte symmetrische Verschlüsselungsalgorithmen (Phase 1 + 2)

– DES

– 3DES

– AES-128, AES-192, AES-256

Unterstützte asymmetrische Verschlüsselungsalgorithmen (Phase 1 + 2)

– DH 1,2,5 (Diffie-Hellmann)

– RSA

Unterstützte Hash-Algorithmen

– MD5

– SHA-1

Zusätzliche Unterstützung für Phase 2

– PFS (Perfect Forward Secrecy)

– IPCOMP (LZS)

– Seamless re-keying

Wird ein Zielsystem im Telefonbuch des Clients mit “IPSec-Tunneling” konfiguriert, so werden zunächst einige Standards gesetzt (siehe unten “Zur Konfiguration ...”):

– IKE Phase 1 Richtlinie - Von Gegenstelle bestimmt

– IKE Phase 2 Richtlinie - Von Gegenstelle bestimmt

– IKE Phase 1 Modus RSA - Main Mode

– IKE Phase 1 Modus PSK - Aggressive Mode

Diese automatisch gesetzten Richtlinien und Verhandlungsmodi sind jedoch im Telefonbuch konfigurierbar gehalten, sodass sie anderslautenden Verbindungsanforderungen entsprechend modifiziert werden können.

Standard IKE-Vorschläge:

1. Bleibt das Feld für “Preshared Key” leer, wenn die Einstellung “von Gegenstelle bestimmt” vorgenommen wurde, so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer mit Zertifikat erfolgt (vgl. → IKE-Richtlinie, Phase-1-Parameter):

Notation:

```
EA    = Encryption Algorithm (Verschlüsselung)
HASH  = Hash Algorithm (Hash)
AUTH  = Authentication Method (Authentisierung)
GROUP = Diffie-Hellmann Group Number (DH-Gruppe)
LT    = Life Type (Dauer)
LS    = Life Seconds (Dauer)
KL    = Key Length (Schlüssellänge)
```

EA	HASH	AUTH	GROUP	LT	LS	KL
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	SHA	RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	RSA	DH2	SECONDS	28800	128
DES3	SHA	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	SHA	RSA	DH5	SECONDS	28800	0
DES3	MD5	RSA	DH5	SECONDS	28800	0
DES3	SHA	XAUTH_RSA	DH2	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH2	SECONDS	28800	0
DES3	SHA	RSA	DH2	SECONDS	28800	0
DES3	MD5	RSA	DH2	SECONDS	28800	0

Wird ein spezifischer IKE-Vorschlag in der IPSec-Konfiguration des Client-Telefonbuchs eingestellt, so wird immer auch automatisch der gleiche Vorschlag zusätzlich mit Extended Authentication generiert und versendet.

2. Wird in das Feld für “Preshared Key” ein String eingetragen, so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer ohne Zertifikat erfolgt:

```
EA       HASH AUTH       GROUP LT      LS     KL
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 256
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 256
AES_CBC SHA  PSK       DH5   SECONDS 28800 256
AES_CBC MD5  PSK       DH5   SECONDS 28800 256
AES_CBC SHA  XAUTH_PSK DH2   SECONDS 28800 256
AES_CBC MD5  XAUTH_PSK DH2   SECONDS 28800 256
AES_CBC SHA  PSK       DH2   SECONDS 28800 256
AES_CBC MD5  PSK       DH2   SECONDS 28800 256
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 192
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 192
AES_CBC SHA  PSK       DH5   SECONDS 28800 192
AES_CBC MD5  PSK       DH5   SECONDS 28800 192
AES_CBC SHA  XAUTH_PSK DH5   SECONDS 28800 128
AES_CBC MD5  XAUTH_PSK DH5   SECONDS 28800 128
AES_CBC SHA  PSK       DH5   SECONDS 28800 128
AES_CBC MD5  PSK       DH5   SECONDS 28800 128
AES_CBC SHA  XAUTH_PSK DH2   SECONDS 28800 128
AES_CBC MD5  XAUTH_PSK DH2   SECONDS 28800 128
AES_CBC SHA  PSK       DH2   SECONDS 28800 128
AES_CBC MD5  PSK       DH2   SECONDS 28800 128
DES3     SHA  XAUTH_PSK DH5   SECONDS 28800 0
DES3     MD5  XAUTH_PSK DH5   SECONDS 28800 0
DES3     SHA  PSK       DH5   SECONDS 28800 0
DES3     MD5  PSK       DH5   SECONDS 28800 0
DES3     SHA  XAUTH_PSK DH2   SECONDS 28800 0
DES3     MD5  XAUTH_PSK DH2   SECONDS 28800 0
DES3     SHA  PSK       DH2   SECONDS 28800 0
DES3     MD5  PSK       DH2   SECONDS 28800 0
```

Als Vorschläge für die IPSec-Richtlinie (Phase 2) wird standardmäßig folgendes geschickt:
Notation:

```
PROTO  - Protocol (Protokoll)
TRANS  - Transform (Transformation (ESP))
LT     - Life Type (Dauer)
LS     - Life Seconds (Dauer)
KL     - Key Length (Schlüssellänge)
COMP   - IP Compression (Transformation (Comp))
```

```
PROTO TRANS AUTH LT      LS     KL  COMP LZS
ESP   AES   MD5  SECONDS 28800 128 Yes  Yes
ESP   AES   SHA  SECONDS 28800 128 Yes  Yes
ESP   AES   MD5  SECONDS 28800 128 No   No
ESP   AES   SHA  SECONDS 28800 128 No   No
ESP   AES   MD5  SECONDS 28800 192 Yes  Yes
ESP   AES   SHA  SECONDS 28800 192 Yes  Yes
ESP   AES   MD5  SECONDS 28800 192 No   No
ESP   AES   SHA  SECONDS 28800 192 No   No
ESP   AES   MD5  SECONDS 28800 256 Yes  Yes
ESP   AES   SHA  SECONDS 28800 256 Yes  Yes
ESP   AES   MD5  SECONDS 28800 256 No   No
ESP   AES   SHA  SECONDS 28800 256 No   No
ESP   DES3  MD5  SECONDS 28800 0   Yes  Yes
ESP   DES3  MD5  SECONDS 28800 0   No   No
```

Zur Konfiguration des VPN-Protokolls “IPSec Tunneling”

Im Telefonbuch des Clients unter “Tunnel-Parameter” kann zwischen den VPN-Protokollen “L2TP” (Layer 2) und “IPSec Tunneling” (Layer 3) gewählt werden. Wird das VPN-Protokoll “IPSec Tunneling” gewählt, so wird die IPSec-Verbindung ohne einen Layer 2-Tunnel (L2TP) hergestellt. Bei Auswahl von “IPSec Tunneling” wird darauf hingewiesen, dass im Konfigurationsfeld “Security” automatisch folgende Einstellungen vorgenommen werden:

Security-Modus	=	IPSec
IKE-Richtlinie	=	Von Gegenstelle bestimmt
IPSec-Richtlinie	=	Von Gegenstelle bestimmt
Austausch-Modus	=	Main Mode

Im Telefonbuch unter der Rubrik “Security” werden die Parameter “IKE ID-Typ” und “IKE ID” zur Konfiguration eingeblendet:

IKE ID-Typ	=	Alternativen: IP-Adresse, Fully Qualified Domain Name, Fully Qualified Username, IP Subnet-Adresse, ASN1 Distinguished Name, ASN1 Group Name, Free String used to identify Groups
IKE ID	=	je nach ausgewähltem ID-Typ muss der zugehörige String eingetragen werden.

“Preshared Key” oder “RSA Signatur”: Entsprechend den Vorgaben durch die Gegenstelle kann als “IKE-Richtlinie” die automatisch vorgenommene Einstellung “Von Gegenstelle bestimmt” auf “Preshared Key” oder “RSA Signatur” (Zertifikat) abgeändert werden. Erwartet die Gegenstelle “Preshared Key”, so muss der Schlüssel in das Feld eingetragen werden. (Der Preshared Key muss in diesem Fall für alle Clients identisch sein.)

IP-Adressen und DNS Server werden über das Protokoll IKE-Config Mode (Draft 2) zugewiesen (kompatibel derzeit nur gegen Cisco, siehe auch unten DHCP-Modus). Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

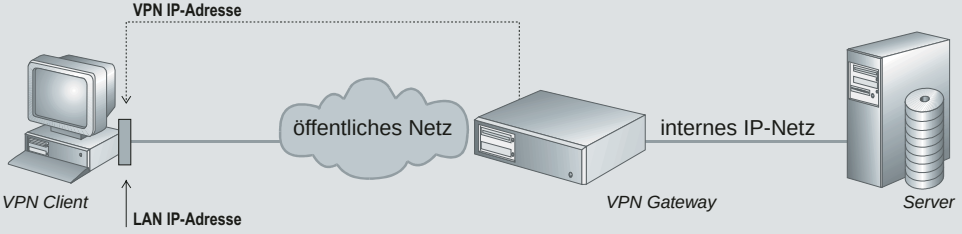
Die Authentisierung bei “IPSec Tunneling” erfolgt über das XAUTH Protokoll (Draft 6). Dazu müssen außerdem noch folgende Parameter im Konfigurationsfeld “Tunnel-Parameter” gesetzt werden:

VPN-Benutzername	=	Kennwort des IPSec-Benutzers
VPN-Passwort	=	Passwort des IPSec-Benutzers
Benutze Zugangsdaten von Zertifikat	=	optional

Bei “IPSec Tunneling” wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der IPSec Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Der Einsatz von NAT Traversal erfolgt beim IPSec Client automatisch und ist immer nötig, wenn auf dem weg zum Zielsystem ein Gerät mit Network Address Translation zum Einsatz kommt.

DHCP-Modus und private IP-Adresse am Client

Die VPN IP-Adresse darf nicht mit der des physikalischen LAN-Adapters übereinstimmen. Desweiteren muss eine private IP-Adresse im Telefonbuch des Clients unter IPSec-Optionen eingetragen werden, wenn der Client keine IP-Adresse vom IPSec Gateway über IKE-Config erhält.



	IKE Config-Mode Verhandlung	DHCP-Modus auf NCP Adapter aktiviert	Private IP-Adresse in IPSec-Optionen eingetragen
LAN IP-Adresse entspricht nicht VPN IP-Adresse	ja	ja	nein
	nein	ja	ja
LAN IP-Adresse entspricht VPN IP-Adresse	ja	nein	nein
	nein	nein	ja

7.5 Sichere End-to-End-Kommunikation auch ohne feste offizielle IP-Adresse

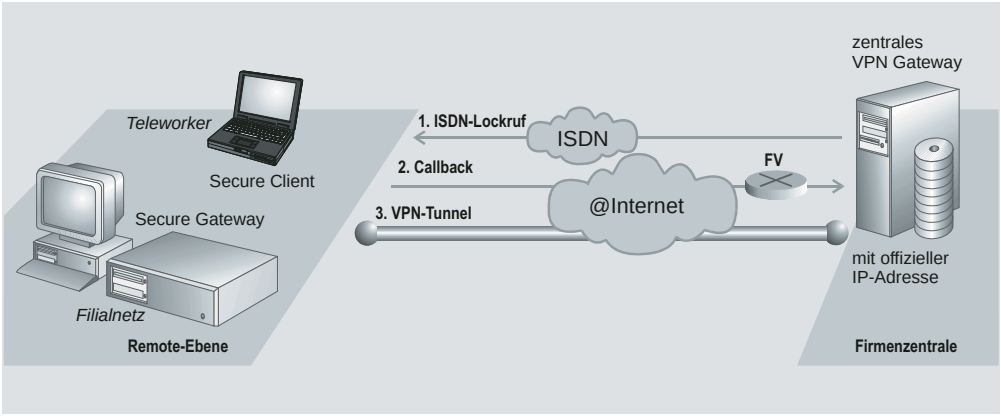
Die Zielsetzung der Unternehmen und Organisationen, Corporate Networks immer kostengünstiger gestalten zu wollen ohne auf Vertrauenswürdigkeit und Vertraulichkeit zu verzichten, hat Virtuelle Private Netze (VPNs) in den Mittelpunkt von Netzwerkplanungen rücken lassen. VPNs ersetzen zunehmend Standleitungs-basierte Datennetze durch virtuelle Unternehmensnetze via Internet und Wählleitungen.

In Internet-VPNs (auch IP-VPNs genannt) ist jeder Kommunikationspartner grundsätzlich nur über eine öffentliche (offizielle) IP-Adresse erreichbar, die ihm vom Internet Service Provider (ISP) bei jeder Einwahl zugeordnet wird. Die Internetzugänge mit festen IP-Adressen als Voraussetzung für einen Verbindungsaufbau über IP sind verhältnismäßig teuer. Deshalb wird mit günstigen Internetzugängen ohne feste IP-Adresse gearbeitet, d.h. der Benutzer bekommt bei jedem Verbindungsaufbau in das Internet eine andere IP-Adresse zugewiesen. Das Auffinden eines solchen Partners erfordert besondere Mechanismen, die von der eingesetzten VPN-Lösung erbracht werden müssen.

Die Leistungsmerkmale “Lockruf” und “DynDNS” (Dynamic Domain Name Server) bieten alle auf diese Kommunikationsbedürfnisse abgestimmten Funktionalitäten. Auf diese Weise ist ein hochsicherer, performanter Datenverkehr via Internet gewährleistet, auch ohne feste IP-Adressen der Kommunikationspartner

Anschließend sind die Funktionalitäten der Leistungsmerkmale im Überblick beschrieben.

