



Benutzerhandbuch be.IP

Workshops

Copyright© Version 08/2020 bintec elmeg GmbH

Rechtlicher Hinweis

Gewährleistung

Änderungen in dieser Veröffentlichung sind vorbehalten.

bintec elmeg GmbH gibt keinerlei Gewährleistung auf die in dieser Bedienungsanleitung enthaltenen Informationen. bintec elmeg GmbH übernimmt keine Haftung für mittelbare, unmittelbare, Neben-, Folge- oder andere Schäden, die mit der Auslieferung, Bereitstellung oder Benutzung dieser Bedienungsanleitung im Zusammenhang stehen.

Copyright © bintec elmeg GmbH

Alle Rechte an den hier beinhalteten Daten - insbesondere Vervielfältigung und Weitergabe - sind bintec elmeg GmbH vorbehalten.

Inhaltsverzeichnis

Kapitel 1	be.IP als VDSL-Modem verwenden	1
1.1	Vorbereitung	1
1.1.1	Inbetriebnahme.	1
1.1.2	Vorkonfigurierte Adresse löschen	1
1.2	Konfiguration.	2
1.2.1	VDSL-Modem und Ethernet-Schnittstelle verbinden	2
1.2.2	Konfiguration auf dem einwählenden Router	4
1.2.3	Nutzung weiterer Funktionen der be.IP	5
1.3	Konfigurationsschritte im Überblick	6
Kapitel 2	Konfigurationszugang für den Benutzer anlegen und spezielle Anwendungen verwenden	8
2.1	Einleitung	8
2.2	Konfiguration.	8
2.2.1	Konfigurationszugang für Benutzer ("User Portal")	9
2.2.2	Anwendungen	10
2.3	Konfigurationsschritte im Überblick	14
Kapitel 3	Zugriff aus dem WAN über HTTPS	15
3.1	Einleitung	15
3.2	Konfiguration.	15
3.2.1	Network Address Translation (NAT) / Port Address Translation (PAT)	16
3.2.2	Stateful Inspection Firewall (SIF)	17
3.2.3	Administrativer Zugriff	18
3.2.4	Zugriff aus dem WAN	20
3.3	Konfigurationsschritte im Überblick	21

Kapitel 4	Zugriff aus dem WAN auf einen WEB-Server im LAN	24
4.1	Einleitung	24
4.2	Konfiguration.	24
4.2.1	Network Address Translation (NAT) / Port Address Translation (PAT) . . .	25
4.2.2	Stateful Inspection Firewall (SIF)	27
4.3	Konfigurationsschritte im Überblick	29
Kapitel 5	Einwahl eines iPhone auf einer be.IP mit IPSec IKEv1	31
5.1	Einleitung	31
5.2	Konfiguration.	31
5.2.1	Anlegen des Einwahlprofils über den Assistenten	31
5.2.2	Anlegen / Ändern der iPhone-spezifischen Parameter	33
5.3	Anlegen des Einwahlprofils auf dem iPhone	41
5.4	Konfigurationsschritte im Überblick	43
Kapitel 6	Zugriff aus dem WAN über die PPPoE-WAN-Verbindung .	45
6.1	Einleitung	45
6.2	Konfiguration.	45
6.2.1	Network Address Translation (NAT) / Port Address Translation (PAT) . . .	45
6.2.2	Stateful Inspection Firewall (SIF)	48
6.2.3	Änderungen am Internet Gateway	50
6.2.4	Schlussbemerkung	51
6.3	Konfigurationsschritte im Überblick	52
Kapitel 7	be.IP Secure Client: Konfiguration eines VPN Remote Zugriffs	54
7.1	Einleitung	54

7.2	Konfiguration	54
7.2.1	Gateway starten	55
7.2.2	Tunnel mit dem Assistenten VPN konfigurieren	55
7.2.3	be.IP Secure Client herunterladen	58
7.2.4	be.IP Secure Client installieren und konfigurieren	58
7.2.5	Software aktivieren und Datei einlesen	66
7.2.6	IPSec-Verbindung aufbauen	68
7.2.7	Tunnel splitten	69
7.3	Konfigurationsschritte im Überblick	70
Kapitel 8	be.IP plus als PBX mit zwei xDSL-Anschlüssen	73
8.1	Vorbemerkung	73
8.2	Konfiguration	74
8.2.1	Einrichtung der WAN-Verbindung	74
8.2.2	Einstellung der WAN-Schnittstelle für die SIP-Verbindung	78
8.2.3	Einrichtung der Lastverteilung	81
8.2.4	Spezielle Lastverteilungs-Behandlung von verschlüsselten Verbindungen	84
8.2.5	Anpassen der Metrik	86
8.3	Abschließende Bemerkungen	87
8.4	Konfigurationsschritte im Überblick	88
Kapitel 9	Telefonieren über einen SIP-Provider mithilfe der be.IP plus	91
9.1	Einleitung	91
9.2	Vorbereitende Konfiguration	93
9.2.1	Variante 1: Netzwerkkonfiguration mit direktem Internetanschluss	93
9.2.2	Variante 2: Netzwerkkonfiguration mit Gateway	93
9.2.3	Variante 1 + 2: Konfiguration der Ländereinstellungen in der be.IP plus	96
9.3	Variante 1 + 2: Konfiguration des SIP-Providers in der be.IP plus	98
9.3.1	SIP-Provider (Einzelrufnummer)	98

9.3.2	SIP-Provider (Durchwahl)	106
9.4	Variante 1 + 2: Konfiguration der Berechtigungsklasse (Optional)	111
9.5	Variante 1 + 2: Konfiguration der Rufnummern in der be.IP plus.	112
9.5.1	Zuordnung der kommenden Anrufe	112
9.5.2	Konfiguration der gehenden Rufnummern	113
9.6	Konfigurationsschritte im Überblick	114
Kapitel 10	bintec 4Ge-LE als WAN-Strecke an einer be.IP.	119
10.1	Einleitung	119
10.2	Konfiguration	120
10.3	Konfigurationsschritte im Überblick	126
Kapitel 11	Zwei gekoppelte be.IP 4isdn an einem Telekom VoIP Durchwahl-Anschluss	128
11.1	Einleitung	128
11.2	Konfiguration.	129
11.2.1	SYNC-Anschluss Einstellungen.	130
11.2.2	be.IP 4isdn Slave konfigurieren (Teil 1)	131
11.2.3	be.IP 4isdn Master konfigurieren	133
11.2.4	be.IP 4isdn Slave konfigurieren (Teil 2)	138
11.3	Konfigurationsschritte im Überblick	142
Kapitel 12	Zwei gekoppelte be.IP 4isdn an einem Telekom VoIP Einzelrufnummern-Anschluss	147
12.1	Einleitung	147
12.2	Konfiguration.	148
12.2.1	SYNC-Anschluss Einstellungen.	149
12.2.2	be.IP 4isdn Slave konfigurieren (Teil 1)	150

12.2.3	be.IP 4isdn Master konfigurieren	152
12.2.4	be.IP 4isdn Slave konfigurieren (Teil 2)	157
12.3	Konfigurationsschritte im Überblick	161
Kapitel 13	be.IP 4isdn als CAPI-Server einrichten	166
13.1	Konfiguration.	166
13.2	Konfigurationsschritte im Überblick	171
Kapitel 14	Konfigurationshilfen.	173
14.1	Startansicht ändern	173
14.1.1	Konfiguration.	173
14.2	Einrichtung an einem Vodafone VDSL-Anschluss	174
14.2.1	Einrichtung der Internet-Verbindung.	174
14.2.2	Einrichtung der Voice-Verbindung.	175
14.3	Konfiguration eines DynDNS-Accounts	177
14.3.1	Konfiguration.	177
14.4	Verwendung von Amtsleistungsmerkmalen und Funktionen am IP-basierten Anschluss	179
14.4.1	be.IP und be.IP plus als Mediagateway	179
14.4.2	be.IP plus als PBX	179

Kapitel 1 be.IP als VDSL-Modem verwenden

Voraussetzungen

- Eine **be.IP**
- Eine **be.IP plus**

Konfigurationsziel

Nutzung einer **be.IP** als VDSL-Modem und Verwendung weiterer Funktionen dieses Geräts

1.1 Vorbereitung

1.1.1 Inbetriebnahme

- (1) Öffnen Sie einen Web-Browser und geben Sie die IP-Adresse `192.168.0.251` in das Adressfeld Ihres Web-Browsers ein.
- (2) Geben Sie in die Felder **Benutzername** und **Kennwort** Ihre Anmeldedaten ein und klicken Sie auf **Anmelden**.
Der Assistent **Schnellstart** öffnet sich.
- (3) Verlassen Sie den Assistenten **Schnellstart**, indem Sie in der Kopfleiste unter **Ansicht** *Vollzugriff* wählen.

1.1.2 Vorkonfigurierte Adresse löschen

Das Löschen der vorkonfigurierten IP-Adresse auf der Schnittstelle `en1-4` (DMZ/WAN Port, blau) ermöglicht eine weitergehende Konfiguration in diesem IP-Bereich. Auf die eigentliche Funktion des PPPoE über diese Schnittstelle hat die Existenz der IP-Adresse keinen Einfluss.

- (1) Gehen Sie zu **LAN->IP-Konfiguration->Schnittstellen->en1-4** .

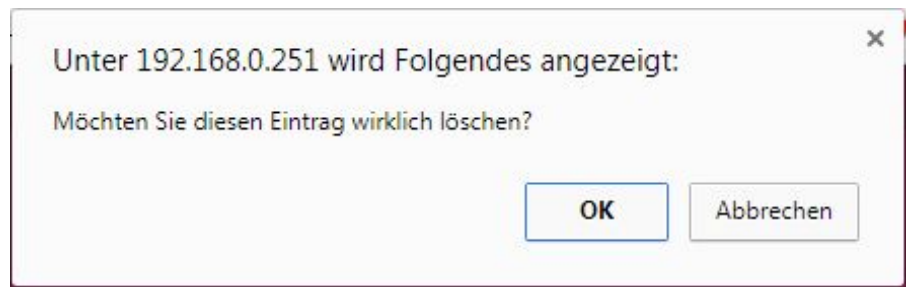
Ethernet-/VLAN-Ports				
Schnittstelle	IPv4-Adresse/Netzmaske	IPv6-Adresse/Länge	Status	Aktion
en1-4	192.168.4.251/255.255.255.0	-		   
efm35-60	Nicht konfiguriert/Nicht konfiguriert	-		   

- (2) Klicken Sie im Feld **IP-Adresse/Netzmaske** auf das Symbol , um den Eintrag zu

löschen.

The screenshot shows two configuration panels. The left panel, titled 'Basisparameter', has a 'Schnittstellenmodus' section with radio buttons for 'Untagged' (selected) and 'Tagged (VLAN)'. Below it is a 'MAC-Adresse' field containing '00:09:4f:6f:5e:80' and a toggle switch for 'Voreingestellte verwenden' which is turned on. The right panel, titled 'Grundlegende IPv4-Parameter', has a 'Sicherheitsrichtlinie' section with radio buttons for 'Nicht Vertrauenswürdig' and 'Vertrauenswürdig' (selected). Below it is an 'Adressmodus' section with radio buttons for 'Statisch' (selected) and 'DHCP'. The 'IP-Adresse / Netzmaske' section contains two input fields: 'IP-Adresse' with '192.168.4.251' and 'Netzmaske' with '255.255.255.0'. A trash icon is visible to the right of the IP address field, and a 'HINZUFÜGEN' button is at the bottom.

- (3) Bestätigen Sie mit **OK**.
- (4) Eine Warnung erscheint.



- (5) Bestätigen Sie mit **OK**.

1.2 Konfiguration

1.2.1 VDSL-Modem und Ethernet-Schnittstelle verbinden

Sie verbinden die Ethernet-Schnittstelle **en1-4** und die VDSL-Schnittstelle des Modems mittels einer Bridge-Gruppe.

- (1) Gehen Sie zu **Systemverwaltung->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen**.
- (2) Wählen Sie unter **en1-4** *Neue Bridge-Gruppe*.
- (3) Wählen Sie unter **Konfigurationsschnittstelle** *Nicht beachten*.

Zugriffsparameter		
#	Schnittstellenbeschreibung	Modus / Bridge-Gruppe
1	en1-0	br0
2	en1-4	Neue Bridge-Gruppe
3	efm35-60	Routing-Modus
4	ethoa35-5	Routing-Modus
5	vss7-10	br0

Konfigurationsschnittstelle
Nicht beachten

- (4) Bestätigen Sie mit **OK**.
Eine Warnung erscheint.

✕

Unter 192.168.0.251 wird Folgendes angezeigt:

Möchten Sie diesen Eintrag wirklich löschen?

OK
Abbrechen

- (5) Bestätigen Sie mit **OK**.
en1-4 wird zur Bridge-Gruppe *br1* hinzugefügt.

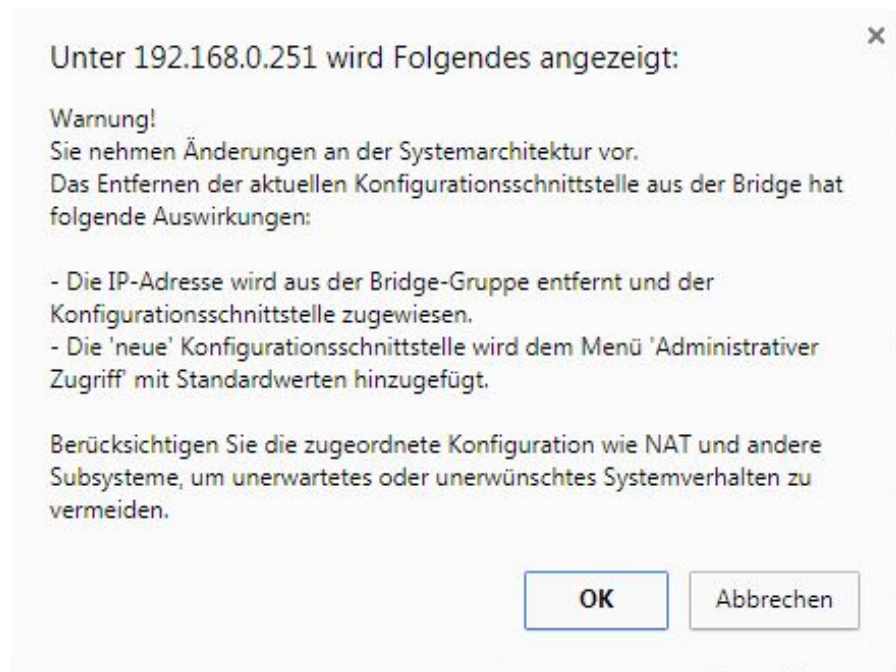
Fügen Sie die Schnittstelle **efm35-60** ebenfalls zur Bridge-Gruppe *br1* hinzu.

- (1) Wählen Sie dazu unter **efm35-60** *br1*.
(2) Wählen Sie unter **Konfigurationsschnittstelle** *Nicht beachten*.

Zugriffsparameter		
#	Schnittstellenbeschreibung	Modus / Bridge-Gruppe
1	en1-0	br0
2	en1-4	br1
3	efm35-60	br1
4	ethoa35-5	Routing-Modus
5	vss7-10	br0

Konfigurationsschnittstelle
Nicht beachten

- (3) Bestätigen Sie mit **OK**.
Eine Warnung erscheint.




- (4) Bestätigen Sie mit **OK**.
efm35-60 wird zur Bridge-Gruppe *br1* hinzugefügt.

Die Schnittstelle **en1-4** steht als eingehende Schnittstelle für eine PPPoE-Verbindung zur Verfügung.

1.2.2 Konfiguration auf dem einwählenden Router

Sie konfigurieren **VLAN-ID = 7** auf dem einwählenden Router (d.h. auf einer **be.IP plus**).

- (1) Gehen Sie zu **WAN->Internet + Einwählen->PPPoE-><Verbindung>->** .
- (2) Aktivieren Sie **VLAN**.
- (3) Geben Sie **VLAN-ID = 7** ein.
- (4) Bestätigen Sie mit **OK**.

Basisparameter

Beschreibung
DTAG_VDSL25

PPPoE-Modus Standard Mehrfachverbindung

PPPoE-Ethernet-Schnittstelle

Benutzername
t-online-com/2TB12JBAA2FK@t-online-co

Passwort

VLAN Aktiviert

VLAN-ID
7

Immer aktiv Aktiviert

- (1) Verbinden Sie die Schnittstellen **en1-4** von beiden Geräten mit einem Ethernet-Kabel. Das VDSL-Modem der **be.IP** synchronisiert sich. Die WAN-Verbindung auf der **be.IP plus** wird aktiv.

1.2.3 Nutzung weiterer Funktionen der be.IP

Sie können weitere Funktionen der **be.IP** nutzen.

Dazu sollten Sie auf der **be.IP**

- die eigene IP-Adresse ändern
- den DHCP-Server deaktivieren
- die Standard-Route zur **be.IP plus** einrichten
- die **be.IP plus** als DNS-Server eintragen.

- (1) Gehen Sie zu **Assistenten->Erste Schritte->Grundeinstellungen**.
- (2) Ändern Sie die eigene **IP-Adresse**, z. B. in *192.168.2.2*.
- (3) Deaktivieren Sie **Dieses Gerät als DHCPv4-Server verwenden**.
- (4) Geben Sie unter **Standard-Gateway-IP-Adresse** z. B. *192.168.2.1* ein, um die Standard-Route auf das Gerät mit den PPPoE-WAN-Verbindungen zeigen zu lassen.
- (5) Geben Sie unter **DNS-Server 1** dieselbe IP-Adresse wie oben ein, um dieses Gerät als DNS-Server einzutragen, z. B. *192.168.2.1*.

Wählen Sie den physikalischen Ethernet Port für die LAN-Verbindung aus?

Physikalischer Ethernet-Port (LAN) ETH1 ▾

Geben Sie die IPv4-LAN-Konfiguration ein:

Logische Ethernet-/Bridge-Schnittstelle br0

Adressmodus Statisch DHCP-Client

IP-Adresse

Netzmaske

Standard-Gateway-IP-Adresse

Feste DNS-Server-Adresse Aktiviert

DNS-Server 1

DNS-Server 2

⚠ Warnung! Konfigurationsverbindung geht möglicherweise beim Ändern der IP-Adresse verloren! Klicken Sie auf "OK", und melden Sie sich erneut an, um fortzufahren!

Wird dieses Gerät als DHCPv4-Server verwendet?

Dieses Gerät als DHCPv4-Server verwenden

IPv6-Konfiguration eingeben

IPv6

Nach gesteckter Verbindung steht z. B. *br0* als Switch-Erweiterung zur Verfügung, aber auch auf weitere Funktionen wie z. B. Access Point oder IPSec können Sie im Netzwerk zugreifen.

1.3 Konfigurationsschritte im Überblick



Vorkonfigurierte Adresse löschen

Feld	Menü	Wert
IP-Adresse / Netzmaske	LAN -> IP-Konfiguration -> Schnittstellen -> en1-4	

VDSL-Modem und Ethernet-Schnittstelle verbinden

Feld	Menü	Wert
en1-4	Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen	<i>Neue Bridge-Gruppe</i>
Konfigurationsschnittstelle	Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen	<i>Nicht beachten</i>
efm35-60	Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen	<i>br1</i>
Konfigurationsschnittstelle	Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen	<i>Nicht beachten</i>

Konfiguration auf dem einwählenden Router

Feld	Menü	Wert
VLAN	WAN->Internet + Einwählen->PP-PoE-><Verbindung>-> 	<i>Aktiviert</i>
VLAN-ID	WAN->Internet + Einwählen->PP-PoE-><Verbindung>-> 	7

Nutzung weiterer Funktionen der be.IP

Feld	Menü	Wert
IP-Adresse	Assistenten->Erste Schritte->Grundeinstellungen	z. B. <i>192.168.2.2</i>
Dieses Gerät als DHCPv4-Server verwenden	Assistenten->Erste Schritte->Grundeinstellungen	<i>Aktiviert</i>
Standard-Gateway-IP-Adresse	Assistenten->Erste Schritte->Grundeinstellungen	z. B. <i>192.168.2.1</i>
DNS-Server 1	Assistenten->Erste Schritte->Grundeinstellungen	z. B. <i>192.168.2.1</i>

Kapitel 2 Konfigurationszugang für den Benutzer anlegen und spezielle Anwendungen verwenden

2.1 Einleitung

Der Administrator des Systems kann allen Benutzern einen individuellen Konfigurationszugang einrichten. So kann sich der Benutzer die wichtigsten persönlichen Einstellungen anzeigen lassen und bestimmte individuell anpassen. Dazu müssen in der Benutzer-HTML-Konfiguration **Benutzername** und **Passwort** eingetragen werden und der persönliche Zugang freigegeben sein.