Dial Out mit Lockruf: Firmenzentrale verfügt über eine feste IP-Adresse



Ablauf des Verbindungsaufbaus: Nachdem das Gateway einen Lockruf via ISDN an die Remote-Ebene abgesetzt hat (1), erfolgt ein Verbindungsaufbau (Rückruf / Callback) an die vorkonfigurierte feste IP-Adresse des Gateways (2), womit gleichzeitig ein VPN-Tunnel aufgebaut wird (3).

7.5.1 Lockruf

Der Lockruf ermöglicht, die Kommunikationsgegenstelle über den Kommunikationswunsch zu informieren, ohne dass diese Online ist.

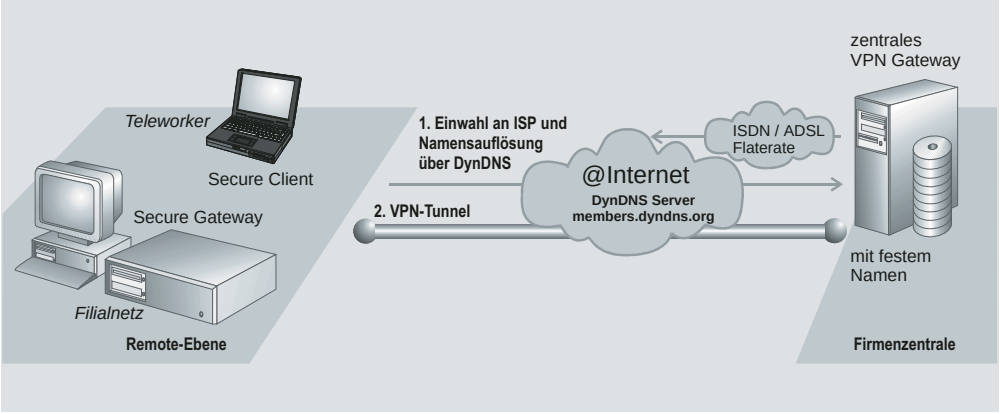
Liegen z.B. Daten in der Firmenzentrale für einen entfernten Anwender vor, so wählt das zentrale Gateway die externe Gegenstelle (Client oder Gateway) an. Die Anwahl erfolgt ohne Verbindungskosten zu verursachen direkt über ISDN mittels “Anklopfen im D-Kanal” d.h. die Rufnummer wird signalisiert. Die Gegenstelle etabliert nach erfolgreicher Überprüfung der Rufnummer selbsttätig einen VPN-Tunnel zum anrufenden Gateway (automatischer Rückruf). Nach erfolgreich durchgeführten Security-Verhandlungen können nun Daten hochsicher, End-to-End zwischen dem zentralen Gateway und dem entfernten Anwender übertragen werden.

■ Zur Konfiguration

Der Lockruf wird vom zentralen Gateway aus angestoßen, indem z.B. ein Ping an die IP-Adresse der Remote-Seite abgesetzt wird. Auf der Remote-Seite wird die im ISDN-D-Kanal signalisierte Rufnummer vom Gateway überprüft. Stimmt die gesendete Rufnummer mit der konfigurierten überein, wird ein automatischer Rückruf ausgeführt.

Die relevanten Konfigurationsparameter heißen “Rufnummer für CLI (Calling Line Identification)” und “Rückrufmodus”. Sie werden am Server Manager für ein zu definierendes Link-Profil gesetzt. Die “Rufnummer für CLI” ist ein exklusives ISDN-Leistungsmerkmal und wird im Link-Profil unter “Authentisierung” konfiguriert. Der Rückrufmodus wird im Link-Profil unter “Line-Management” eingestellt.

Dial In mit DynDNS: Firmenzentrale verfügt über keine feste IP-Adresse



Ablauf des Verbindungsaufbaus: Der feste Name (DNS-Name) des zentralen Gateways ist am DynDNS Server registriert, dem mittels eines DynDNS Clients die jeweils aktuelle IP-Adresse (vom ISP) übermittelt wird. Der DNS-Name ist auf der Remote-Seite anstatt einer IP-Adresse konfiguriert. Bei der Einwahl der Remote-Seite am ISP erfolgt eine Namensauflösung (1), womit die Remote-Seite die gerade aktuelle IP-Adresse des zentralen Gateways erhält und den VPN-Tunnel dorthin aufbauen kann (2).

7.5.2 Dynamic DNS

Da die IP-Adresse des zentralen Gateways im Beispiel nicht bekannt ist, wird mit dem Hostnamen statt einer TEP IP-Adresse gearbeitet. Der Benutzer muss lediglich im Klartext den Namen des Zielsystems eingeben, die Umsetzung in die entsprechende IP-Adresse übernimmt ein DNS-Server. Die im Internet befindlichen DNS-Server sind für alle statischen DNS-Namen (feste IP-Adressen) nicht aber für dynamische IP-Adressen vorgesehen. Für dynamische (wechselnde) IP-Adressen kommen in diesem Fall DynDNS-Server zum Einsatz.

Versucht A eine Verbindung zu einem Partner B via Internet herzustellen, kontaktiert er den zunächst den DNS Server des ISP und fragt nach der IP-Adresse von B. Ist keine feste IP-Adresse vorhanden, befragt der ISP den DynDNS-Server nach der derzeit gültigen IP-Adresse von B. Sobald er diese hat, wird sie an A übermittelt, der dann eine direkte Verbindung zu B aufbauen kann. Im Unterschied zum Lockruf muss der gewünschte Kommunikationspartner immer online sein, also über eine Flatrate verfügen, um erreichbar zu sein.

■ Zur Konfiguration

Da das VPN Gateway vom ISP bei jeder erneuten Einwahl eine andere IP-Adresse erhält, kann die eindeutige Identifikation durch den Secure Client nicht mehr über eine fest konfigurierte IP-Adresse erfolgen. Auf Seiten des Clients wird nun statt der (festen) IP-Adresse für den Tunnel-Endpunkt (siehe → Client-Telefonbuch, Tunnel-Para-

meter) der, beim DynDNS Service Provider hinterlegte Name des Gateways eingetragen (DNS Name). Der DNS-Name wird in das Feld “Tunnel-Endpunkt (Ziel)” eingetragen.

Zur Abfrage der aktuellen IP-Adresse des Gateways findet nun vor dem Tunnelaufbau vom Client zum Gateway ein DNS Request statt, über den eine Auflösung des DNS Namens erfolgt. Damit erhält der Client die jeweils aktuelle IP-Adresse des Gateways, und der Tunnelaufbau zum Gateway kann erfolgen.

Beachten Sie bitte, dass eine Verbindung vom Client zum Gateway natürlich nur stattfinden kann, solange das Gateway eine Verbindung zum Internet unterhält (z.B. über DSL Flatrate). Beachten Sie außerdem, dass eine Nutzung von DynDNS nicht möglich ist, wenn der Client für seinen Link den Microsoft RAS-Dialer nutzt (siehe → Zielsystem, Benutze Microsoft RAS-Dialer).

Konfiguration am Server: Die Verbindung vom Gateway zum ISP wird als ausgehender Link konfiguriert. Der Wert für den Parameter “DynDNS-Hostname”, der im Parameterfeld “Routing” eingegeben wird, ist der Name des Gateways, der auch bei der Registrierung des Gateways beim DynDNS Service Provider und am Client im Telefonbuch unter “Tunnel-Parameter” eingegeben wurde (z.B. test.dyndns.org; siehe unten). In der neuen Hauptgruppe des Konfigurationsbaums “DynDNS” am Server Manager wird der Zugang zum Dynamic DNS Server konfiguriert, indem dessen Server Name “Hostname DynDNS Server” (z.B. members.dyndns.org) und die Zugangsdaten, die bei der Registrierung als Benutzername (User ID) und Passwort verwendet wurden, eingegeben werden. Die Funktion “Benutze DynDNS” wird “aktiv” geschaltet.

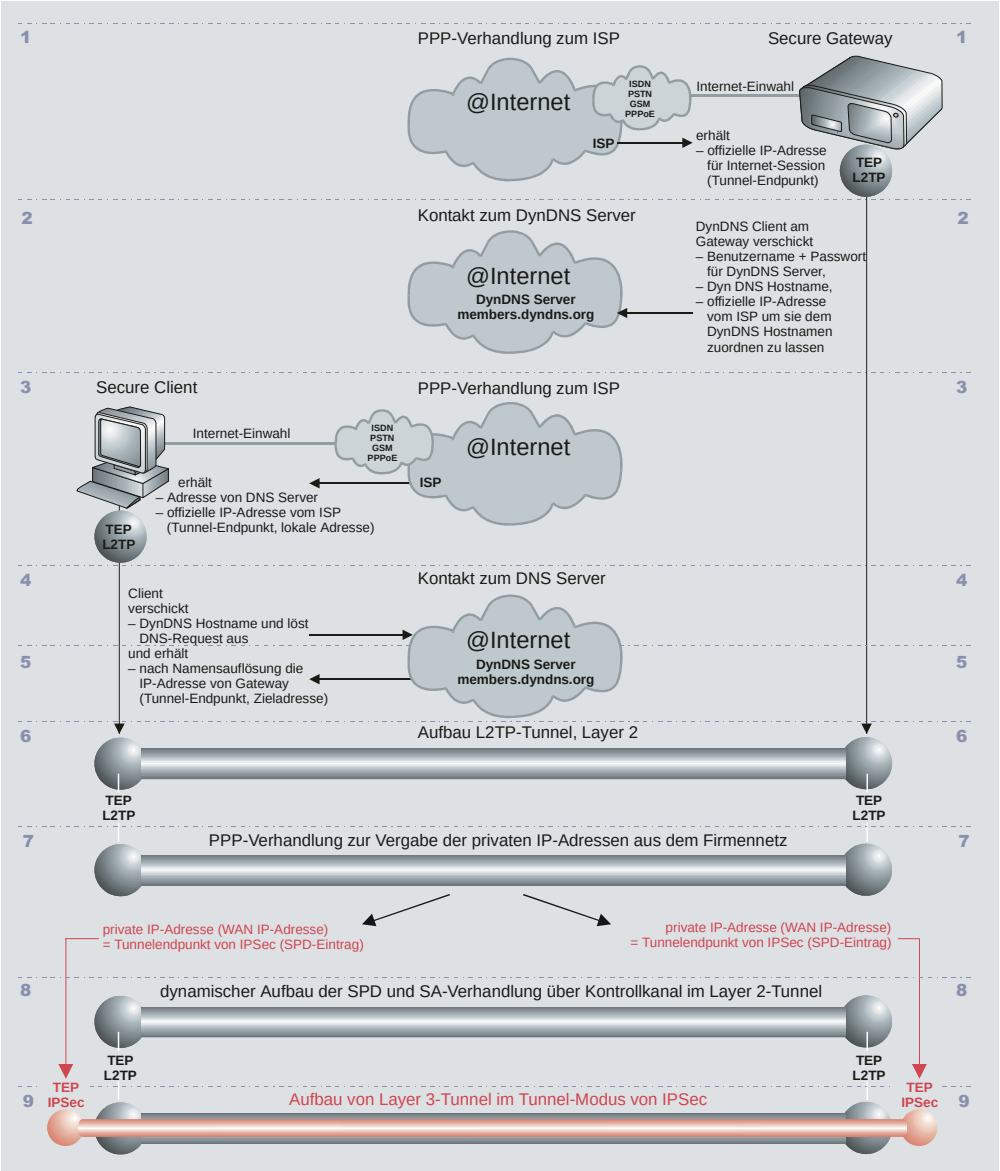
Automatische Einrichtung für den DynDNS Client: Nach den eingegebenen Werten, inklusive der vom ISP zugewiesenen IP-Adresse, wird die Batch-Datei NCPDDNS.BAT automatisch wie folgt generiert und gestartet:

```
rem the input to this batchfile is as follows
rem ncpddns members.dyndns.org test test 172.16.15.52
test.dyndns.org
rem %1 = members.dyndns.org : Name of the DDNS provider
rem %2 = test               : UserID to the DDNS provider
rem %3 = test               : Password to the DDNS provider
rem %4 = 172.16.15.52       : IPAddress to be assigned
rem %5 = test.dyndns.org    : The Name of the IPAddress above
rem The NCP DDNS client is by default called
rem 1. -h DynDNSServer
rem 2. -u UserID
rem 3. -w Password
rem 4. -i IPAddress
rem 5. -n DNSName
rem -p Port              Default HTTP:80, HTTPS:443
rem -x Proxy Ip Address  Default none
rem -y Proxy Port        Default 80
rem -s Use HTTPS

e:\win2000s\ncprtr\ncpdnscl -h %1 -u %2 -w %3 -i %4 -n %5 -s
```

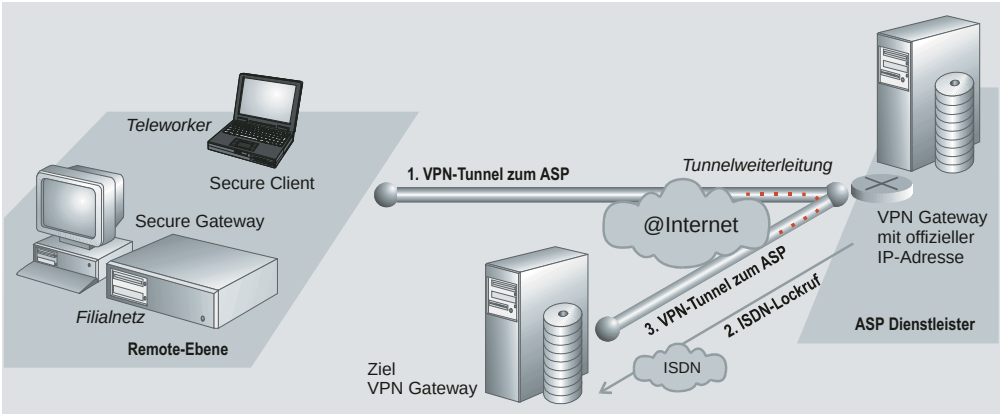
Die Batch-Datei enthält alle nötigen Parameter für den NCP-DynDNS Client. Wird ein anderer DynDNS Client verwendet, so kann die Batch-Datei abgeändert werden.