Grundsätzlich gibt es zwei unterschiedliche Arten von Benutzerzugängen: Die der durch den Administrator frei definierbaren Zugänge, und die den Anwendungen System-Telefonbuch, Verbindungsdaten, Hotelfunktion und Mini-Callcenter zugeordneten Benutzer. Die vom Administrator erstellten Benutzer haben Zugriff auf eine stark reduzierte Konfigurationsoberfläche. Für die den Anwendungen zugeordneten Benutzern steht jeweils das den Anwendungen entsprechende Menü so zur Verfügung, wie es auch dem Administrator zur Verfügung steht.

Hilfe zu den verfügbaren Konfigurationsoptionen erhalten Sie über das Online-Hilfe-System.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.


Voraussetzungen

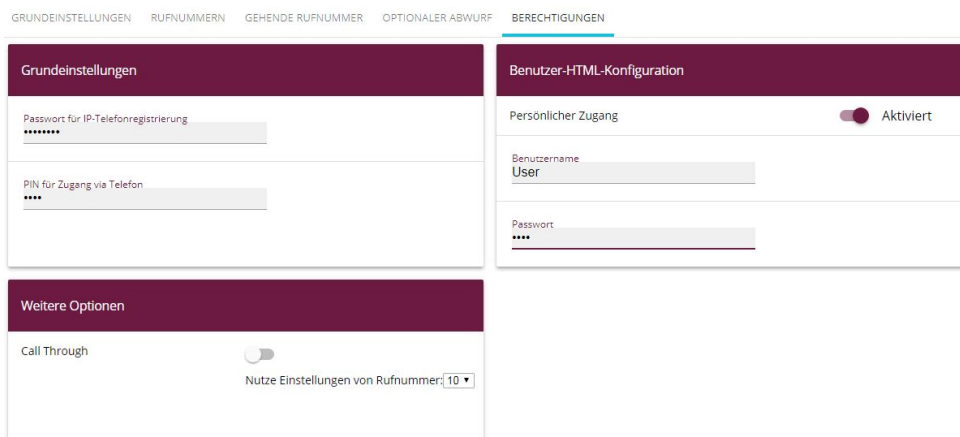
- Eine **be.IP** oder eine **be.IP plus**
- Ein konfiguriertes Basis-Szenario für Telefonie über VoIP oder ISDN und wahlweise ein konfiguriertes Szenario für Mini-Callcenter. Für die Konfiguration von Basis-Szenarien beachten Sie bitte die Anleitung in der **Kurzanleitung** und die entsprechenden **Workshops**.

2.2 Konfiguration

2.2.1 Konfigurationszugang für Benutzer ("User Portal")

Richten Sie jedem Benutzer Ihres Systems einen eigenen Konfigurationszugang (ein sogenanntes User Portal) ein, über den er seine Telefonie-Einstellungen ändern und Statusinformationen abrufen kann.

- (1) Gehen Sie zu **Nummerierung** -> **Benutzereinstellungen** -> **Benutzer** . Wählen Sie das Symbol , um vorhandenen Eintrag zu bearbeiten. Klicken Sie auf **Berechtigungen**.



The screenshot shows a web interface with a navigation bar at the top containing: GRUNDEINSTELLUNGEN, RUFNUMMERN, GEHENDE RUFNUMMER, OPTIONALER ABWURF, and **BERECHTIGUNGEN**. Below the navigation bar, there are three main configuration panels:

- Grundeinstellungen**: Contains two input fields: "Passwort für IP-Telefonregistrierung" (masked with 7 dots) and "PIN für Zugang via Telefon" (masked with 4 dots).
- Benutzer-HTML-Konfiguration**: Contains a toggle switch for "Persönlicher Zugang" (set to "Aktiviert"), a "Benutzername" field with the value "User", and a "Passwort" field (masked with 4 dots).
- Weitere Optionen**: Contains a "Call Through" toggle switch (set to off) and a dropdown menu labeled "Nutze Einstellungen von Rufnummer:" with the value "10".

Abb. 1: Nummerierung -> Benutzereinstellungen -> Benutzer ->  -> Berechtigungen

Gehen Sie folgendermaßen vor:

- (1) Aktivieren Sie **Persönlicher Zugang**.
- (2) Geben Sie einen **Benutzernamen** für diesen Benutzer ein, z. B. *User*.
- (3) Geben Sie ein **Passwort** für diesen Benutzer ein, z. B. *User*. Diese Angaben werden für den Login in die Benutzeroberfläche benötigt.
- (4) Klicken Sie auf **Übernehmen**.

Die Konfiguration ist hiermit abgeschlossen. Der Benutzer kann sich jetzt mit dem Benutzernamen und dem Passwort anmelden und bestimmte Konfigurierungen über die HTML-Konfiguration selbst vornehmen.

Ergebnis:

Benutzerdaten	
Name, Vorname	Benutzer 1 a/b1 Tel
Beschreibung	a/b1 Tel 10

Interne Rufnummern & Verbindungskosten	
10.a/b1 Tel 10	0,00 EUR

Weitere Einstellungen	
Aktuelle Berechtigungsklasse	Uneingeschränkt
Wahlberechtigung	Uneingeschränkt
Manuelle Bündelbelegung zulassen	Deaktiviert
Pick-Up-Gruppe	0

Abb. 2: Konfigurationsoberfläche des Benutzers

2.2.2 Anwendungen

Für die Anwendungen System-Telefonbuch, Verbindungsdaten und Mini-Callcenter-Management können Konfigurationszugänge durch den Administrator eingerichtet werden, über welche die jeweiligen Benutzer ihre speziellen Aufgaben erfüllen können.

System-Telefonbuch

Im Untermenü **Allgemein** legen Sie den Benutzernamen und das Passwort zur Administration des System-Telefonbuchs fest.

- (1) Gehen Sie zu **Anwendungen** -> **System-Telefonbuch** -> **Allgemein**.

Abb. 3: **Anwendungen -> System-Telefonbuch -> Allgemein**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie bei **Benutzername für Webzugang** einen Benutzernamen für den System-Telefonbuch-Administrator ein, z. B. *Zentrale*. Der Administrator kann im Bereich Telefonbuch das Telefonbuch einsehen, ändern und Daten importieren sowie exportieren.
- (2) Geben Sie ein **Passwort für Webzugang** für den System-Telefonbuch-Administrator ein, z. B. *Zentrale*.
- (3) Bestätigen Sie Ihre Angaben mit **OK**.

Ergebnis:

Beschreibung	Telefonnummer	Kurzwahl	Call Through

Seite: 1, Max. Anzahl 1000

Abb. 4: Konfigurationszugang System-Telefonbuch-Administrator

Verbindungsdaten

Für die Verwaltung der **Verbindungsdaten** des Systems können Sie einen speziellen Konfigurationszugang einrichten, über den die erfassten Daten der kommenden und gehenden Verbindungen eingesehen werden können. Außerdem kann die Art und das Format der erfassten Daten konfiguriert werden, aktuelle Datensätze können exportiert oder gelöscht werden.

- (1) Gehen Sie zu **Anwendungen -> Verbindungsdaten -> Allgemein**.

The screenshot shows two side-by-side panels. The left panel, titled 'Grundeinstellungen', contains the following fields and options:

- Benutzername für Webzugang Verbindungen: [Text input field]
- Passwort für Webzugang: [Password input field]
- Gehende Verbindungen speichern: Keine Alle Nur mit Projekt-Nummer
- Kommende Verbindungen speichern: Keine Alle Nur mit Projekt-Nummer
- Rufnummernverkürzung: Gehende Verbindungen [Nein] | Kommende Verbindungen [Nein]

The right panel, titled 'Aktionen', contains two buttons:

- Verbindungsdaten exportieren [EXPORTIEREN]
- Verbindungsdaten löschen [LÖSCHEN]

Abb. 5: **Anwendungen -> Verbindungsdaten -> Allgemein**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie bei **Benutzername für Webzugang** einen Benutzernamen für den Verbindungsdaten-Administrator ein, z. B. *Verbindungen*.
- (2) Geben Sie ein **Passwort für Webzugang** für den Verbindungsdaten-Administrator ein, z. B. *Verbindungen*.
- (3) Bestätigen Sie Ihre Angaben mit **OK**.

Ergebnis:

The screenshot shows a configuration page with a dark header 'Gehend'. Below the header, there is a field for 'Automatisches Aktualisierungsintervall' set to '60' and the unit 'Sekunden', with an 'ÜBERNEHMEN' button. At the bottom, there is a table with the following columns: Datum, Zeit, Dauer, Benutzer, Int. Rufnr., Angerufener Name, Gewählte Rufnummer, Projektnummer, Schnittstelle, and Kosten.

Abb. 6: *Konfigurationszugang Verbindungsdaten-Administrator*

Mini-Callcenter

Das Mini-Callcenter ist eine im System integrierte Call-Center Lösung für bis zu 16 Agents. Im Untermenü **Allgemein** können Sie einen HTML-Weboberflächen-Zugang für den Mini-Callcenter-Leiter einrichten. Dieser kann dann den Status der Leitungen und Agents überwachen und die Einstellungen der Leitungen und Agents ändern.

- (1) Gehen Sie zu **Anwendungen -> Mini-Callcenter -> Allgemein**.



Grundeinstellungen

Benutzername für Webzugang
Minicall

Passwort für Webzugang
•••••••

Abb. 7: **Anwendungen -> Mini-Callcenter -> Allgemein**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie bei **Benutzername für Webzugang** einen Benutzernamen für den Mini-Callcenter-Administrator ein, z. B. *Minicall*. Wenn sich ein Benutzer mit diesem Namen in die Benutzeroberfläche einloggt, steht ihm die Benutzeroberfläche mit ausgewählten Parametern für die Verwaltung des Callcenters zur Verfügung.
- (2) Geben Sie ein **Passwort für Webzugang** für den Mini-Callcenter-Administrator ein, z. B. *Minicall*.
- (3) Bestätigen Sie Ihre Angaben mit **OK**.

Ergebnis:



Status

Automatisches Aktualisierungsintervall 60 Sekunden ÜBERNEHMEN

Ansicht: Alle ▾

Abb. 8: Konfigurationszugang Mini-Callcenter-Administrator

2.3 Konfigurationsschritte im Überblick

Konfigurationszugang für Benutzer

Feld	Menü	Wert
Persönlicher Zugang	Nummerierung -> Benutzereinstellungen -> Benutzer -> Berechtigungen	Aktiviert
Benutzername	Nummerierung -> Benutzereinstellungen -> Benutzer -> Berechtigungen	z. B. <i>User</i>
Passwort	Nummerierung -> Benutzereinstellungen -> Benutzer -> Berechtigungen	z. B. <i>User</i>

System-Telefonbuch-Administration

Feld	Menü	Wert
Benutzername für Webzugang	Anwendungen -> System-Telefonbuch -> Allgemein	z. B. <i>Zentrale</i>
Passwort für Webzugang	Anwendungen -> System-Telefonbuch -> Allgemein	z. B. <i>Zentrale</i>

Verbindungsdaten-Administration

Feld	Menü	Wert
Benutzername für Webzugang	Anwendungen -> Verbindungsdaten -> Allgemein	z. B. <i>Verbindungen</i>
Passwort für Webzugang	Anwendungen -> Verbindungsdaten -> Allgemein	z. B. <i>Verbindungen</i>

Mini-Callcenter-Administration

Feld	Menü	Wert
Benutzername für Webzugang	Anwendungen -> Mini-Callcenter -> Allgemein	z. B. <i>Minicall</i>
Passwort für Webzugang	Anwendungen -> Mini-Callcenter -> Allgemein	z. B. <i>Minicall</i>

Kapitel 3 Zugriff aus dem WAN über HTTPS

3.1 Einleitung

Im Folgenden wird beschrieben, wie sie einen Zugriff aus dem WAN auf eine **be.IP** / **be.IP plus** über HTTPS konfigurieren.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

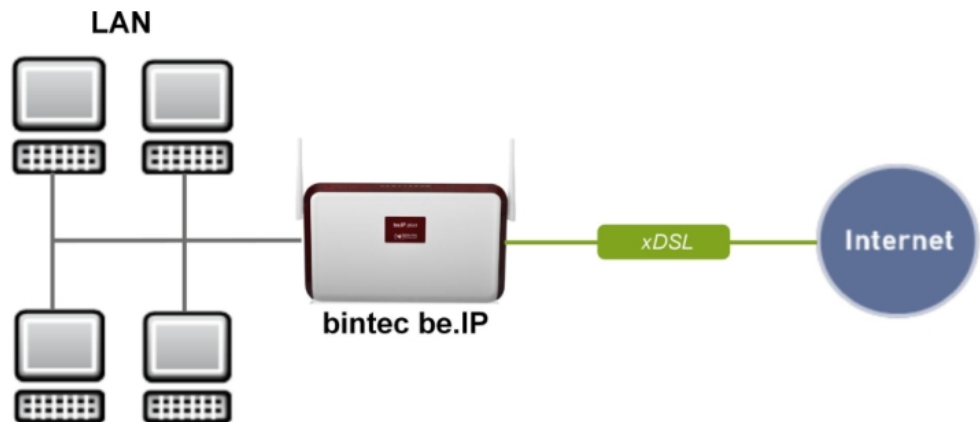


Abb. 9: Beispielszenario

Voraussetzungen

Eine **be.IP** oder eine **be.IP plus** mit aktueller Firmware, einer Grundkonfiguration und die Einstellung der **Ansicht** auf *Vollzugriff*.

3.2 Konfiguration

3.2.1 Network Address Translation (NAT) / Port Address Translation (PAT)

Die Anfrage an die offizielle IPv4-Adresse der **be.IP** (die der WAN-Verbindung) wird in eine lokale Adresse umgesetzt und an die gewünschte IPv4-Adresse im LAN (Exposed Host) oder an eine spezielle DMZ (demilitarisierte Zone; abgetrennte und mittels zusätzlicher Firewallregeln überwachte Schnittstelle) weitergeleitet. In unserem Beispiel ist das Ziel der Umsetzung die **be.IP** selbst, es wird daher der Localhost (127.0.0.1) verwendet.

Um Portscans auf die gängigen TCP-Ports (z. B. 22 (SSH), 23 (Telnet), 80 (HTTP), 443 (HTTPS)) keine Angriffsfläche zu bieten, konfigurieren Sie eine Port Address Translation (PAT) vom externen Port 4443 auf den internen Port 443.

- (1) Gehen Sie zu **Netzwerk->NAT->NAT-Konfiguration ->Neu**.

The screenshot shows the NAT configuration interface with the following settings:

- Basisparameter:**
 - Beschreibung: Admin_https_4443
 - Schnittstelle: WAN_GERMANY - TELEKOM ENTERTAIN
 - Art des Datenverkehrs: eingehend (Ziel-NAT)
- Ursprünglichen Datenverkehr angeben:**
 - Dienst: Benutzerdefiniert
 - Protokoll: TCP
 - Quell-IP-Adresse/Netzmaske: Beliebig
 - Original Ziel-IP-Adresse/Netzmaske: Beliebig
 - Original Ziel-Port/Bereich: Port angeben (dropdown) 4443 bis (dropdown)
- Substitutionswerte:**
 - Neue Ziel-IP-Adresse/Netzmaske: Host (dropdown) 127.0.0.1
 - Neuer Ziel-Port: Original (checkbox) 443

Abb. 10: **Netzwerk->NAT->NAT-Konfiguration ->Neu**

- (2) Geben Sie eine **Beschreibung** ein, z. B. *Admin_https_4443*.
- (3) Wählen Sie eine **Schnittstelle** aus, z. B. *WAN_GERMANY - TELEKOM ENTERTAIN*.
- (4) Belassen Sie die Einstellung **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*.
- (5) Belassen Sie den **Dienst** als *Benutzerdefiniert*.
- (6) Wählen Sie unter **Protokoll** *TCP*.
- (7) Wählen Sie **Original Ziel-Port/Bereich** = *Port angeben* und geben Sie *4443* ein.
- (8) Geben Sie bei der Option **Neue Ziel-IP-Adresse/Netzmaske** = *Host* den Wert *127.0.0.1* ein.
- (9) Unter **Neuer Ziel-Port** deaktivieren Sie *Original* und geben *443* ein.
- (10) Bestätigen Sie Ihre Einstellungen mit **OK**.

3.2.2 Stateful Inspection Firewall (SIF)

Die Firewall blockiert Pakete, die von der NAT durchgelassen wurden, da in der Standard-einstellung die WAN-Verbindung als „nicht vertrauenswürdig“ gilt. Es dürfen daher von dieser Schnittstelle keine initialen Anfragen gestellt werden, sondern nur Anfragen von „vertrauenswürdigen“ Schnittstellen beantwortet werden. (Standardmäßig gelten alle LAN-Schnittstellen als vertrauenswürdig.)

Sie müssen eine Regel konfigurieren, die den Zugriff der WAN-Schnittstelle als Ausnahme vom Standardverhalten erlaubt.



Hinweis

In der Firewall gilt die Regel, dass Pakete, die durch eine Regel erlaubt werden, später nicht mehr verboten werden können und umgekehrt. Die Reihenfolge der Regeln ist entscheidend!

In unserem Beispiel muss der Dienst HTTPS für den Zugriff von der WAN-Schnittstelle auf die lokale Schnittstelle `127.0.0.1` erlaubt werden.



Hinweis

HTTPS kann verwendet werden, weil PAT bereits erfolgt ist.

Im Beispiel sind alle benötigten Schnittstellen und der Dienst bereits vordefiniert, ggf. ist eine gesonderte Definition unter den Adressen bzw. Diensten im Vorfeld nötig.

(1) Gehen Sie zu **Firewall->Richtlinien->IPv4-Filterregeln->Neu**.

Basisparameter

Quelle	WAN_GERMANY - TELEKOM ENTERTAIN ▼
Ziel	LOCAL ▼
Dienst	http (SSL) ▼
Aktion	Zugriff ▼

Abb. 11: Firewall->Richtlinien->IPv4-Filterregeln->Neu

- (2) Wählen Sie eine **Quelle** z. B. `WAN_GERMANY_TELEKOM_ENTERTAIN`.
- (3) Wählen Sie das **Ziel** `LAN_LOCAL`.
- (4) Wählen Sie den **Dienst** `http (SSL)`.
- (5) Belassen Sie **Aktion** `Zugriff`.
- (6) Bestätigen Sie Ihre Einstellungen mit **OK**.

Unter **Firewall->Richtlinien->IPv4-Filterregeln** sehen Sie folgenden Überblick:

Filterregeln						
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv	
1	WAN_GERMANY - TELEKOM ENTERTAIN	LOCAL	http (SSL)	Zugriff	<input checked="" type="checkbox"/>	Aktiviert

Standardfilterregeln						
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv	
n+1	Vertrauenswürdige Schnittstellen		Bellebig	Bellebig	Zugriff	<input checked="" type="checkbox"/> Aktiviert
n+2	Nicht vertrauenswürdige Schnittstellen		Bellebig	Bellebig	Verweigern	<input checked="" type="checkbox"/> Aktiviert

Abb. 12: Firewall->Richtlinien->IPv4-Filterregeln

3.2.3 Administrativer Zugriff

Erlauben Sie als Nächstes den administrativen Zugriff auf die Konfigurationsoberfläche der **be.IP** für das gewünschte Szenario. Hierzu muss zuerst die WAN-Schnittstelle der Liste der Schnittstellen hinzugefügt werden und dann der Zugriff mit dem Dienst `HTTPS` erlaubt werden.

- (1) Gehen Sie zu **Systemverwaltung -> Administrativer Zugriff -> Zugriff**.

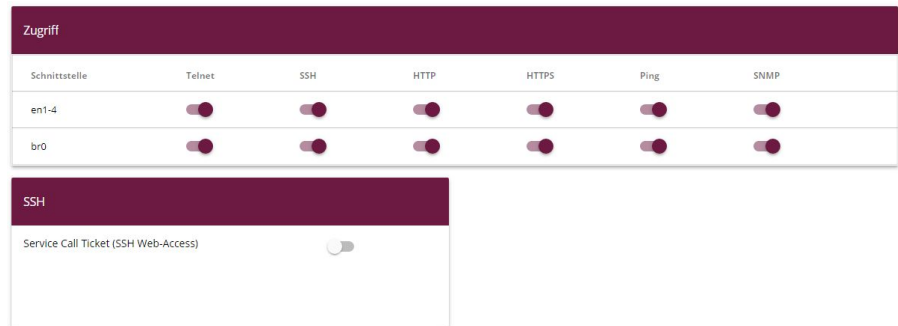


Abb. 13: **Systemverwaltung -> Administrativer Zugriff -> Zugriff**

- (2) Klicken Sie auf **Hinzufügen**, um die WAN-Schnittstelle hinzuzufügen.
 (3) Wählen Sie die WAN-Schnittstelle aus, z. B. *Germany - Telekom Entertain*.



Abb. 14: **Systemverwaltung -> Administrativer Zugriff -> Zugriff -> Hinzufügen**

- (4) Bestätigen Sie Ihre Auswahl mit **OK**.
 (5) Erlauben Sie den Zugriff mit dem Dienst HTTPS.