Austausch der IP-Adressen unter Einsatz von DynDNS



Bildbeschreibung:
Bereits vor der Einwahl des Clients ins Internet (Phase 3) muss sich das Ziel-Gateway im Internet eingewählt haben, um die Verhandlungen mit dem ISP und dem DynDNS Server abschließen zu können. Das heißt, nur wenn beide Teilnehmer online sind, kann auch ein erfolgreicher DNS-Request (Phase 4) mit Namensauflösung (Phase 5) stattfinden und die Verbindung vom Client zum Ziel-Gateway aufgebaut werden. Mit dem dazu etablierten L2TP-Tunnel (Phase 6) wird die sichere End-to-End-Kommunikation eingeleitet – im abgebildeten Fall mit IPSec over L2TP.

Tunnelweiterleitung (Tunnel-Forwarding) über Service Provider (ASP, MSSP)



Ablauf des Verbindungsaufbaus: Ein Benutzer aus der Remote-Ebene wählt sich beim Dienstleister über Internet ein und baut einen VPN-Tunnel zu dessen offizieller IP-Adresse auf (1). Das VPN Gateway des Dienstleisters erkennt die Zugehörigkeit des Remote-Teilnehmers zu einer vorkonfigurierten Domain-Gruppe und setzt einen Lockruf via ISDN an das zu dieser Gruppe gehörige Ziel-Gateway ab (2). Vom Ziel-Gateway wird daraufhin ein Rückruf (Callback) über das Internet an den Dienstleister ausgeführt und damit ein Tunnel zu dessen fester IP-Adresse aufgebaut (3). Damit ist eine Tunnelweiterleitung von der Remote-Ebene zum Ziel-Gateway hergestellt.

7.5.3 Managed VPNs

Eine Alternative zu selbstunterhaltenen VPNs bilden so genannte “Managed VPNs”, bei denen Einrichtung, Betrieb und Administration der kompletten VPN-Security durch einen Dienstleister erbracht wird. Diese Managed Security Service Provider (MSSP) oder Application Service Provider (ASP) bilden quasi eine Relaisstation zwischen den entfernten Anwendern und der Firmenzentrale. MSSPs verfügen immer über eine feste IP-Adresse und sind demzufolge standardmäßig erreichbar. Die Verbindungen werden sowohl bei Remote Access als auch bei Dial Outs mittels der Lockruf-Funktionalität durch den MSSP etabliert.

Versucht A eine Verbindung zu einem Partner B via Internet herzustellen, wählt er das Gateway den MSSP an. Dieses erkennt den Verbindungswunsch und aktiviert mittels Lockruf den Aufbau des VPN Tunnels von Partner B zum MSSP. Nunmehr kann Partner A und B über den weitergeleiteten Tunnel (Tunnel-Forwarding) kommunizieren.

■ Zur Konfiguration

Datenpakete von Mitgliedern einer Domain-Gruppe können vom zentralen VPN Gateway, das bei einem Application Service Provider betrieben wird, über Tunnel an das entfernte Ziel-Gateway weitergeleitet werden. Dazu wird für die entsprechende Domain-Gruppe im Parameterfeld “Allgemein” ein jeweils zu konfigurierendes Link-Pro-

fil für eine ausgehende Verbindung zugeordnet, über welches der Tunnel zum gewünschten Ziel-Gateway hergestellt (bzw. initiiert) wird.

Verfügt das Ziel-Gateway nicht über eine feste IP-Adresse, so erfolgt via ISDN vom ASP Gateway ein Lockruf an das Ziel-Gateway, womit ein Tunnelaufbau vom Ziel-Gateway zum ASP initiiert wird.

7.5.4 Szenarien in Internet-VPNs

Differenzierungskriterien für die Nutzung der Leistungsmerkmale:
– Anschlusslage der Kommunikationspartner: Wählleitung oder Festverbindung
– Kommunikationsrichtung : Remote Access (Dial In) und/oder Dial Out

Art / öffentl. Netze	Teleworker / Filiale	Firmenzentrale	Bemerkungen
Dial In	Einwahl in das Firmennetz		
Dial In	ISDN	ISDN/Flatrate	DynDNS
Dial In	ISDN	ADSL/Flatrate	DynDNS
Dial In	ADSL	ADSL/Flatrate	DynDNS
Dial In	Modem	ISDN/ADSL/Flatrate	DynDNS
Dial In	GSM, GPRS, WLAN	ISDN/ADSL/Flatrate	DynDNS
Dial In / Dial Out	Auswahl aus dem Firmennetz / Einwahl in das Firmennetz		
Dial In / Dial Out	ISDN	Festverbindung	Lockruf
Dial In / Dial Out	ADSL	Festverbindung	Lockruf
Dial In / Dial Out	ISDN	ISDN/Flatrate	DynDNS/Lockruf
Dial In / Dial Out	ISDN	ADSL/Flatrate	DynDNS/Lockruf
Dial In / Dial Out	Managed Security Services durch Dienstanbieter		

7.5 Rückruf

Im folgenden sind die wichtigen Parameter im Telefonbuch des Secure Client beschrieben. Die entsprechenden Einstellungen für den Secure Server Manager entnehmen Sie bitte dem Handbuch zum Secure Server.

7.5.1 Rückruf des Zielsystems an den Secure Client

Der Secure Client wird wie folgt konfiguriert:

- **Parameterfeld Netzeinwahl**

Benutzer = erhalten Sie vom Administrator. Wird für die Authentisierung bei der Anwahl der Secure Client benötigt. Ist im Secure Server als „Remote User ID" gespeichert.

Passwort = erhalten Sie vom Administrator. Wird für die Authentisierung bei der Anwahl der Secure Client benötigt. Ist im Secure Server als „Remote Password" gespeichert.

Rufnummer Ziel = erhalten Sie vom Administrator. Ohne korrekte Rufnummer ist keine Anwahl der Secure Client möglich. Ist im Secure Server als „Controllers/Controllern (Phone Number)" gespeichert.

Fester Rückruf

Wenn Sie beispielsweise als Teleworker von zuhause aus tätig sind und das Zielsystem, mit dem Sie kommunizieren, immer einen Rückruf an dieselbe Rufnummer ausführen soll (feste Rufnummer), brauchen Sie im Telefonbuch keine weiteren Eintragungen für den Rückruf vorzunehmen. Auf Seiten des Secure Servers muss für diese Rufnummer und Ihre User-ID und Passwort "Fester Rückruf" definiert sein.

Variabler Rückruf

Wenn Sie mit dem Secure Client mobil sind und an den verschiedensten Aufenthaltorten vom Zielsystem zurückgerufen werden wollen, so müssen Sie folgende Parameter im Telefonbuch definieren:

- **Parameterfeld Rückruf**

Verhandle PPP Callback = aktiv (Wenn Secure Server PPP(B-Channel)-Rückruf macht). In diesem Fall kann in das Feld "Rückrufnummer" ein Eintrag gemacht werden. Tragen Sie die Rufnummer in das Feld ein, unter der Sie gerade erreichbar sind.

Achten Sie bitte darauf die Rufnummer mit allen nötigen Vorwahlnummern einzugeben.

Rückrufmodi

COSO = (Charge-One-Side-Only) auch Low-Level- oder D-Kanal-Rückruf. Diese Methode kann nur im ISDN angewendet werden. Wenn die Secure Client einen Rückruf im ISDN D-Kanal initiiert, prüft der NCP Secure Server die im D-Kanal übermittelte Rufnummer. Wenn Sie als COSO-Rückrufnummer registriert ist, wird der Rückruf an diese ISDN-Nummer ausgeführt. Dies bedeutet, dass keinerlei Gebühren für die Workstation anfallen. COSO ist auch Cisco-kompatibel.

PPP = Diese Rückrufmethode kann in jedem Wählnetz genutzt werden (z.B. PSTN, ISDN, GSM). PPP-Rückruf wird für den variablen Rückruf genutzt. In diesem Fall für die Secure Client zunächst einen Ruf an den Secure Server aus, mit dem der Rückruf initiiert wird. Nachdem die Authentisierung erfolgreich verlaufen ist, wird die Secure Client vom NCP Secure Server (oder einem anderen NAS, der PPP-Rückruf unterstützt) an der Rückrufnummer, die im Parameterfeld “Rückruf” eingegeben wurde, zurück gerufen.

7.5.2 Rückruf des Secure Client an das Zielsystem

Es ist auch möglich, dass die Secure Client einen Rückruf an ein Zielsystem ausführt. Dazu konfigurieren Sie die Secure Client wie folgt:

- **Parameterfeld Rückruf**

Unter “Rückruf für eingehende Verbindungen” wählen Sie den Rückrufmodus aus, der auch vom Zielsystem unterstützt wird.

- **Parameterfeld Eingehende Rufe**

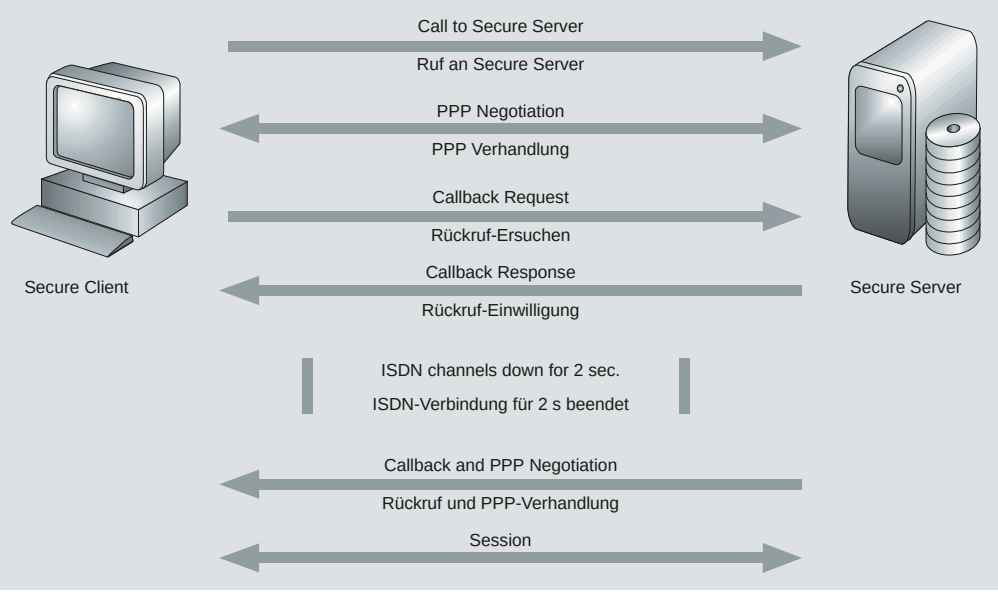
“Benutzer lokal” und “Passwort lokal”, die Sie hier angeben, müssen Sie dem Administrator des Zielsystems mitteilen, da sich das Zielsystem mit ihnen authentisiert.

Die eigene Rufnummer der Secure Client muss als „Rufnummer lokal” eingetragen sein, wenn mehrere ISDN-Geräte den gleichen Anschluss nutzen. In diesem Fall handelt es sich um die MSN des Secure Client. Sie entspricht der „CLI Rufnummer”, wenn Coso-Rückruf vom Secure Server stattfindet.)

“Gegenseitige Authentisierung” aktivieren Sie nur, wenn erforderlich. Nicht aktiviert bedeutet, dass sich nur das Zielsystem authetisieren muss.

Unter “Richtung” wählen Sie “eingehend” oder “bidirektional”.

Ablauf der Callback-Funktion



7.6 Parallele Verbindungen ins Internet und zu einem VPN IP-Netz

Der Secure Client unterscheidet die Art der Verbindung anhand der verwendeten „offiziellen" IP-Adressen.

1 Konfigurieren Sie ein Ziel zu Ihrem ISP im Telefonbuch des Secure Client (z.B. „Internet1"). Achten Sie darauf, dass IP Network Address Translation aktiv ist.

Führen Sie anschließend folgenden Test durch, um zu sehen ob zusätzlich ein VPN-Tunnel aufgebaut werden kann: Öffnen Sie eine DOS-Box und pingen Sie das VPN-Gateway an. Bitte beachten Sie dabei, dass das VPN-Gateway nicht antworten kann, wenn der Zugang durch eine Firewall geschützt ist, dass VPN-Datenströme aber dennoch das VPN-Gateway erreichen können.