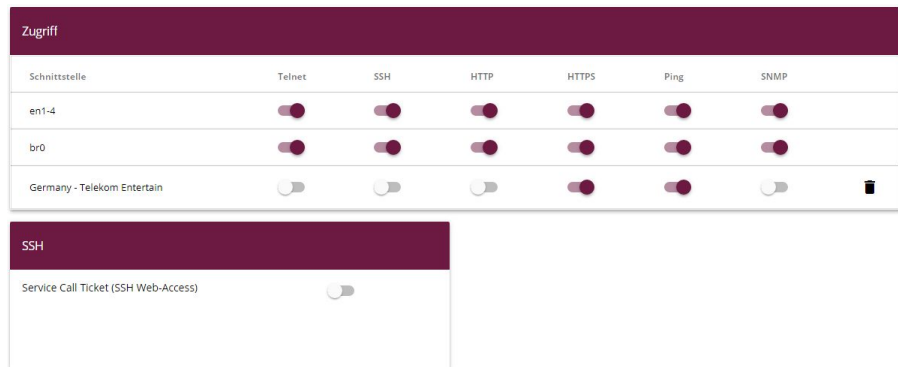
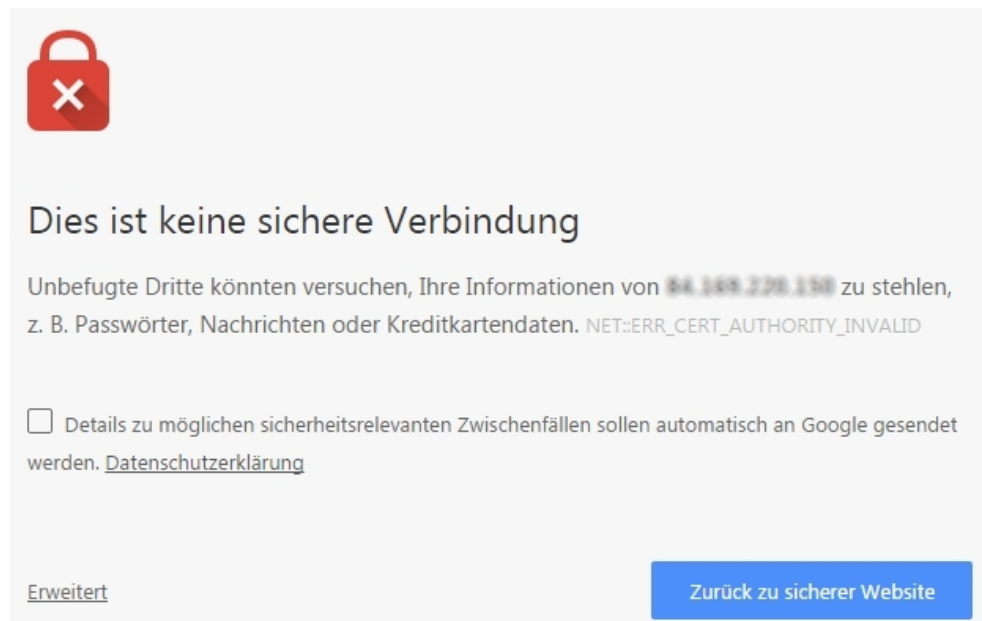


Abb. 15: **Systemverwaltung -> Administrativer Zugriff -> Zugriff -> Hinzufügen**

- (6) Aktivieren Sie in der Zeile **Germany - Telekom Entertain** das Kontrollkästchen in der Spalte *HTTPS*.
- (7) Bestätigen Sie Ihre Einstellungen mit **OK**.
- (8) Sichern Sie die Konfiguration mit **Konfiguration speichern**.

3.2.4 Zugriff aus dem WAN

Ein Zugriff aus dem WAN auf die offizielle IPv4-Adresse der WAN-Verbindung mit dem Port 4443 führt zum Hinweis auf eine „nicht sichere Verbindung“, da im Browser das von der **be.IP** hinterlegte Zertifikat nicht über eine ihm bekannte CA verifiziert werden kann.



Wenn Sie die Verbindung trotzdem zulassen, gelangen Sie zur Login-Seite der **be.IP**.

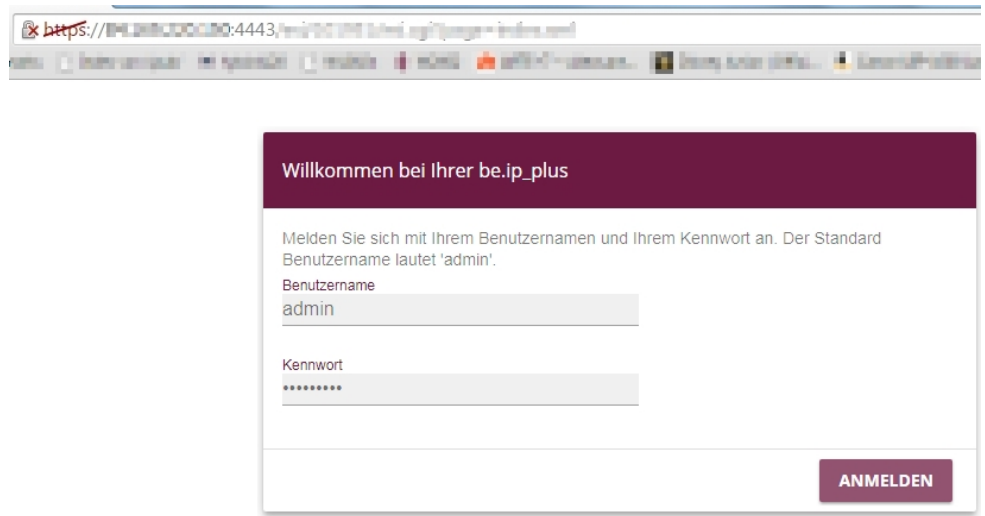


Abb. 18: Login-Seite der **be.IP**

Wenn die Sicherheitswarnung nicht mehr erscheinen soll, müssen Sie ein Zertifikat erwerben, das vom Browser als sicher eingestuft wird und dieses in der **be.IP** hinterlegen.

3.3 Konfigurationsschritte im Überblick

NAT / PAT

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>Ad-min_https_4443</i>
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>WAN_GERMANY - PROVIDER</i>
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>eingehend (Ziel-NAT)</i>
Dienst	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Benutzerdefiniert</i>
Protokoll	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>TCP</i>
Original Ziel-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Port angeben: 4443</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Host: 127.0.0.1</i>
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Original deaktivieren, 443</i>

SIF

Feld	Menü	Wert
Quelle	Firewall->Richtlinien->IPv4- Filterregeln->Neu	z. B. <i>WAN_GERMANY-PROVIDER</i>
Ziel	Firewall->Richtlinien->IPv4- Filterregeln->Neu	<i>LAN_LOCAL</i>
Dienst	Firewall->Richtlinien->IPv4- Filterregeln->Neu	<i>http (SSL)</i>
Aktion	Firewall->Richtlinien->IPv4- Filterregeln->Neu	<i>Zugriff</i>

Administrativer Zugriff

Feld	Menü	Wert
Schnittstelle	Systemverwaltung->Administrativer Zugriff->Zugriff->Hinzufügen	z. B. <i>Germany - Provider</i>

Feld	Menü	Wert
Germany - Telekom Entertain	Systemverwaltung ->Administra- tiver Zugriff->Zugriff	HTTPS aktiviert

Kapitel 4 Zugriff aus dem WAN auf einen WEB-Server im LAN

4.1 Einleitung

Im Folgenden wird beschrieben, wie Sie ein Zugriff aus dem WAN über HTTP auf einen WEB-Server konfigurieren.

Zur Konfiguration wird das **GUI** (Graphic User Inteface) verwendet.

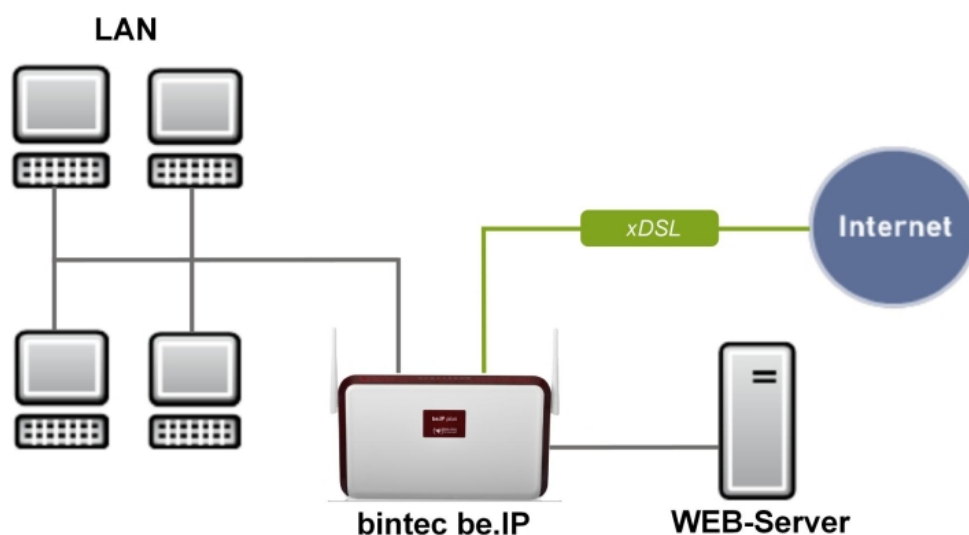


Abb. 19: Beispielszenario

Voraussetzungen

Eine **be.IP** oder eine **be.IP plus** mit aktueller Firmware, einer Grundkonfiguration und in der **Ansicht = Vollzugriff**.

4.2 Konfiguration

4.2.1 Network Address Translation (NAT) / Port Address Trans-

lation (PAT)

Die Anfrage an die offizielle IPv4-Adresse der **be.IP** (die der WAN-Verbindung) wird auf eine lokale Adresse umgesetzt und an die gewünschte IPv4 Adresse im LAN (Exposed Host) oder an eine spezielle DMZ (demilitarisierte Zone; abgetrennte und mittels zusätzlicher Firewallregeln überwachte Schnittstelle) weitergeleitet. In unserem Beispiel ist das Ziel der Umsetzung ein Web-Server.

Um Portscans auf die gängigen TCP Ports (z. B. 22 (SSH), 23 (Telnet), 80 (HTTP), 443 (HTTPS)) keine Angriffsfläche zu bieten, können Sie eine Port Address Translation (PAT) vom externen Port 8080 auf den internen Port 80 konfigurieren. Für die weitere Konfiguration ist dies jedoch keine Voraussetzung.