2 Um zusätzlich zum ISP einen VPN-Tunnel zu einem IP-Netz (VPN IP-Netz) aufbauen zu können, werden zu den oben konfigurierten Parametern des Ziels „Internet1" in den folgenden Parameterfeldern weitere Einstellungen vorgenommen:

- **Parameterfeld Tunnel-Parameter**

VPN-Protokoll	=	L2TP
Benutzer (VPN)	=	(abgestimmt mit Administrator)
Passwort (VPN)	=	(abgestimmt mit Administrator)
Tunnel Secret	=	(abgestimmt mit Administrator)
Tunnel IP-Adr. (Ziel)	=	"offizielle" IP-Adresse des VPN Gateways
Tunnel IP-Adr. (lokal)	=	leer

- **Parameterfeld VPN IP-Netze**

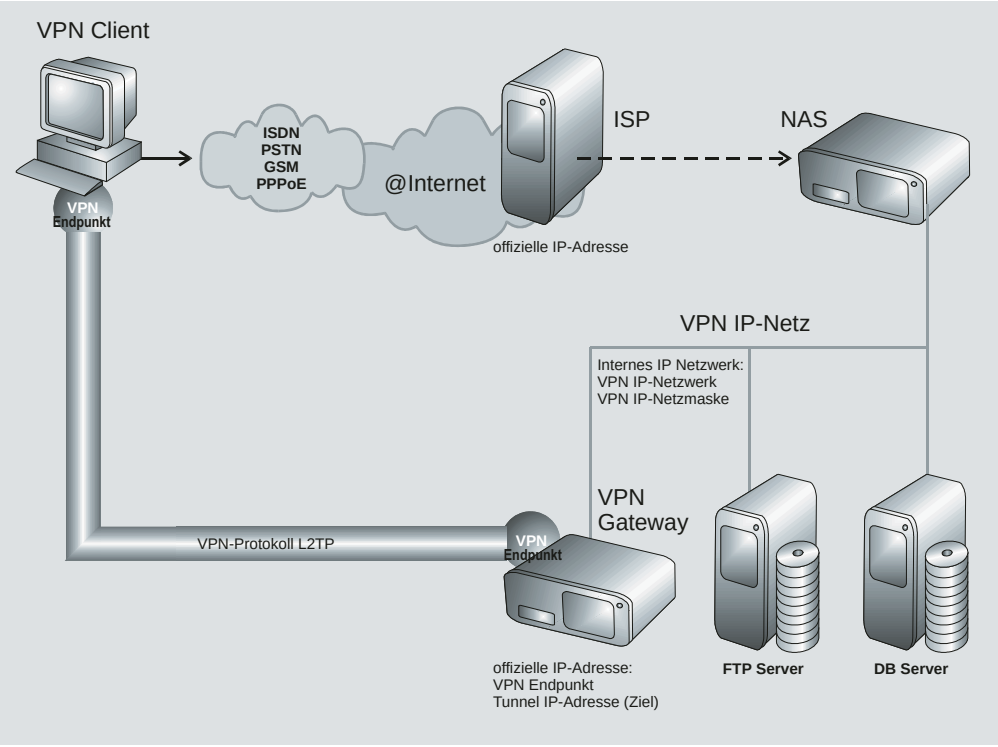
VPN IP-Netzwerk	=	firmeninterne IP-Adresse des IP-Netzes (nur zu dem hier eingetragenen Netz oder Netzen wird ein Tunnel aufgebaut. Ist keine Netzadresse eingetragen, so wird immer zum VPN-Gateway über Tunnel übertragen, sobald für dieses Ziel Tunneling aktiviert ist. D.h. in diesem Fall würde die Verbindung zum ISP über Tunnel und NAS aufgebaut werden, gestrichelte Linie)
VPN IP-Netzmaske	=	IP-Adresse der Netzmaske

Bitte achten Sie darauf, dass die offizielle Internet IP-Adresse nicht im Bereich der internen Firmenadressen liegt.

3 Die Verbindung zum Ziel „Internet1" wird über den Secure Client hergestellt.

4 Anwendung für das VPN IP-Netz (z.B. E-Mail oder Datenbank-Recherche) wird gestartet.

Parallele Verbindungen ins Internet und zu einem VPN IP-Netz



7.8 Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am Secure Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

7.8.1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Windows-Verzeichnis \ncple\cacerts\ gespielt. Das Einspielen kann bei einer Software-Distribution mit Disketten automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software im Root-Verzeichnis der ersten Diskette befinden. Nachträglich können Aussteller-Zertifikate automatisch über den Secure Update Server verteilt werden (siehe → Handbuch zum Update Server), oder – sofern der Benutzer über die notwendigen Schreibrechte in genanntem Verzeichnis verfügt von diesem selbst eingestellt werden (siehe → CA-Zertifikate anzeigen).

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung – Zertifikate – CA-Zertifikate anzeigen” eingesehen werden.

Wird am Secure Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der NCP Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis NCPLE\CA-CERTS\. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

7.8.2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben. Für den Secure Client und den Secure Server sind drei Erweiterungen von Bedeutung:

– KeyUsage
– extendedKeyUsage
– subjectKeyIdentifier
– authorityKeyIdentifier
– CDP (Certificate Distribution Point)

- **KeyUsage**

Ist in einen eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:
– Digital Signatur
– Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
– Key Aggrenment (Schlüsselaustaschverfahren)
Ist eines des Bits nicht gesetzt, wird die Verbindung abgebaut.

- **extendedKeyUsage**

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Secure Client, ob der definierte erweiterte Verwendungszweck “SSL-Server-Authentisierung” enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

Ausnahme: Bei einem Rückruf des Servers an den Client nach einer Direkteinwahl ohne VPN aber mit PKI prüft der Server das Zertifikat des Clients auf die Erweiterung extendedKeyUsage. Ist diese vorhanden, muss der Verwendungszweck “SSL-Server-Authentisierung” beinhaltet sein, sonst wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

- **subjectKeyIdentifier / authorityKeyIdentifier**

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades. (Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

- **CDP (Certificate Distribution Point)**

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festge-

stellt, dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Verzeichniss ncple\crls gespeichert.

7.8.3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem Secure Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Windows-Verzeichnis \ncple\crls\ gespielt. Ist eine CRL vorhanden, so überprüft der Secure Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Windows-Verzeichnis \ncple\arls\ gespielt werden muss.

Sind eingehende Zertifikate in den Listen von CRL oder ARL enthalten, wird die Verbindung nicht zugelassen. Sind CRLs oder ARLs nicht vorhanden findet keine diesbezügliche Überprüfung statt.

7.9 Stateful Inspection-Technologie für die Firewall-Einstellungen

Die Firewall-Technologie der Stateful Inspection kann für alle Netzwerkadapter wie auch für RAS-Verbindungen eingesetzt werden. Sie wird am Client im Telefonbuch unter “Firewall-Einstellungen” aktiviert (siehe → Konfigurations-Parameter, Firewall-Einstellungen). Am Gateway ist sie dann aktiv, wenn im Server Manager unter “Routing Interfaces – Allgemein” die Funktion “LAN-Adapter schützen” eingeschaltet wird.

Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und z.B. Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ab ein Datenpaket durchgelassen wird oder nicht.

Stateful Inspection ist die Firewall-Technologie, die den derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz bietet. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung “Tochterverbindungen” geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf. Alternative Bezeichnungen für Stateful Inspection sind: Stateful Packet Filter, Dynamic Packet Filter, Smart Filtering, Adaptive Screening.

Stateful Inspection vereinigt konzeptionell die Schutzmöglichkeiten von Packet Filter und Application Level Gateways d.h. sie integriert als Hybrid die Funktionen beider Security-Verfahren und arbeitet sowohl auf der Netz- als auch Anwenderschicht. Bei der “zustandsabhängigen Paket-Filterung” werden nicht nur die Internet- und Transportschicht sondern auch Abhängigkeiten vom Zustand einer Verbindung berücksichtigt. Alle aktuellen und initiierten Verbindungen werden mit Adresse und zugeordnetem Port in einer dynamischen Verbindungstabelle hinterlegt. Der Stateful Inspection-Filter entscheidet anhand festgelegter Raster (Informationen), welche Pakete zu welcher Verbindung gehören. Zustände können sein: Verbindungsaufbau, Übertragung, Verbindungsabbau und gelten sowohl für TCP- als auch UDP-Verbindungen. Ein Beispiel an einer Telnet-Sitzung: Der Zustand “Verbindungsaufbau” wird dadurch definiert, dass noch keine Benutzer-Authentisierung stattgefunden hat. Hat der Benutzer sich mit Benutzername und Kennwort angemeldet, wird diese Verbindung in den Zustand “normale Verbindung” gesetzt. Da der jeweilige Status einer Verbindung ständig überwacht wird, bleibt Unbefugten der Zugriff auf das interne Unternehmensnetz verwehrt.

Der Vorteil gegenüber statischen Paketfiltern ist, dass die Entscheidung, ob ein NCP Secure Gateway oder Client ein Paket weiterleitet oder nicht, nicht nur auf Grund von Quell- und Zieladresse oder Ports fällt. Das Security-Management prüft darüber hinaus

den Zustand (state) der Verbindung zu einem Partner. Weitergeleitet werden ausschließlich die Pakete, die zu einer aktiven Verbindung gehören. Datenpakete, die sich keiner etablierten Verbindung zuordnen lassen, werden verworfen und im Log-File protokolliert. Neue Verbindungen lassen sich nur entsprechend der konfigurierten Regeln öffnen.

In der einfachsten Firewall-Funktion werden nur die ein- und ausgehenden Verbindungen im Hinblick auf das Protokoll (TCP/IP, UDP/IP, ICMP, IPX/SPX), die entsprechenden Ports und die beteiligten Rechner überprüft und überwacht. Verbindungen werden in Abhängigkeit eines festgelegten Regelwerkes erlaubt oder gesperrt. Weitere Prüfungen (z.B. Inhalt der übertragenen Daten) finden nicht statt.

Die Stateful Inspection Filter sind eine Weiterentwicklung der dynamischen Packet-Filter und bieten eine komplexere Logik. Die Firewall prüft, ob eine am Portfilter erlaubte Verbindung auch zu dem definierten Zweck aufgebaut wird.

Es werden folgende zusätzliche Informationen zu einer Verbindung verwaltet:

– Nr. zur Identifizierung einer Verbindung
– Zustand der Verbindung (z.B. Aufbau, Datenübertragung, Abbau)
– Quell-Adresse des ersten Pakets
– Ziel-Adresse des ersten Pakets
– Interface, durch welches das erste Paket kam
– Interface, durch welches das erste Paket verschickt wurde

Anhand dieser Informationen kann der Filter entscheiden, welche nachfolgenden Pakete zu welcher Verbindung gehören. So kann ein Stateful Inspection-System auch das UDP-Problem ausschalten. Hintergrund ist die verhältnismäßig leichte Fälschbarkeit von UDP-Paketen z.B. beim UDP-basierten Dienst DNS. Da Stateful Inspection-Filter in der Lage sind, sich die aktuelle Status- und Kontextinformation einer Kommunikationsbeziehung zu merken, ist es erforderlich, dass neben der Quell- und Zieladresse sowie Quell- und Zielport, auch der DNS-Header im Anfrage-Paket in die Speicherung der Status- und Kontextinformation einbezogen wird. Es erfolgt eine Interpretation auf der Anwendungsschicht.

Beispiel: Eine gehenden Verbindung zum Port 21 eines Rechners ist für einen reinen Portfilter eine FTP-Verbindung. Eine weitere Überprüfung findet nicht statt. Der Stateful Inspection-Filter prüft zusätzlich, ob die über diese Verbindung übertragenen Daten zu einer etablierten FTP-Verbindung gehören. Wenn nicht, wird die Verbindung sofort unterbrochen. Weiter ist ein Stateful Inspection-Filter in der Lage, Regeln in Abhängigkeit von notwendigen Kommunikationsprozessen anzupassen. Wenn z.B. eine abgehende FTP-Verbindung erlaubt ist, so ermöglicht die Firewall auch automatisch die Etablierung des zugehörigen Rückkanals. Die entsprechenden Informationen (Ports) werden aus der Kontrollverbindung herausgelesen.

Ein vorteilhafter Aspekt von Stateful Inspection-Filtern ist die Fähigkeit, die Daten auf allen Protokollebenen (d.h. von Netzwerk- bis Anwendungsebene) zu prüfen. So kann z.B. ein FTP-GET erlaubt, ein FTP-PUT jedoch verboten werden. Ein positiver Effekt der im Vergleich zu konventionellen Paketfiltern erhöhten Eigenintelligenz ist die Op-

tion, einzelne Pakete während einer Kommunikationsbeziehung zu assemblieren und damit erweiterte Möglichkeiten zur Benutzer-Authentisierung zur Anwendung zu bringen. Als Folge der nicht verlässlichen Trennung der Netzwerksegmente sind Stateful Inspection-Filter nicht immun gegen bestimmte auf unteren Protokollebenen stattfindende Angriffe. So z.B. werden fragmentierte Pakete i.d.R. von außen nach innen ohne weitere Prüfung durchgelassen.

Diese Seite ist frei →

© NCP engineering GmbH

8. Abkürzungen und Begriffe

3DES	TripleDES. Verschlüsselungsstandard mit 112 Bit.
AES	Advanced Encryption Standard. Europäische Entwicklung der belgischen Verschlüsselungsexperten Joan Daemen und Vincent Rijmen (“Rijndael-Algorithmus”). Nachfolger von DES (Data Encryption Standard). Verschlüsselungsalgorithmus, der bis zu 256 Bit Schlüssellänge besitzt. n hoch 256 gilt als Maßeinheit für die mögliche Anzahl der Schlüssel, die mit diesem Algorithmus generiert werden können. Trotz steigender Prozessorgeschwindigkeiten wird erwartet, dass der AES-Algorithmus eine akzeptable Sicherheit für die nächsten 30 Jahre bietet. Wird in VPN- und SSL-Verschlüsselungen bald große Verbreitung finden.
AH	Authentication Header RFC 2402
Asymmetrische Verschlüsselung	(Public-Key-Verfahren) Bei einer asymmetrischen Verschlüsselung besitzt jeder Teilnehmer zwei Schlüssel: einen geheimen, privaten und einen öffentlichen Schlüssel. Beide Schlüssel stehen in einer mathematisch definierten Beziehung zueinander. Der private Schlüssel des Teilnehmer ist streng geheim, der öffentliche Schlüssel für jedermann zugänglich. Das Schlüsselmanagement gestaltet sich auch bei großen Teilnehmerzahlen überschaubar: Zwei Schlüssel pro Teilnehmer – ergibt insgesamt 2.000 Schlüssel, um 1.000 Teilnehmern in allen Sender-Empfänger-Kombinationen die sichere Kommunikation zu ermöglichen. Das bekannteste asymmetrische Verschlüsselungsverfahren ist RSA. Nachteil der asymmetrischen Verfahren: Sie sind rechenintensiv und damit vergleichsweise langsam.

Basisanschluss (So / BRI = Basic Rate Interface)
ISDN-Anschlusstyp mit So-Schnittstelle (“S” für Subscriber Interface: Benutzerschnittstelle), bestehend aus einem D-Kanal (Bandbreite: 16 kBit/s) für die Steuerung und zwei B-Kanälen (Bandbreite jeweils 64 kBit/s) für die Übertragung von Nutzinformationen.

BCP
Bridge Control Protocol

BITS
Bump In The Stack. Art der Implementierung von IPsec.

BITW
Bump In The Wire. Art der Implementierung von IPsec.

Blowfish
Verschlüsselungsstandard mit 128/448 Bit

BRI
Basic Rate Interface (ISDN-Schnittstelle, Basis So) mit 2 B-Kanälen und 1 D-Kanal.

Browser
Der Browser stellt die Anwender-Schnittstelle zum Internet dar. Mit seiner HTTP-Fähigkeit (Hypertext-Transfer-Protokoll) kann er verschiedene Formate (z.B. HTML, GIF, CAD), die für eine multimediale Darstellung der Information benötigt werden, in Sound und Grafik umsetzen.

CA
Certification Authority, auch Trust Center (z.B. D-Trust, ein Gemeinschaftsunternehmen der Bundesdruckerei und Debis). Eine CA stellt mittels PKI-Manager (Software) digital signierte Bestätigungen (Zertifikate) aus und brennt sie auf eine Smartcard (Chipkarte). Eine CA kann ein privater Dienstleister oder eine öffentiche Einrichtung sein. Diese Zertifizierungsstellen bedürfen nicht der Genehmigung durch den Staat. Sie haften für die Richtigkeit der Zertifikate.

CAPI
Common Application Programm Interface. Diese Schnittstelle wird im ISDN als Common ISDN API bezeichnet und entspricht der PCI-Schnittstelle (Programmable Communication Interface). Die Schnittstelle erlaubt den direkten Zugang zum ISDN und den unteren Protokoll-schichten (Ebene 1-3). Höhere Protokolle (Anwendungen) wie Telex oder Filetransfer können unabhängig von der eingesetzten Hardware-Plattform verwendet werden. Die CAPI gibt es in zwei Versionen, 1.1 und 2.0.

	Entsprechend sind auch dieISDN-Anwendungsprogramme programmiert, die entweder auf CAPI 1.1 oder CAPI 2.0 aufsetzen, bzw. die jeweilige CAPI voraussetzen. Eine Hybrid-CAPI gestattet sowohl den Einsatz einer Anwendungs-Software für CAPI 1.1 als auch den von CAPI 2.0-Software. (Siehe Hybrid-CAPI)
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Identification (Rufnummern-Identifizierung im Euro-ISDN)
COSO	Charge One Side Only. COSO-Rückruf, auch Low Level- oder D-Kanal Rückruf. Für den Initiator des Rückrufs im D-Kanal fallen keine Gebühren an.
CTAPI	Schnittstelle zu Smartcard Readern
CUG	Closed User Group (geschlossene Benutzergruppe im Euro-ISDN)
DES	Datenverschlüsselungsnorm, Data Encryption Standard
DHCP	Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass für jede Session automatisch eine IP-Adresse zugewiesen wird.
Directory Service	Remote Access-Zugänge werden wie E-Mail-Adressen, Telefonnummern etc. in Verzeichnissen auf unterschiedlichen Datenbanken abgelegt. Das Problem bei dieser Vielzahl von Verzeichnissen ist, dass einerseits viele Daten mehrfach erfasst werden und zudem die einzelnen Einträge nicht untereinander verknüpft sind. Der Pflegeaufwand ist enorm und Inkonsistenzen sind nicht auszuschließen. Gefordert ist ein standardisiertes Prozedere, mit Hilfe dessen die Erfassung und Pflege aller Informationen in einer zentralen Directory ermöglicht wird. Das T-Online Security Management unterstützt die standardisierten Protokolle Radius (Remote Authorization Dial In User Service) und LDAP (Lightweight Directory Access Protocol), wobei letztere den Zugriff auf zentralisierte Verzeichnisdienste gewährleistet.

DMZ Demilitarisierte Zone, zwischen Firewall und Unternehmensnetz, zum Beispiel mit Web-, Email- und VPN-Server.

DNS Der Domain Name Server (DNS) stellt die IP-Adresse für eine Internet-Sitzung zur Verfügung, nachdem die Anwahl mit Benutzername und Passwort erfolgte. Er routet weiter im Internet, indem er die Namen, die im Browser als gewünschtes Ziel angegeben werden, in IP-Adressen rückübersetzt und die Verbindung zu dieser Adresse herstellt.

D-Kanal-Protokoll Das D-Kanal-Protokoll sorgt dafür, dass sich Endgeräte mit dem Netz verständigen können. Es steuert unter anderem Verbindungsauf- und abbau. Es umfasst Schicht 2 und 3. Auf Schicht 2 von ISDN ist HDLC für die logische Datenübertragungssteuerung eingesetzt. Das eigentliche D-Kanal-Protokoll ist auf Schicht 3 angesiedelt. Mittlerweile ist DSS1 als europaweites D-Kanal-Protokoll verfügbar.

DSA Directory System Agent

DSS1 European Digital Subscriber System No. 1. Europäisches ISDN-Protokoll für den D-Kanal.

DUA Directory User Agent

ECP Encryption Control Protocol

ESP Encapsulating Security Payload RFC 2406

Euro-ISDN ITU-Standard für Europäisches ISDN; bezieht sich auf das D-Kanal-Protokoll DSS1 und mögliche Dienstmerkmale, wie Gebührenanzeige (Advice of Charge), Rückruf bei Besetzt (Completion of Calls to Busy Subscriber), Rufumleitung (Call Forwarding), Anklopfen (Call Waiting), etc. Im Euro-ISDN mit dem D-Kanal-Protokoll DSS1 werden einzelne Endgeräte mit der Multible Subscriber Number (MSN) adressiert.

Firewall Trennt Public-Netz von Private-Netz. Schutzmechanismus in Netzen, der den Zugriff der Stationen regelt. Ein Firewall-Rechner schottet ein Netz-

	werk vor allem WAN-seitig gegen unautorisierten Zugriff ab. Die Berechtigung kommender und abgehender Verbindungen wird zum Beispiel geregelt durch Herausfiltern bestimmter Netzteilnehmer und Netzdienste und Festlegung der Zugriffsberechtigungen. Vom WAN aus betrachtet stehen hinter der Firewall (in der DMZ) für gewöhnlich Web-Server, Email-Server und VPN-Server.
FTP	File Transfer Protocol. Basiert auf TCP und dem Terminalprotokoll TELNET (Port 21).
GPRS	Standard für schnelle Handy-Kommunikation
GRE	Generic Router Encapsulation. CISO-Spezifisches Tunnel-Protokoll.
GSM	Global System Mobile. Standard für Handy-Kommunikation
Hash-Wert	siehe Signatur
HBCI	Standard für Smartcard Reader (Online Banking)
HTTP	Hypertext Transfer Protocol. Multimedia-Network im Internet (Port 80)
Hybride Verschlüsselung	Hohe Performance plus viel Sicherheit: Hybride Verschlüsselung vereint die Vorteile symmetrischer und asymmetrischer Verfahren. Während die Inhalte der Kommunikation mit schnellen symmetrischen Algorithmen gesichert werden, erfolgen Authentisierung der Teilnehmer und Schlüsselaustausch auf Basis asymmetrischer Verfahren. Die eigentliche Verschlüsselung der Daten eines Dokuments geschieht auf Basis einer Zufallszahl (Session-Key), die für jede einzelne Kommunikationsverbindung neu erzeugt wird. Dieser Einmalschlüssel wird mit dem öffentlichen Schlüssel des Empfängers chiffriert und der Nachricht beigefügt. Der Empfänger wiederum rekonstruiert mit seinem privaten Schlüssel den Session-Key und entschlüsselt die Nachricht.
IETF	Internet Engineering Task Force. Interessengemeinschaft, die sich mit Problemen des TCP/IP und dem Internet befasst, unter anderem den Well Known Ports (Ports 0 bis 1023).

IKE

Internet Key Exchange. Bestandteil von IPsec für sicheres Schlüssel-Management. Separate security association negotiation and key management protocol RFC 2409

Internet

Das Internet ist ein weltweites, offenes Rechnernetz. Es ist allgemein zugänglich. Jeder Betrieb und jede Privatperson kann sich daran anschließen und mit allen anderen angeschlossenen Benutzern kommunizieren, unabhängig von der eingesetzten Rechnerplattform oder der jeweiligen Netztopologie. Damit der Datenaustausch zwischen den unterschiedlichen Rechnern und Netzen innerhalb des Internets möglich wird, ist ein allen gemeinsames Netzwerkprotokoll nötig. (siehe TCP/IP)

IP-Adresse

Jeder Rechner im Internet besitzt für die Dauer seiner Zugehörigkeit zum Internet eine IP-Adresse (Internet-Protokoll-Adresse), die ihn eindeutig identifiziert. Eine IP-Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen. Für jede Zahl stehen 8 Bits zur Verfügung, womit sie 256 Werte annehmen kann. Die Anzahl der möglichen IP-Adressen insgesamt bleibt jedoch begrenzt. Der Internet-User bekommt daher nicht einmalig eine unveränderliche IP-Adresse zugeteilt, sondern für jede seiner Sessions die IP-Adresse, die gerade noch nicht vergeben ist. Die IP-Adressen werden also für die Dauer eines Zeitschlitzes zugeteilt. Diese Adress-Zuteilung er-folgt im Regelfall automatisch per PPP-Verhandlung über DHCP. Die IP-Adresse kann von speziellen Programmen in einen Namen übersetzt werden. Diese Programme laufen auf einem Domain Name Server (DNS).