Konfiguration ohne PAT

Bei einer Konfiguration ohne PAT gehen Sie folgendermaßen vor:

- (1) Gehen Sie zu **Netzwerk->NAT->NAT-Konfiguration ->Neu**.

The screenshot shows a configuration interface for NAT. It is divided into two main sections: 'Basisparameter' and 'Ursprünglichen Datenverkehr angeben'.

Basisparameter:

- Beschreibung:** WEB-Server
- Schnittstelle:** WAN_WAN-PROVIDER
- Art des Datenverkehrs:** eingehend (Ziel-NAT)

Ursprünglichen Datenverkehr angeben:

- Dienst:** http
- Quell-IP-Adresse/Netzmaske:** Beliebig
- Original Ziel-IP-Adresse/Netzmaske:** Beliebig

Substitutionswerte:

- Neue Ziel-IP-Adresse/Netzmaske:** Host | 192.168.2.10
- Neuer Ziel-Port:** Original

Abb. 20: **Netzwerk->NAT->NAT-Konfiguration ->Neu**

- (2) Geben Sie eine **Beschreibung** ein, z. B. *WEB-Server*.
- (3) Wählen Sie eine **Schnittstelle** aus, z. B. *WAN_WAN-Provider* als Schnittstelle der WAN-Verbindung.
- (4) Belassen Sie die Einstellung **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*.
- (5) Wählen Sie den **Dienst** = *http*.
- (6) Geben Sie mit **Neue Ziel-IP-Adresse/Netzmaske** = *Host* den Wert *192.168.2.10* als IP-Adresse des WEB-Servers ein.
- (7) Belassen Sie **Neuer Ziel-Port** = *Original*.
- (8) Bestätigen Sie Ihre Einstellungen mit **OK**.

Konfiguration mit PAT

Gehen Sie alternativ zu einer Konfiguration ohne PAT bei einer Konfiguration mit PAT folgendermaßen vor:

- (1) Gehen Sie zu **Netzwerk->NAT->NAT-Konfiguration ->Neu**.

The screenshot shows the configuration interface for NAT. It is divided into three main sections:

- Basisparameter:**
 - Beschreibung: WEB-Server
 - Schnittstelle: WAN_WAN-PROVIDER
 - Art des Datenverkehrs: eingehend (Ziel-NAT)
- Ursprünglichen Datenverkehr angeben:**
 - Dienst: Benutzerdefiniert
 - Protokoll: TCP
 - Quell-IP-Adresse/Netzmaske: Beliebig
 - Original Ziel-IP-Adresse/Netzmaske: Beliebig
 - Original Ziel-Port/Bereich: Port angeben, 8080 bis
- Substitutionswerte:**
 - Neue Ziel-IP-Adresse/Netzmaske: Host, 192.168.2.10
 - Neuer Ziel-Port: Original (deaktiviert), 80

Abb. 21: **Netzwerk->NAT->NAT-Konfiguration ->Neu**

- (2) Geben Sie eine **Beschreibung** ein, z. B. *WEB-Server*.
- (3) Wählen Sie eine **Schnittstelle** aus, z. B. *WAN_WAN-Provider* als Schnittstelle der WAN-Verbindung.
- (4) Belassen Sie die Einstellung **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*.
- (5) Belassen Sie den **Dienst** als *Benutzerdefiniert*.
- (6) Wählen Sie unter **Protokoll** *TCP*.
- (7) Wählen Sie **Original Ziel-Port/Bereich** = *Port angeben* und geben Sie *8080* ein.
- (8) Geben Sie mit **Neue Ziel-IP-Adresse/Netzmaske** = *Host* den Wert *192.168.2.10* als IP-Adresse des WEB-Servers ein.
- (9) Unter **Neuer Ziel-Port** deaktivieren Sie *Original* und geben *80* ein.
- (10) Bestätigen Sie Ihre Einstellungen mit **OK**.

4.2.2 Stateful Inspection Firewall (SIF)

Die Firewall blockiert die Pakete, die von der NAT durchgelassen wurden, da in der Standardeinstellung die WAN-Verbindung als „nicht vertrauenswürdig“ gilt. Es dürfen daher von dieser Schnittstelle keine initialen Anfragen gestellt werden, sondern nur Anfragen von „vertrauenswürdigen“ Schnittstellen beantwortet werden. (Standardmäßig gelten alle LAN-Schnittstellen als vertrauenswürdig.)

Sie müssen eine Regel konfigurieren, die den Zugriff seitens der WAN-Schnittstelle als Ausnahme vom Standardverhalten erlaubt.



Hinweis

In der Firewall gilt die Regel, dass Pakete, die durch eine Regel erlaubt werden, später nicht mehr verboten werden können und umgekehrt. Die Reihenfolge der Regeln ist entscheidend!

In unserem Beispiel muss der Dienst HTTP für den Zugriff seitens der WAN-Schnittstelle auf die Schnittstelle `192.168.2.10` erlaubt werden.

Im Beispiel sind alle benötigten Schnittstellen und der Dienst bereits vordefiniert, ggf. ist eine gesonderte Definition unter den Adressen bzw. Diensten im Vorfeld nötig.

(1) Gehen Sie zu **Firewall->Adressen->Adressliste->Neu**.

Basisparameter	
Beschreibung	WEB-Server
IPv4	<input checked="" type="checkbox"/> Aktiviert
Adresstyp	<input checked="" type="radio"/> Adresse/Subnetz <input type="radio"/> Adressbereich
Adresse/Subnetz	192.168.2.10 / 255.255.255.0
IPv6	<input type="checkbox"/>

Abb. 22: Firewall->Adressen->Adressliste->Neu

- (2) Geben Sie eine **Beschreibung** ein, z. B. *WEB-Server*.
- (3) Belassen Sie **IPv4** *Aktiviert*.
- (4) Belassen Sie **Adresstyp** = *Adresse/Subnetz*.
- (5) Geben Sie unter **Adresse/Subnetz** z. B. *192.168.2.10* als Adresse des WEB-Servers ein.
- (6) Bestätigen Sie Ihre Einstellungen mit **OK**.
- (1) Gehen Sie zu **Firewall->Richtlinien->IPv4-Filterregeln->Neu**.

Basisparameter	
Quelle	WAN_WAN-PROVIDER
Ziel	WEB-Server
Dienst	http
Aktion	Zugriff

Abb. 23: Firewall->Richtlinien->IPv4-Filterregeln->Neu

- (2) Wählen Sie eine **Quelle** z. B. *WAN_WAN-PROVIDER*.

- (3) Wählen Sie das **Ziel** *WEB-Server*.
- (4) Wählen Sie den **Dienst** *http*.
- (5) Belassen Sie **Aktion** *Zugriff*.
- (6) Bestätigen Sie Ihre Einstellungen mit **OK**.

Unter **Firewall->Richtlinien->IPv4-Filterregeln** sehen Sie folgenden Überblick:

Filterregeln						
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv	
1	WAN_WAN-PROVIDER	WEB-Server	http	Zugriff	<input checked="" type="checkbox"/>	Aktiviert

Standardfilterregeln						
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv	
n+1	Vertrauenswürdige Schnittstellen		Beliebig	Beliebig	Zugriff	<input checked="" type="checkbox"/> Aktiviert
n+2	Nicht vertrauenswürdige Schnittstellen		Beliebig	Beliebig	Verweigern	<input checked="" type="checkbox"/> Aktiviert

Abb. 24: Firewall->Richtlinien->IPv4-Filterregeln

4.3 Konfigurationsschritte im Überblick

NAT / ohne PAT

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>WEB-Server</i>
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>WAN_WAN-Provider</i>
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>eingehend (Ziel-NAT)</i>
Dienst	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>http</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Host: 192.168.2.10</i>
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Original</i>

NAT / mit PAT

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>WEB-Server</i>
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>WAN_WAN-Provider</i>
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>eingehend (Ziel-NAT)</i>
Dienst	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Benutzerdefiniert</i>
Protokoll	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>TCP</i>
Original Ziel-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Port angeben: 8080</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Host: 192.168.2.10</i>
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Original deaktivieren, 80</i>

SIF

Feld	Menü	Wert
Beschreibung	Firewall ->Adressen ->Adressliste ->NeuNeu	<i>WEB-Server</i>
IPv4	Firewall ->Adressen ->Adressliste ->Neu	<i>Aktiviert</i>
Adresstyp	Firewall ->Adressen ->Adressliste ->Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall ->Adressen ->Adressliste ->Neu	z. B. <i>192.168.2.10/255.255.255.0</i>
Quelle	Firewall->Richtlinien->IPv4- Filterregeln->Neu	z. B. <i>WAN_WAN-PROVIDER</i>
Ziel	Firewall->Richtlinien->IPv4- Filterregeln->Neu	<i>WEB-Server</i>
Dienst	Firewall->Richtlinien->IPv4- Filterregeln->Neu	<i>http</i>
Aktion	Firewall->Richtlinien->IPv4- Filterregeln->Neu	<i>Zugriff</i>

Kapitel 5 Einwahl eines iPhone auf einer be.IP mit IPsec IKEv1

5.1 Einleitung

Im Folgenden wird beschrieben, wie sich ein iPhone über einen IPsec-VPN-Tunnel auf einer **be.IP** oder einer **be.IP plus** einwählt.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

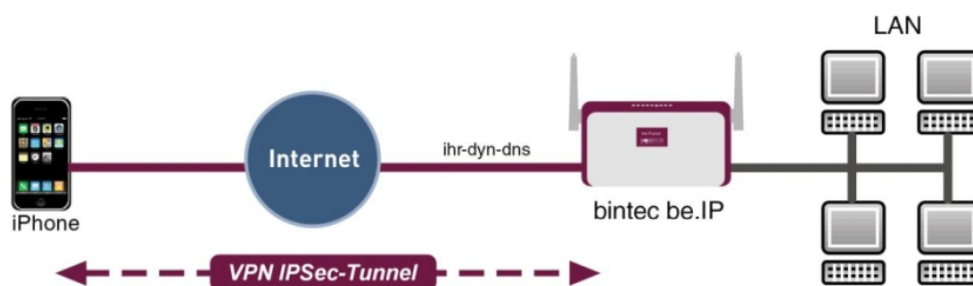


Abb. 25: Beispielszenario

Voraussetzungen

- Eine **be.IP** oder eine **be.IP plus**
- Eine bestehende Konfiguration wie sie von einem durchlaufenen **Schnellstartassistenten** angelegt wird.
- Die BOSS-Version V.10.1 Rev. 5 oder höher. Die BOSS-Version Ihrer **be.IP** können Sie im Menü **Systemverwaltung** -> **Status** überprüfen.

5.2 Konfiguration

5.2.1 Anlegen des Einwahlprofils über den Assistenten

Verlassen Sie den Assistenten **Schnellstart**, indem Sie in der Kopfleiste unter **Ansicht Vollzugriff** wählen. Erstellen Sie zuerst die VPN-Verbindung.

Gehen Sie dazu in das Menü **Assistenten->VPN->VPN-Verbindungen->Neu**.

Wählen Sie das VPN-Szenario aus: ?

VPN-Szenario IPSec - Einwahl eines einzelnen Clients ▾

Abb. 26: Assistenten->VPN->VPN-Verbindungen->Neu

Gehen Sie folgendermaßen vor:

- (1) Bei **VPN-Szenario** wählen Sie *IPSec - Einwahl eines einzelnen Clients* aus.
- (2) Klicken Sie auf **Weiter**, um Ihre Auswahl zu bestätigen.

Im nächsten Schritt geben Sie die erforderlichen Daten für das IPSec-Szenario ein.

Verbindungsdetails ?

Beschreibung

Lokale IPSec ID

Entfernte IPSec ID

Preshared Key

Entferntes Netzwerk ?

Lokale Netzwerke

IP-Adresse	Netzmaske
192.168.4.251	255.255.255.0
192.168.0.251	255.255.255.0

IP-Adresspool auswählen DHCP Adressbereich ▾

IP-Adresspool für Einwahl-Clients 192.168.0.10-192.168.0.30

Weitere Konfigurationsschritte auswählen: ?

Konfigurationsdatei für bintec Secure IPSec Client exportieren

Abb. 27: Assistenten->VPN->VPN-Verbindungen->Weiter

Gehen Sie folgendermaßen vor:

- (1) Bei **Beschreibung** geben Sie einen Namen für die Verbindung, z. B. *iPhone-Einwahl* ein.
- (2) Bei **Entfernte IPSec ID** geben Sie die ID des entfernten IPSec-Peers ein, z. B. *iPho-*

ne_peer.

- (3) Für die Authentifizierung wird **Preshared Key** verwendet. Es wird eine Kombination aus Buchstaben, Zahlen und Sonderzeichen empfohlen.
- (4) Unter **IP-Adresspool auswählen** wählen Sie *DHCP Adressbereich intern* aus.
- (5) Die **Lokale IPSec ID** lassen Sie bitte unverändert.
- (6) Bestätigen Sie Ihre Angaben mit **OK**.

5.2.2 Anlegen / Ändern der iPhone-spezifischen Parameter

Das iPhone benötigt spezielle IPSec-Einstellungen sowie ein XAUTH-Profil.

Gehen Sie in das Menü **VPN ->IPSec->XAUTH-Profile-> Neu**.

Basisparameter

Beschreibung
XAUTH-Pool

Rolle Server ▼

Modus Lokal ▼

Benutzer

Name	Passwort
iPhone_xauth

HINZUFÜGEN

Abb. 28: **VPN ->IPSec->XAUTH-Profile-> Neu**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine **Beschreibung** für das XAUTH-Profil ein, z. B. *XAUTH-Pool*.
- (2) Als **Rolle** wählen Sie *Server* aus.
- (3) Als **Modus** wählen Sie *Lokal* aus.

- (4) Zur besseren Unterscheidung vom Namen des IPSec-Peers geben Sie hier bei **Benutzer** für **Name** z. B. *iPhone_xauth* ein.
- (5) Geben Sie das Authentifizierungspasswort (**Passwort**) ein.
- (6) Bestätigen Sie mit **OK**.

Im nächsten Schritt muss das Profil für Phase 2 angepasst werden.

Gehen Sie in das Menü **VPN->IPSec->Phase-2-Profile**.

IPSec-Phase-2-Profile					
Standard	Beschreibung	Proposals	PFS-Gruppe	Lebensdauer	
<input checked="" type="radio"/>	Multi-Proposal	[ESP(AES/SHA-2)] [ESP(AES/SHA-1)] [ESP(3DES/SHA-1)]	5(1536 Bit)	0KB / 2h / 80%	 
<input type="radio"/>	wz_ipsec_1	[ESP(AES-128/SHA-1)]	5(1536 Bit)	0KB / 8h / 80%	 

Abb. 29: **VPN->IPSec->Phase-2-Profile**

Klicken Sie auf das -Symbol, um das konfigurierte Profil *wz_ipsec_1* zu bearbeiten.

Phase-2-Parameter (IPSEC)

Beschreibung
wz_ipsec_1

Proposals

Verschlüsselung	Authentifizierung	Aktiviert
AES-128 ▼	SHA1 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input type="checkbox"/>

PFS-Gruppe verwenden 2(1024 Bit) ▼

Lebensdauer

7200 Sekunden 0 kBytes Schlüssel erneut

erstellen nach 80 % Lebensdauer

Abb. 30: VPN->IPSec->Phase-2-Profile ✎

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Proposals** die **Authentifizierung** *SHA1* aus.



Hinweis

Es ist wichtig, dass Sie NICHT SHA2 auswählen!

- (2) Deaktivieren Sie die Option **PFS-Gruppe verwenden**.
- (3) Bestätigen Sie Ihre Eingaben mit **OK**.

Ebenso wie für die Phase 2 muss das Profil für die Phase 1 angepasst werden.

Gehen Sie in das Menü **VPN->IPSec->Phase-1-Profile**.

IKEv1 (Internet Key Exchange, Version 1)						
Standard	Beschreibung	Proposals	Authentifizierung	Modus	DH-Gruppe	Lebensdauer
<input type="radio"/>	wz_ike_1	[AES/SHA1]	Preshared Keys	Aggressiv	5(1536 Bit)	0KB / 8h
<input checked="" type="radio"/>	Multi-Proposal	[AES/SHA2 256][AES/SHA1][3DES/SHA1]	Preshared Keys	Aggressiv	5(1536 Bit)	0KB / 4h
NEUES IKEV1-PROFIL ERSTELLEN						

IKEv2 (Internet Key Exchange, Version 2)			
Standard	Beschreibung	Proposals	Lebensdauer
<input checked="" type="radio"/>	Multiproposal	[AES/SHA2 256][AES/SHA1][3DES/SHA2 256][3DES/SHA1]	4h
NEUES IKEV2-PROFIL ERSTELLEN			

Abb. 31: VPN->IPSec->Phase-1-Profile

Klicken Sie auf das -Symbol, um das konfigurierte Profil `wz_ike_1` zu bearbeiten.

Phase-1-Parameter (IKE)

Beschreibung
wz_ike_1

Proposals

Verschlüsselung	Authentifizierung	Aktiviert
AES	SHA1	<input checked="" type="checkbox"/>
AES	MD5	<input type="checkbox"/>
AES	MD5	<input type="checkbox"/>

DH-Gruppe 2(1024 Bit)

Lebensdauer 14400 Sekunden 0 kBytes

Authentifizierungsmethode Preshared Keys

Modus Main Modus (ID Protect) Aggressiv Strikt

Lokaler ID-Typ Fully Qualified Domain Name (FQDN)

Lokaler ID-Wert
be.ip_plus

Abb. 32: VPN->IPsec->Phase-1-Profil ✎

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Proposals** die **Authentifizierung** *SHA1* aus.



Hinweis

Es ist wichtig, dass Sie NICHT SHA2 auswählen!

- (2) Wählen Sie die **DH-Gruppe 2 (1024 Bit)** aus.
- (3) Klicken Sie auf **Erweiterte Einstellungen**.
- (4) Wählen Sie bei **Erreichbarkeitsprüfung** die Option *Dead Peer Detection (Idle)* aus.
- (5) Bestätigen Sie Ihre Angaben mit **OK**.

Anschließend muss der IPSec-Peer angepasst werden.

Gehen Sie in das Menü **VPN->IPSec->IPSec-Peers**.

IKEv1 (Internet Key Exchange, Version 1)							
Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status	Aktion
IPSec-Statische-Peers							
1	iPhone-Einwahl		iPhone_peer	wz_ike_1	wz_ipsec_1		

IKEv2 (Internet Key Exchange, Version 2)							
Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status	Aktion

Abb. 33: **VPN->IPSec->IPSec-Peers**

Klicken Sie auf das -Symbol, um das konfigurierte Profil *iPhone-Einwahl* zu bearbeiten.

The screenshot shows two panels of the VPN configuration interface. The left panel, titled 'Peer-Parameter', includes fields for 'Administrativer Status' (Aktiv), 'Beschreibung' (iPhone-Einwahl), 'Peer-Adresse' (IP-Version: IPv4 bevorzugt), 'Peer-ID' (Schlüssel-ID), 'IKE (Internet Key Exchange)' (IKEv1), 'Preshared Key', and 'IP-Version des Tunnelnetzwerks' (IPv4). The right panel, titled 'IPv4-Schnittstellenrouten', includes 'Sicherheitsrichtlinie' (Vertrauenswürdig), 'IPv4-Adressvergabe' (Server im IKE-Konfigurationsmodus), 'Konfigurationsmodus' (Pull), 'IPv4-Zuordnungs-Pool' (DHCP Adressbereich), and 'Lokale IPv4-Adresse' (192.168.0.101).

Abb. 34: VPN->IPSec->IPSec-Peers 

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie über das Drop-Down-Menü bei **Peer-ID** den Wert *Schlüssel-ID* aus.
- (2) Klicken Sie auf **Erweiterte Einstellungen**.

The screenshot shows the 'Erweiterte Einstellungen' (Advanced Settings) interface. It is divided into two main sections: 'Erweiterte IPsec-Optionen' and 'Erweiterte IP-Optionen'. The 'Erweiterte IPsec-Optionen' section includes 'Phase-1-Profil' (wz_ike_1), 'Phase-2-Profil' (wz_ipsec_1), 'XAUTH-Profil' (XAUTH-Pool), 'Anzahl erlaubter Verbindungen' (Ein Benutzer), and 'Startmodus' (Auf Anforderung). The 'Erweiterte IP-Optionen' section includes 'Öffentliche Schnittstelle' (Vom Routing ausgewählt), 'Öffentliche IPv4-Quelladresse' (disabled), 'Öffentliche IPv6-Quelladresse' (disabled), 'Überprüfung der IPv4-Rückroute' (disabled), and 'IPv4 Proxy ARP' (Nur aktiv).