IP Network Address Translation

(IP Network Address Translation wird bei der Installation der Workstation Software bereits vorgesehen und ist standardmäßig beim Anlegen eines neues Zielsystems aktiviert!) Wenn IP Network Address Translation verwendet wird, werden alle übertragenen Frames mit der ausgehandelten (PPP) IP-Adresse verschickt. Die Workstation Software übersetzt diese öffentliche IP-Adresse in die systemeigene des Intranets oder, im Falle der Workstation, in deren eigene vom Benutzer festgelegte. Allgemein: Über NAT ist es möglich, in einem LAN mit inoffiziellen IP-Adressen, die nicht

© NCP engineering GmbH

	im Internet gültig sind, zu arbeiten und trotzdem vom LAN aus auf das Internet zuzugreifen. Dazu werden die inoffiziellen IP-Adressen von der Software in offizielle IP-Adressen übersetzt. Dies spart zum einen ofizielle IP-Adressen, die nicht in unbegrenzter Anzahl zur Verfügung stehen. Zum anderen wird damit ein gewisser Schutz (Firewall) für das LAN aufgebaut.
IPCP	Internet Protocol Control Protocol
IPsec	Standards festgelegt von IETF: RFCs 2401-2412 (12/98)
IPX	Internet Packet Exchange, Netware-Protokoll von Novell
IPXCP	Internetwork Packet Exchange Control Protocol
ISDN	Integrated Services Digital Network. Dienste-integrierendes digitales Fernmeldenetz. Digitales Netz mit Integration aller Schmalband-Kommunikationsdienste (z.B. Fernsprechen, Telex, Telefax, Teletext, Bildschirmtext), bestehend aus Kanälen mit einer Übertragungsgeschwindigkeit von 64.000 bit/s. Ein Basisanschluss im sogenannten Schmalband-ISDN besitzt drei Übertragungskanäle:Kanal B1: 64.000 bit/sKanal B2: 64.000 bit/sKanal D: 16.000 bit/sDie Gesamtübertragungsrate beträgt 144.000 bit/s. Dieses Netz soll bis zum Ende dieses Jahrtausends europaweit einheitlich aufgebaut werden. Die Spezifikationen hierfür werden von ITU und CEPT erarbeitet.
ISDN-Adapter	ISDN-Adapter ermöglichen den Anschluss von vorhandenen, nicht ISDN-fähigen Endgeräten an das ISDN. Der Adapter übernimmt dabei die sowohl soft- als auch hardwaremäßige Anpassung der Endgeräteschnittstelle an die ISDN-Schnittstelle (So). Ein ISDN-Adapter mit Upo-Schnittstelle ermöglicht an ISDN TK-Anlagen die Umsetzung der ISDN-Zweidraht-Schnittstelle Upo (Reichweite ca. 3,5km) auf die busfähige ISDN-Vierdraht-Schnittstelle So (Reichweite ca. 150m) nach den Richtlinien der Telekom.
ISP	Internet Service Provider

Kryptographie	Anwendungen sind Verschlüsselung, elektronische Signatur, Authentifikation und Hash-Wert-Berechnung. Mathematische Verfahren, die mit Schlüssel verwendet werden.
L2TP	Tunnel- bzw. VPN-Protokoll Layer 2 Tunneling Protocol
L2Sec	IPSec im Layer-2-Tunnel, funktional im RFC 2716 beschrieben
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol, siehe Directory Service
MAC-Adresse	Medium Access Control Layer-Adresse. Physikalische Adresse im Netzwerk.
MIB	Management Information Base. Beschreibt die Struktur der Managementinformationen beim SNMP.
MD5	Message Digit 5. Verfahren zur Bildung eines Hash-Werts
Name	Namen, genauer Internet-Namen, sollen den Benutzern des Internets die Arbeit erleichtern. Im Internet Browser werden die Namen eingetragen, die dann vom Domain Name Server (DNS) in IP-Adressen übersetzt werden.
NAS	Network Access System
NetBios	Network Basic Input Output System. Schnittstelle, die Datagramm- und streamorientierte Kommunikation bietet.
OCSP	Online Certificate Status Protocol. Wird als Protokoll für die Online-Prüfung von Zertifikaten verwendet.
OSI-Referenzmodell	Von der ISO standardisiertes Modell, das Kommunikation in sieben Schichten beschreibt: 7. Anwendungsschicht (application layer), 6. Darstellungsschicht (presentation layer), 5. Steuerungsschicht (session layer), 4. Transportschicht (transport layer), 3. Netzwerkschicht (network layer), 2. Daten-

	verbindungsschicht (data link layer), 1. physikalische Schicht (physical layer). Die im Netz zu übermittelnden Daten durchlaufen auf der Senderseite die Schichten von 7 – 1, auf der Empfängerseite in umgekehrter Reihenfolge.
PAP	Password Authentication Protocol. Sicherungsmechanismus innerhalb des PPP zur Authentisierung der Gegenstelle. PAP definiert eine Methode, nach dem Aufbau einer Verbindung anhand eines Benutzernamens und eines Passworts die Rechte des Senders zu prüfen. Dabei geht das Passwort im Klartext über die Leitung. Der Empfänger vergleicht die Parameter mit seinen Daten und gibt bei Übereinstimmung die Verbindung frei.
PC/SC	Schnittstelle zu Smartcard Readern
PEM	Ältere Form von Soft-Zertifikaten (ohne Private Key).
Personal Firewall	Die Security-Mechanismen der Client Software vereinigen Tunneling-Verfahren und Personal Firewalling. IP-Network Address Translationen (IP-NAT) sowie universelle Filtermechanismen. Von zentraler Bedeutung ist IP-NAT, denn es sorgt dafür, dass nur vom Rechner ins Internet ausgehende Verbindungen möglich sind. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filterings nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard. Verschlüsselungssystem mit öffentlichem Schlüssel.
PKCS#10	Die Form, wie ein Zertifikat vom PKI-Manager an die CA (Certification Authority) übertragen wird. Meist geschieht dies per Http – mit SSL verschlüsselt als Https.
PKCS#11	Basis des Smartcard-Standards

PKCS#12	Soft-Zertifikat. Standard der die Syntax der Dateistruktur beschreibt.
PKCS#15	Pointerbeschreibung: Wo befindet sich was auf der Smartcard.
PKI	(Public Key Infrastructure) Die erforderliche Schlüsselinfrastrukur zur authentischen Verteilung öffentlicher Schlüssel wird PKI genannt. Private und öffentliche Schlüssel werden für asymmetrische Kryptographie verwendet. Transaktionsbezogene Sicherheit erfordert eine eindeutige Partner-Authentisierung mittels Zertifikaten, die von einer vertrauenswürdigen PKI ausgestellt wurden. Insbesondere für E-Commerce bietet PKI den Rahmen für Vertraulichkeit (Geheimhaltung), Integrität (Fälschungssicherheit), Authentizität (Identitätssicherheit) und Nichtbestreitbarkeit.
PoP	Point of Presence
POP3	Protokoll zum Download von E-Mails. Gegenstück zu SMTP (Port 110)
PPP	Point-to-Point-Protokoll. Übertragunsprotokoll in verbindungsorienten Netzen.
PPP-Verhandlung	Point-to-Point-Protokoll. In einer PPP-Verhandlung wird die IP-Adresse nach Anwahl an den Provider automatisch übergeben.
PRI	Primary Rate Interface (ISDN-Schnittstelle, Primär-Multiplex S2m) mit 30 B-Kanälen und 2 D-Kanälen.
Radius	Remote Authentication Dial In User Service, siehe Directory Service
RA	Registration Authority. Meist ist die Registrierungsstelle die Stelle, die die Daten für die Beantragung eines Zertifikats entgegen nimmt. Die RA ist auch die Stelle, der der Verlust oder der Verfall eines gültigen Zertifikats gemeldet wird und die eine Widerrufsliste (Revocation List) ungültig gewordener Zertifikate herausgibt.
RAS	Remote Access Services. Firmenspezifische (Microsoft) Einwahlhilfe für Remote Access.

RIP Routing Information Protocol, auch Routing-Modus

RFC Request for Comment. Normentwurf, Vornorm, die im Internet diskutiert wird und so lange in der Liste der RFCs gehalten wird, so lange sie sich in der Praxis bewährt. Vorformen der RFCs sind Drafts.

Routing-Tabellen Router benötigen für die Wegewahl im Netz Informationen über die günstigsten Routen von der Quelle zum Ziel. Mit Hilfe der Routing-Tabellen werden diese Strecken vom Router kalkuliert. Während beim statischen Routing die Tabellen fest vorgegeben sind, erhält der Router beim dynamischen Routing über Router-Informationsprotokolle (z.B. RIP, NLSP, OSPF) Informationen über das Netz, die zu selbst erlernten Routing-Tabellen zusammengesellt werden und ständig aktualisiert werden.

RSA Das erste Verfahren, das die Anforderungen an die Public Key-Kryptographie erfüllte. Wurde 1977 von Ron Rivest, Adi Shamier und Leonard Adlemann erfunden.

Schnittstelle (Interface) Festlegung der zwischen zwei Geräten – bei der Datenfernübertragung im allgemeinen zwischen Datenendeinrichtung und Datenübertragungseinrichtung – erforderlichen elektrischen Verbindungsleitungen, der auf diesen herrschenden elektrischen Werten, der zur Funktion erforderlichen Signale sowie der Betriebsweise und Bedeutung dieser Signale. Man unterscheidet nach parallelen und seriellen Interfaces.

SHA Secure Hash Algorithm, siehe auch Signatur

Signatur Bei der digitalen Signatur wird mathematisch eine Verknüpfung zwischen Dokument und dem geheimen, persönlichen Signaturschlüssel des Teilnehmers erzeugt. Der Absender des Dokuments generiert eine Prüfsumme (sogenannter Hash-Wert), diese codiert er wiederum mit seinem Geheimschlüssel und erzeugt so einen digitalen Signaturzusatz zur ursprünglichen Nachricht. Der Empfänger des Dokuments kann mit dem öffentlichen Schlüssel des Absenders die Signatur prüfen, indem er seinerseits den Hash-Wert aus der Nach-

	richt bildet und diesen mit der entschlüsselten Signatur vergleicht. Da die Signatur des Absenders unmittelbar in das Dokument eingebunden ist, würde jede spätere Änderung bemerkt. Auch ein Abfangen oder Abhören der Signatur über Lauschangriffe erwiese sich als zwecklos: Die digitale Signatur ist nicht nachahmbar, da sie den geheimen, privaten Schlüssel verwendet; eine Ermittlung des geheimen Schlüssels aus der Signatur ist nicht möglich.
Smartcard	Wird die Funktionalität der Smartcard genutzt, so wird nach der CHAP-Authentisierung (User ID und Passwort) die "Erweiterte Authentisierung" (Strong Authentication) mittels der auf Smartcard und Gateway hinterlegten Zertifikate durchgeführt. Auf der Smartcard befinden sich unter anderm das Benutzer-Zertifikat, das Root-Zertifikat und der geheime private Schlüssel. Die Smartcard kann nur mit PIN genutzt werden.
SMTP	Simple Mail Transport Protocol. Internet Standard zur Verteilung elektronischer Post. Ist textorientiert und setzt auf TCP auf (Port 25)
SNA	Systems Network Architecture. Hierarchisch orientiertes Netz zur Steuerung von Terminals und zur Unterstützung des Zugriffs auf Anwendungen in IBM Host-Systemen.
SNMP	Simple Network Management Protocol. Netzwerk-Managementprotokoll auf Basis von UDP/IP.
Source Routing	Möglichkeit, in Token Ring-Netzwerken eine Wegewahl zwischen Bridges zu optimieren. Dabei werden die Wegeinformationen an den Datenblock angehängt mit übertragen. Auf diese Weise liegt auch der Weg für die Bestätigung eindeutig fest.
SPD	Security Policy Database
SSL	Secure Socket Layer. Gemäß dem SSL-Protokoll kann der dynamische Schlüsselaustausch (Dynamic Key Exchange) genutzt werden. SSL, von Netscape entwickelt, ist mittlerweile das Standard-Protokoll für dynamischen Schlüsselaustausch.
SSLCP	Secure Socket Layer Control Protocol

STARCOS	Betriebssystem für Smartcards
Symmetrische Verschlüsselung	Sender und Empfänger verwenden bei der symmetrischen Chiffrierung und Dechiffrierung den gleichen Schlüssel. Symmetrische Algorithmen sind sehr schnell und sehr sicher – dies allerdings nur dann, wenn die Schlüsselübergabe zwischen dem Sender und dem Empfänger ungefährdet erfolgen kann. Gelangt ein Unbefugter in den Besitz des Schlüssels, so kann dieser alle Nachrichten entschlüsseln bzw. sich unter Verwendung des Schlüssels als Absender von Nachrichten ausgeben. Soll bei der symmetrischen Verschlüsselung in größeren Gruppen jeder Teilnehmer nur an ihn adressierte Nachrichten lesen können, so ist für jedes Sender-Empfänger-Paar ein eigener Schlüssel notwendig. Die Folge: ein aufwendiges Schlüsselmanagement. So sind bei 1.000 Teilnehmern bereits 499.500 (!) unterschiedliche Schlüssel erforderlich, um sämtliche Wechselbeziehungen zu unterstützen. Bekannteste symmetrische Verschlüsselung ist heute der DES-Algorithmus.
TCP/IP	Transmission Control Protocol / Internet Protocol. TCP/IP ist ein Netzwerkprotokoll für heterogene Netze und an kein Transportmedium gebunden. Es kann auf X.25, Token Ring oder einfach auf die serielle Schnittstelle aufsetzen und eignet sich deshalb besonders als Kommunikati-onsprotokoll für unterschiedliche (Netz-) Topologien und Rechner-Plattformen, wie sie im Internet gekoppelt sind. Dabei wird jeder Rechner im Netzverbund Internet durch seine IP-Adresse identifiziert. TCP/IP umfaßt außerdem vier Internet-Standardfunktonen: 1. FTP: File Transfer Protocol für den Dateitransfer von einem zum anderen Rechner, 2. SMTP: Simple Mail Transport Protocol für E-Mail, 3. TELNET: Teletype Network für Terminalemulation, 4. RLOGIN: Remote Login zur Rechnerfernbedienung
TECOS	Betriebssystem für Smartcards (Versionen 1.2, 2.0)
Token Ring	Netzwerktopologie mit Ringstruktur von IBM.
UDP	User Data Protocol. Baut direkt auf dem darunter liegenden Internet Protokoll auf. Wurde definidert,

	um auch Anwendungsprozessen die direkte Möglichkeit zu geben, Datagramme zu versenden. UDP liefert über die Leistungen von IP hinaus lediglich eine Portnummer und eine Prüfsumme der Daten. Durch das Fehlen des Overheads mit Quittungen und Sicherungen ist es besonders schnell und effizient.
UMTS	Universal Mobile Telecommunications Service. Künftiger Standard für schnelle Handy-Kommunikation.
VPN	Virtual Private Network. Ein VPN kann als virtuelles Netz grundsätzlich über alle IP-Trägernetze – also auch das Internet – eingerichtet werden. Für die Realisation haben sich zwei Spezifikationen herauskristallisiert: L2F (Layer 2 Forwarding) und L2TP (Layer 2 Tunneling Protocol). Beide Verfahren dienen dazu, einen Tunnel aufzubauen, den man als eine Art "virtuelle Standleitung" bezeichnen kann. Über eine solche logische Verbindung lassen sich neben IP-Frames auch IPX-, SNA- und NetBIOS-Daten transparent übertragen. Am Tunnelende müssen die Datenpakete interpretiert und zu einem Datenstrom auf der Basis des verwendeten Protokolls umgewandelt werden.
WAP	Wireless Application Protocol. Entwicklung von Nokia, Ericson und Motorola.
X.509 v3	Standard Zertifizierung
Zertifikate	Zertificate (Certificates) werden von einer CA (Certification Authority) mit-tels PKI-Manager (Software) ausgestellt und auf eine Smartcard (Chipkarte) gebrannt. Diese Smartcard enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen.

9. Fehler- und ISDN-Meldungen

9.1 Fehlermeldungen

Ereignet sich ein Fehler während des Verbindungsaufbaus, so wird dieVerbindung nicht hergstellt und die Fehlerursache im Monitor angezeigt.

Diese Fehlermeldungen sind selbsterklärend und in folgende Gruppen eingeteilt:

Admin-Fehler (General)

“Zurückweisen eingehender Verbindungen” ist gesetzt
Interner Fehler

ISDN-Fehler

Kabel ist nicht angeschlossen
Falsche Rufnummer
Anschluss ist besetzt
Anwender antwortet nicht
Ungültiges Rufnummernformat
Kein Kanal verfügbar

COMX-Fehler

Falsches Modem wurde konfiguriert
Kein Wählton
Besetzt
Kein Trägermedium
Keine Antwort
Fehler

L2TP-Fehler

Falsches “Tunnel Secret”
HA Server konnte nicht gefunden werden
Verbindung zum VPN Gateway verloren
Tunnelprotokollfehler (Control Connection)
Tunnelprotokollfehler (Client Connection)
Kein lokaler Tunnel-Endpunkt konfiguriert
Kein freier Kanal vorhanden
Kein Kanal für eingehende Rufe frei
Kein Port für eingehende Rufe frei; Anzahl der Lizenzen überschritten

LCP-Fehler

Eingehender Ruf -> HA Server hat Sperre gesetzt
Eingehender Ruf -> Maximale Anzahl der Kanäle erreicht
Eingehender Ruf -> “Zurückweisen eingehender Verbindungen” ist gesetzt

PAP CHAP-Fehler

Falsches Passwort
Radius-Benutzer abgewiesen
Radius Timeout
Keine PIN eingegeben
Interner Fehler
Stimmt nicht mit konfigurierter Richtung überein
CLI-Fehler

IPCP-Fehler

Keine freie IP-Adresse aus Pool verfügbar

SSL-Fehler

Letzter Hash-Wert falsch
Client-Hello wurde nicht erhalten
Keine Client-Parameter erhalten
Keine Server-Parameter erhalten
Keine Zertifikats-Parameter erhalten
Keine letzten SSL-Parameter erhalten
Client-Hello und falsche SSL-Version
Client-Hello und falsche Verschlüsselungsvorschläge
Client-Hello und keine Resourcen
Client-Hello und falsche SSL-Version
Konnte Server-Zertifikat nicht entschlüsseln
Falsche Signature im Server-Schlüsselaustausch

ECP-Fehler

Lokaler Benutzer ist nicht für die Security konfiguriert
Entfernter Benutzer ist nicht für die Security konfiguriert

Lizenz-Fehler

Testversion abgelaufen
Maximale Anzahl der Kanäle erreicht
Maximale Anzahl der Tunnels erreicht
Falsche OEM-Version
Seriennummer mehrfach vorhanden
HA Server hat Sperre gesetzt (Lizenz)

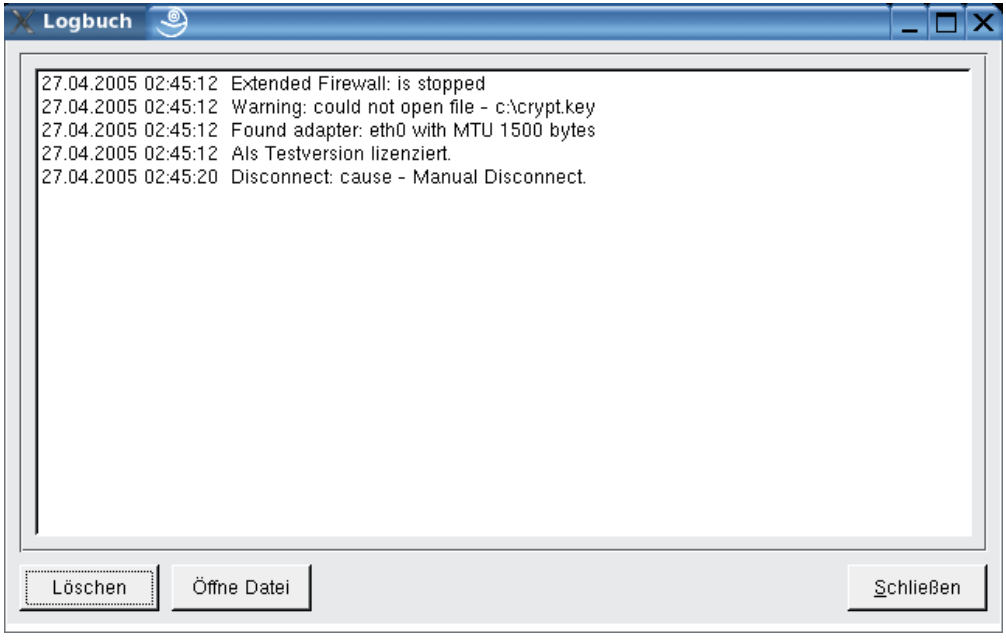
IKE-Fehler

IKE (Phase1) - Vorschlag wird nicht akzeptiert
IKE (Phase1) - Keine entsprechenden PKI-Einstellungen
IKE (Phase1) - Kontakt zur Gegenstelle verloren
IKE (Phase1) - Ungültige remote ID
IKE (Phase1) - Ungültiger Hash-Wert im Preshared Key-Modus
IKE (Phase1) - Ungültiger Signatur-Wert im PKI-Modus
IKE (Phase1) - Entschlüsselungsfehler wegen falschem Preshared Key
IKE (Phase2) - Kontakt zur Gegenstelle verloren
IKE (Phase2) - Vorschlag wird nicht akzeptiert

9.2 ISDN-Meldungen

Wie in Kapitel 3.1 dieses Handbuchs beschrieben, werden im Protokollierungs-Fenster alle Aktivitäten der Workstation protokolliert. Ein wichtiger Bestandteil dieser Protokolle sind die mit der CAPI 2.0 zusammenhängenden Meldungen. Jede CAPI-Meldung besteht aus einem 4-stelligen Code, der seine jeweils spezifische Bedeutung hat. Diese Codes sind nach den Standards der ETSI-Empfehlungen implementiert (European Telecommunications Standards Institute) und sind daher für alle ISDN-Produkte gültig, die auf der CAPI-Version 2.0 aufsetzen. Diese Codes werden mit den jeweiligen An- und Abwahlvorgängen der Workstation mitprotokolliert und im „Protokoll-Fenster" dargestellt.

Unten sehen Sie ein „Protokoll-Fenster" abgebildet. Die CAPI-Codes mit kurzen Erklärungen, die hilfreich bei der Fehlersuche sein können, finden Sie auf den folgenden Seiten.



Codes der CAPI 2.0

0001	NCPIwird nicht unterstützt
0002	Flags werden nicht unterstützt
0003	Alert bereits von einer anderen Applikation geschickt

CAPI Register-Fehler

1001	Zu viele Applikationen
1002	Logische Blockgröße zu klein, Minimum: 128 Bytes
1003	Buffer überschreitet 64 kByte
1004	Message Buffer Size zu klein, Minimum: 1024 Bytes
1005	Maximalzahl der logischen Links nicht unterstützt
1007	Message nicht akzeptiert wegen internem Belegtzustand
1008	Kein Speicher vorhanden
1009	CAPI nicht installiert
100A	Controller unterstützt externes Gerät nicht
100B	Controller unterstützt nur externes Gerät

Message-Fehler

1101	Unzulässige Applikationsnummer
1102	Unzulässiger Befehl oder Message-Länge weniger als 10 Octets
1103	Message nicht akzeptiert wegen voller Warteschlange
1104	Warteschlange leer
1105	Überlauf der Warteschlange, eine Message wurde verloren
1106	Unbekannter Notification Parameter
1107	Message nicht akzeptiert wegen internem Belegtzustand
1108	Kein Speicher vorhanden
1109	CAPI nicht installiert
110A	Controller unterstützt externes Gerät nicht
110B	Controller unterstützt nur externes Gerät

Code-Fehler

2001	Message im aktuellen Zustand nicht unterstützt
2002	Unzulässiger Controller / PLCI / NCCI
2003	PLCI fehlerhaft
2004	NCCI fehlerhaft
2005	LISTEN fehlerhaft
2006	FAX Ressourcen fehlerhaft (Protokoll T.30)
2007	Unzulässiger Message Parameter Code

Service-Fehler

3001	B1-Protokoll nicht unterstützt
3002	B2-Protokoll nicht unterstützt
3003	B3-Protokoll nicht unterstützt
3004	Parameter des B1-Protokolls nicht unterstützt
3005	Parameter des B2-Protokolls nicht unterstützt
3006	Parameter des B3-Protokolls nicht unterstützt
3007	Kombination des B-Protokolls nicht unterstützt
3008	NCPI nicht unterstützt
3009	CIP-Wert unbekannt
300A	Flags nicht unterstützt (reservierte Bits)
300B	Einrichtung nicht unterstützt
300C	Datenlänge nicht von richtigem Protokoll unterstützt
300D	Reset-Vorgang von aktuellem Protokoll nicht unterstützt

Protokoll-Fehler

3301	Protokoll-Fehler auf Layer 1 (Verbindung unterbrochen oder B-Kanal von Signalprotokoll entfernt)
3302	Protokoll-Fehler auf Layer 2
3303	Protokoll-Fehler auf Layer 3
3304	Der Ruf ging an eine andere Applikation

T.30

3311	Verbindungsaufbau nicht erfolgreich (kein Fax G3)
3312	Verbindungsaufbau nicht erfolgreich (Training Error)
3313	Verbindung vor der Übertragung unterbrochen (remote Station unterstützt den Übertragungs-Mode nicht)
3314	Verbindung während der Übertragung von der Gegenseite unterbrochen
3315	Verbindung während der Übertragung unterbrochen (Fehler der Gegenseite, z.B. Wiederholung von T.30-Befehlen nicht erfolgreich)
3316	Verbindung während der Übertragung unterbrochen (local tx data underrun)
3317	Verbindung während der Übertragung unterbrochen (local rx data overflow)
3318	Verbindung während der Übertragung unterbrochen (lokaler Abbruch)

Disconnect (ETS 300102-1/Q.931.)

3481	Nummer nicht zugewiesen
3482	Keine Route zum angegebenen Transit-Netz
3483	Keine Route zum Ziel
3486	Kanal kann nicht akzeptiert werden

3487	Ruf wird in einem eingerichteten Kanal zugestellt
3490	Normale Verbindungsauslösung
3491	Anwender belegt
3492	Anwender antwortet nicht
3493	Anwender antwortet nicht (Anwender ist gewarnt)
3495	Ruf wird abgewiesen
3496	Nummer geändert
349A	Nicht ausgewählter Anwender gelöscht
349B	Ziel nicht ordnungsgemäß
349C	Ungültiges Nummernformat
349D	Einrichtung abgewiesen
349E	Antwort auf STATUS ENQUIRY
34A2	Kein Satz / Kanal verfügbar
34A6	Fehler im Netz
34AA	Überlastung in der Vermittlungseinrichtung
34AB	Zugangsinformationen ungültig
34AC	Angeforderter Satz / Kanal nicht verfügbar
34B1	Dienstmerkmal nicht verfügbar
34B2	Angeforderte Einrichtung nicht freigeschaltet
34B9	Trägerleistung nicht autorisiert
34BA	Trägerleistung derzeit nicht verfügbar
34C1	Trägerleistung nicht eingerichtet
34C2	Kanaltyp nicht eingerichtet
34C5	Angeforderte Einrichtung nicht vorhanden
34C6	Nur eingeschränkte digitale Informationsträgerleistung verfügbar
34CF	Dienst oder Option nicht implementiert
34D1	Ungültiger Call Reference Value
34D2	Der identifizierte Kanal existiert nicht
34D3	Anhängiger Ruf existiert, diese Verbindungskennung jedoch nicht
34D4	Verbindungskennung in Gebrauch
34D5	Kein Ruf anhängig
34D6	Ruf mit der geforderten Verbindungskennung gelöscht
34D8	Ziel inkompatibel
34DB	Ungültige Auswahl des Transitnetzes
34E0	Vorgeschriebenes Informationselement fehlt
34E1	Meldungstyp existiert nicht / nicht eingerichtet
34E2	Meldungstyp existiert nicht / nicht eingerichtet / nicht kompatibel
34E3	Informationselement existiert nicht / nicht eingerichtet
34E4	Ungültiger Informationsinhalt
34E5	Meldung nicht mit Verbindungszustand kompatibel
34E6	Wiederaufbau nach Timer-Ablauf
34EF	Protokoll-Fehler

Diese Seite ist frei →

© NCP engineering GmbH

10. Index

A

Access Server (Standard Security) 22
Advanced Encryption Standard 247
Advanced Security 18
AES-128, AES-192, AES-256 222
Aggressive Mode 141, 185, 218
AH 206, 209, 213, 214
Aktivierung (der DVE-Funktionalität) 155
Aktivierung (der Firewall) 165
Allgemein |SPD 177
Alternative Rufnummern 119
Amtsholung 94, 119
Anklopfen im D-Kanal 229
Anschluss 121
APN 122
ARL 242
Art der Gültigkeit 170, 174
Art der ID (Ausgehende / Eingehende Verbindung) 182
Asymmetrische Verschlüsselung 247
Ausführung 178
Ausschließlich Kommunikation im Tunnel zulassen 165
Aussteller 63
Aussteller des eingehenden Zertifikats 162
Aussteller-Zertifikat anzeigen 63
Austausch-Modus 169, 185, 218
Authentication Header 206, 208
Authentisierung 169, 170
Authentisierung (nur ESP) 173, 175
Authentisierung |SPD 181
authorityKeyIdentifier 66
automatischer Verbindungsaufbau 189
Autostart 110
AVM - PPP over CAPI 31, 61

B

Baudrate 121
Beenden (der Verbindung) 71
Beenden (des Monitors) 71
Bei Booten verbinden 125
Beim Schließen minimieren 110
Bekannte Netze, Firewall 90
Benutze SHA1 Fingerprint statt MD5 163
Benutzer des eingehenden Zertifikats 162
Benutzer lokal 133
Benutzer-Zertifikat anzeigen 63
Benutzername 118
Benutzername der Gegenstelle 133
Betriebssystem 30
bidirektional 133
BITS 207
BITW 207
Bluetooth 31

C

Callback 229
CAPI 2.0 264
CAPI-Meldung 264
CDP (Certificate Distribution Point) 66
Certification Authority 248
CHAP 133, 204
Charge-One-Side-Only 131, 236
Chipkarte 100
Chipkartenleser (PC/SC-konform) 97
CLI (Calling Line Identification) 229
Com Port 121
COSO 131
CPD (Certificate Distribution Point) 64
CRL 242

D

Dateiname |Security 139
Dauer 170, 174
Demilitarisierte Zone 250
Destination IPSec Gateway 153
DH-Gruppe 169, 171, 173, 175, 208
DHCP 143, 145
Dial In mit DynDNS 230
Dial Out mit Lockruf 229
Dial Prefix 122
Diffie-Hellmann 208
Diffie-Hellmann-Gruppe 171
Directory Service 249
DNS 250
DNS / WINS 156
DNS Request 231, 232
DNS-Server 157
Domain Name 157
DPD (Dead Peer Detection) 227
Durchsatz 60
DVE Secret 155
DVE-Server 155
DX25 159
Dynamic DNS 230
Dynamic VPN Endpoint 154
Dynamische Linkzuschaltung 126
dynamische SPD 206, 221
DynDNS 228, 230
DynDNS-Hostname 231

E

EAP-Optionen 101
Eingehende Rufe 132
Eingehendes Zertifikat anzeigen 64
Encapsulating Security Payload 206, 208
End to Site VPN 205, 210
Entrust Profil 96
Erlaube eingehende IP-Verbindungen 143
ESP 206, 209, 213, 214
Exchange Mode 218
Extended Authentication 224
extendedKeyUsage 66
Extensions 66

F

Fehlermeldungen 261
Festverbindung 18
Fingerprint 63
Fingerprint des Aussteller-Zertifikats 163
Firewall 17, 250
Firewall, Firewall-Regeln 84
Firewall, Grundeinstellungen 82
Firewall-Einstellungen 80
Firewall-Regel / Allgemein 85
Firewall-Regel / Lokal 87
Firewall-Regel / Remote 88
Firewall-Regel, Bekannte Netze 90
Firewall-Regeln, Firewall 84
Friendly Nets 90
FS Server 25

G

gegenseitige Authentisierung 133, 134
GPRS 31
GPRS / UMTS 116
Grundeinstellungen, Firewall 82
GSM 31, 115
Gültigkeitsdauer der Zertifikate 63

H

HA Manager 27
HA-Server 155
Hardware-Zertifikat 67, 102
Hash 169, 171
Hash |IKE-Richtlinie 171
Hayes-Befehlssatz 30
High Availability Server (HA Server) 25
Hostname DynDNS Server 231
HotSpot 59
HotSpot-Anmeldung 59
HSCSD 31
HTTP Proxy für CRL Download 67
Hybride Verschlüsselung 251

I

ID String (Ausgehende / Eingehende Verbindung) 182
Identity Protection Mode 185, 218
IKE 205
IKE ID 147, 226
IKE ID |Security 141
IKE ID-Typ 147, 226
IKE ID-Typ |Security 141
IKE Security Association 170
IKE-Config 226, 227
IKE-Modi 218
IKE-Modus 169, 170, 218
IKE-Richtlinie 167, 184, 216, 218
IKE-Richtlinie |Security 139
Index |Security 138
Intergration von IPSec 207
Internet 75
Internet Key Exchange 169, 205, 218
IP Broadcast erlaubt 143
IP Network Address Translation 17, 143, 238, 252
IP-Adr. halten bei manuellem Verbindungsaufbau 124

IP-Adresse 143
IP-Adresse (Quelle) 180
IP-Adresse (Ziel) 180
IP-NAT 143
IP-Netzmaske 198, 199, 200
IP-Protokoll 180
IPCOMP (LZS) 223
IpEncap 160
IPSec 75, 138, 201, 205
IPSec für Remote Access 220
IPSec native 222
IPSec over L2Sec 74
IPSec over L2TP 18, 138, 201, 220, 221, 230, 232, 233
IPSec Policy 208
IPSec Tunneling 222, 226
IPSec, Konfigurationsparameter 167
IPSec-Anwendungen 211
IPSec-Endpunkt (lokal) 187
IPSec-Endpunkt (Ziel) 187
IPSec-Konfiguration 78
IPSec-Maschine 206, 210
IPSec-Richtlinie 167, 172, 184, 216
IPSec-Richtlinie |Security 140
IPSec-Richtlinien 208
IPSec-Tunneling 139, 141, 147, 148
IPX Frames 144
IPX-Protokoll 144
IPX/SAP Spoofing 144
IR-Schnittstelle (Infrarot) 31
ISDN 115, 126, 144
ISDN D-Kanal 158
ISDN-Meldungen 261

K

KeyUsage 64, 66
Kompression 61, 126
Konfigurations-Assistent 74
Kontrollkanal 181, 217

L

L2Sec 18, 74, 138, 201, 202, 203, 204
L2TP 138, 146, 147, 202, 203
LAN (over IP 128
LAN (over IP) 115
LAN IP-Adresse 197
LAN over IP 61
LAN-Adapter schützen 243
Layer-3-Tunneling 205
LB Server 25
Link Einstellungen 142
Link Firewall 80, 164
Lockruf 228, 229
Log-Funktion 106
Logbuch 106
Lokales System 34
Low-Level Callback 131, 236

M

MAC-Adresse 145
Main Mode 141, 185, 218
Managed VPNs 233

Management Server 157
manueller Verbindungsaufbau 189
MD5 223
MD5 (Message Digit 5) 163
Modem 115, 120, 121
Modem Init. String 122
Modus 187
Multilink 61

N

NAS 159
NAT-T (NAT Traversal) 148, 227
native IPSec 141
NCP 131
NCPDDNS.BAT 231
NetBios over IP 144
NetKey 2000 . . . . . 33, 98
Netzeinwahl 117
NTBA 134

O

Optionen, Firewall 91
OTP-Token 127

P

PAP 134
Parametersperre aufheben 71
Passwort 118
Passwort der Gegenstelle 133
Passwort für OTP-Token 193
Passwort für VPN-Einwahl 193
Passwort lokal 133
Passwort speichern 118
Passwörter und Benutzernamen 192
Personal Firewall 17
PFS (Perfect Forward Secrecy) 223
Phase-1-Parameter 169
Phase-2-Parameter 173
PIN ändern 70
PIN eingeben 68
PIN-Abfrage 100
PIN-Eingabezwang 69
PIN-Richtlinie 101
PIN-Status 69
PKCS#11-Modul 99
PKCS#12-Datei 64, 96, 98
Policies 216
Port (Quelle) 180
Port (Ziel) 180
PPP 131
PPP over Ethernet 115, 128
PPP-Verhandlung 157, 203
PPTP 116
Preshared Key 140, 170, 211, 219, 224, 225, 226
Preshared Key |Security 139
Private IP-Adresse 153
Protokoll 173, 174, 264
Protokollierung, Firewall 92
PSK (Preshared Key) 222
Public Key Infrastucture 220

R

RAS Script-Datei 119
Registration Authority 98
Remote-Administration 55
Revocation List 242
RFC 2401 205
RFC 2401 - 2409 205
RFC 2409 205
RFC 2716 202
RFC 2888 220
Richtlinie von Gegenstelle bestimmt 140
Richtlinien 78, 216
Richtlinien |IPSec 167
Richtung 133, 178
RSA-Signatur 140, 170, 218, 219
Rückruf 128, 229
Rückruf für ausgehende Verbindungen 129
Rückruf für eingehende Verbindungen 130
Rückrufmodus 119, 130
Rückrufnummer 129
Rufnummer (Ziel) 118
Rufnummer für CLI 229
Rufnummer lokal 134
Rx 126
Rx und Tx Bytes 61

S

SA 206, 212, 213
SA-Verhandlung 216, 217
Schlüsselaustausch 61
Schlüsselmanagement 203
Schwellwert für Linkzuschaltung 126
Seamless re-keying 223
Secure Policy Database 169, 176, 206, 209, 212, 214
Secure Policy Database, dynamisch 167, 201, 221
Secure Policy Database, statisch 167, 201, 215, 218
Secure Server Manager 26
Security 201
Security |SPD 183
Security Association 206, 212, 213
Security Management 16
Security Parameter Index 213
Security-Modus 138
Security-Richtlinie 206
Selektor 206, 213, 215
Selektoren |SPD 179
Seriennummer 63
SHA1 (Secure Hash Algorithm 1) 163, 223
Sicherheits-Verknüpfung 213
Signtrust 33, 98
SIM PIN 122
SIM PIN AT-Befehl 122
Site to Site VPN 205
Softzertifikatsauswahl aktivieren 100
Source Routing 258
SPD Entry 206, 214
SPD Filtertabelle 212
SPD, dynamische 169
SPD, statische 169
SPD-Eintrag 213, 214, 215

Sperrlisten 242
SPI 213
SPX Spoofing 144
SSL-Server-Authentisierung 66, 241
STAC 126
STAC mit History 126
Standard Security 17
Stateful Inspection 243
statische SPD 201
Statischer Schlüssel 184
Statischer Schlüssel |Security 139
Strong Security 19
subjectKeyIdentifier 66
Symmetrische Verschlüsselung 259
symmetrischer Schlüssel 171

T

TC Trust (CardOS M4) 33
TEI-Wert 160
Telefonbuch 41, 73
Testversion 40
Timeout 60, 124, 125, 194
Timeout-Richtung 125
Timeout-Werte 123
Token (PKCS#11) 33
Transformation (Comp) 173, 174
Transformation (ESP) 173, 174
Transportmodus 187, 206, 209, 210, 214
Trennen 194
Tunnel - Parameter 146
Tunnel |SPD 186
Tunnel Secret 148
Tunnel-Endpunkt (Lokal) 149
Tunnel-Endpunkt (Ziel) 148
Tunnel-Parameter 238
Tunnelmodus 187, 206, 209, 210, 214
Tunnelweiterleitung (Tunnel-Forwarding) 233
TxRx 126

U

Übertragungskanal 159

V

Verbinden 189
Verbindungs-Informationen 60
Verbindungsabbau 100
Verbindungsabruch 194
Verbindungsart 61, 115, 120
Verbindungsaufbau 124
Verbindungssteuerung 123
Verbindungssteuerung |Konfiguration 100
Verbindungszeit 60
Verhandle PPP Callback 130
Verschlüsselung 61, 141, 169, 171
Verschlüsselung |Security 138
Verschlüsselungsart 202
Verwende VPN-Benutzername 149
Virtual Private Network 18, 260
VPN 18
VPN IP-Netze 238
VPN IP-Netzmasken 151

VPN IP-Netzwerke 151
VPN-Benutzername 148
VPN-Gateway 23, 146
VPN-Passwort 148
VPN-Protokoll 147
VPN-Tunnel 151
VPN/PKI Gateway (Strong Security) 24

W

Wählverbindung 18
wechselnder Verbindungsaufbau 189
WINS-Server 157
wireless LAN 31
WLAN-Adapter 31

X

X.25 Link-Protokoll 160
X.25 Window Size 160
X.31 . . . . . 158, 161
X.509 19
xDSL 115
xDSL (AVM - PPP over CAPI) 115
xDSL (PPPoE) 31, 61

Z

Zertifikat, Auswahl 98
Zertifikate |Konfiguration 95
Zertifikate |Verbindung 62
Zertifikats-Überprüfungen 240
Zertifikatspfad 100
Zertifikatsverlängerung 101
Zielsystem 114
Zielsystem, konfigurieren 76
Zuletzt zugewiesenes Gateway benutzen 155