Abb. 35: VPN->IPSec->IPSec-Peers->  -> **Erweiterte Einstellungen**


- (3) Überprüfen Sie ob die folgenden Werte ausgewählt sind:
- (4) **Phase-1-Profil**: *wz_ike_1*
- (5) **Phase-2-Profil**: *wz_ipsec_1*
- (6) **XAUTH-Profil**: in unserem Beispiel *XAUTH-Pool* (das von Ihnen angelegte XAUTH-Profil)
- (7) Wählen Sie unter **IPv4 Proxy ARP** die Option *Nur aktiv* aus.
- (8) Bestätigen Sie Ihre Angaben mit **OK**.

Damit das iPhone eine DNS-Auflösung vornehmen kann, muss noch im DHCP-Pool der DNS-Server angegeben werden.

Gehen Sie dazu in das Menü **Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration** .

IP Pools:			
IP-Poolname	IP-Adressbereich	Primärer DNS-Server	Sekundärer DNS-Server
DHCP Adressbereich	192.168.0.10 - 192.168.0.30	0.0.0.0	0.0.0.0

Abb. 36: Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration

Klicken Sie auf das -Symbol, um *DHCP Adressbereich intern* zu bearbeiten.

Basisparameter

IP-Poolname
DHCP Adressbereich intern

IP-Adressbereich
192.168.0.10 - 192.168.0.30

DNS-Server

Primär
192.168.0.1

Sekundär

Abb. 37: Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration 

Gehen Sie folgendermaßen vor:

- (1) Geben Sie bei **DNS-Server** die Primäre IP-Adresse des DNS-Servers ein. Normalerweise handelt sich dabei um die IP-Adresse der **be.IP**. Standardmäßig ist das die IP-Adresse *192.168.0.1*.
- (2) Bestätigen Sie Ihre Angaben mit **OK**.

Die Konfiguration ist hiermit abgeschlossen. Sichern Sie die aktuelle Konfiguration über die Schaltfläche **Konfiguration speichern** als Boot-Konfiguration.

5.3 Anlegen des Einwahlprofils auf dem iPhone

Im letzten Schritt wird nun das IPsec-Profil auf dem iPhone angelegt.

Wählen Sie dazu **Einstellungen** -> **VPN** -> **VPN hinzufügen**.



Hinweis

Beachten Sie, dass ab iOS 10 die Standardeinstellung für VPN-Profile *IKEv2* ist.

IKEv1 steht aber nach wie vor zur Verfügung. Tippen Sie auf den Menüpunkt **Typ** und wählen Sie in der folgenden Auswahl *IPsec* aus. Danach stehen wieder die im Folgenden verwendeten Optionen zur Verfügung.

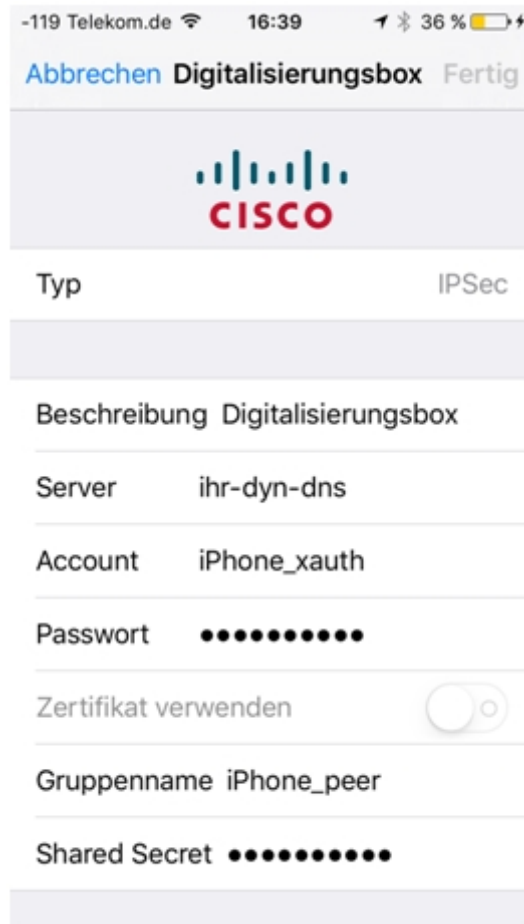


Abb. 38: **Einstellungen** -> **VPN** -> **VPN hinzufügen**

Sie sehen folgende Daten auf Ihrem Display:

Typ: IPSec

Server: Ihre feste öffentliche IP-Adresse oder DynDNS

Passwort: Passwort des XAUTH Profil-Users

Gruppenname: Name des IPSec Peers, den Sie unter IPSec Peers erstellt haben

Shared Secret: Passwort, das Sie für den IPSec Peer verwendet haben

5.4 Konfigurationsschritte im Überblick



Anlegen des Einwahlprofils über den Assistenten

Feld	Menü	Wert
VPN-Szenario	Assistenten->VPN->VPN-Verbindungen->Neu	<i>IPSec - Einwahl eines einzelnen Clients</i>
Beschreibung	Assistenten->VPN->VPN-Verbindungen->Weiter	z. B. <i>iPhone-Einwahl</i>
Entfernte IPSec ID	Assistenten->VPN->VPN-Verbindungen->Weiter	z. B. <i>iPhone_peer</i>
Preshared Key	Assistenten->VPN->VPN-Verbindungen->Weiter	z. B. <i>SuperSecret</i>
IP-Adresspool auswählen	Assistenten->VPN->VPN-Verbindungen->Weiter	<i>DHCP Adressbereich intern</i>

Anlegen / Änderung der iPhone spezifischen Parameter

Feld	Menü	Wert
Beschreibung	VPN ->IPSec->XAUTH-Profil->Neu	z. B. <i>XAUTH-Pool</i>
Rolle	VPN ->IPSec->XAUTH-Profil->Neu	<i>Server</i>
Modus	VPN ->IPSec->XAUTH-Profil->Neu	<i>Lokal</i>
Benutzer	VPN ->IPSec->XAUTH-Profil->Neu	Name z. B. <i>iPhone_xauth</i> Passwort z. B. <i>SuperSecret</i>



Phase-2-Profil anpassen

Feld	Menü	Wert
Proposals	VPN->IPSec->Phase-1-Profil-> 	Authentifizierung <i>SHA1</i>
PFS-Gruppe verwenden	VPN->IPSec->Phase-1-Profil-> 	<i>Deaktiviert</i>


Phase-1-Profil anpassen

Feld	Menü	Wert
Proposals	VPN->IPSec->Phase-1-Profile-> 	Authentifizierung <i>SHA1</i>
DH-Gruppe	VPN->IPSec->Phase-1-Profile-> 	2 (1024 Bit)
Erreichbarkeitsprüfung	VPN->IPSec->Phase-1-Profile->  ->Erweiterte Einstellungen	Dead Peer Detecti- on (Idle)

IPSec-Peers anpassen

Feld	Menü	Wert
Peer-ID	VPN->IPSec->IPSec-Peers-> 	Schlüssel-ID
IPv4 Proxy ARP	VPN->IPSec->IPSec-Peers->  ->Erweiterte Einstellungen	Nur aktiv

IP-Pool konfigurieren

Feld	Menü	Wert
DNS-Server	Lokale Dienste->DHCP-Server->IP- Pool-Konfiguration-> 	Primär z. B. 192.168.0.1

Kapitel 6 Zugriff aus dem WAN über die PP-PoE-WAN-Verbindung

6.1 Einleitung

Im Folgenden werden die NAT- und Firewall-Einstellungen am Beispiel eines „Exposed Host“ zum IPv4-Zugriff aus dem WAN auf ein Internet Gateway über die PPPoE-WAN-Verbindung einer **be.IP** beschrieben.

Voraussetzungen

- Eine **be.IP** mit aktueller Firmwareversion in der **Ansicht** = *Vollzugriff*.
- Ein bestehendes Internet Gateway (z. B. Firewall Appliance) soll weiterhin aus dem Internet für alle Dienste erreichbar sein (z. B. für IPSec) und als Default Gateway und Firewall für den Datenverkehr des schon bestehenden Netzwerkes arbeiten, die IP- Telefonie und alle damit verbundenen Mechanismen (z. B. QoS auf der WAN-Verbindung) sollen aber von der **be.IP** übernommen werden. Dabei werden bei Verbindungen aus dem WAN folgende Systeme durchlaufen und müssen dementsprechend darauf vorbereitet sein:
 - Network Address Translation (NAT/PAT)
 - Stateful Inspection Firewall (SIF).
- Ebenso muss für Dienste, die ggf. einen gleichbleibenden Quellport benötigen, dieses durch eine ausgehende NAT-Regel konfiguriert werden. Es wird eine „normale“ WAN-Konfiguration ohne Lastverteilung-Szenario und ohne erweitertes Routing mit der aktuellen Firmwareversion vorausgesetzt.

6.2 Konfiguration

6.2.1 Network Address Translation (NAT) / Port Address Translation (PAT)

Das erste durchlaufene Subsystem beim IPv4-Zugriff aus dem WAN ist die Network Address Translation (NAT).

Hier wird die Anfrage an die offizielle IPv4-Adresse der **be.IP** (die der WAN-Verbindung) umgesetzt und an die gewünschte IPv4-Adresse im LAN (Exposed Host) oder an einen Server in einer speziellen DMZ (De-Militarized Zone, abgetrennte und mittels zusätzlicher

Firewallregeln überwachte Schnittstelle) weitergeleitet. In unserem Beispiel ist das Ziel der Umsetzung in dem LAN, das an br0 (IPv4-Adresse 192.168.2.254) angeschlossen ist. Deswegen wird die Bezeichnung „Exposed Host“ verwendet.

Gehen Sie in das Menü **Netzwerk->NAT->NAT-Konfiguration ->Neu**.

The screenshot shows a web-based configuration interface for NAT. It is divided into three main sections:

- Basisparameter:**
 - Beschreibung:
 - Schnittstelle:
 - Art des Datenverkehrs:
- Ursprünglichen Datenverkehr angeben:**
 - Dienst:
 - Protokoll:
 - Quell-IP-Adresse/Netzmaske:
 - Original Ziel-IP-Adresse/Netzmaske:
- Substitutionswerte:**
 - Neue Ziel-IP-Adresse/Netzmaske:

Abb. 39: **Netzwerk->NAT->NAT-Konfiguration ->Neu**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine **Beschreibung** ein, z. B. *All_to_Firewall*.
- (2) Wählen Sie eine **Schnittstelle** aus, z. B. *WAN_GERMANY - TELEKOM BUSINESS*.
- (3) Belassen Sie die Einstellung **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*.
- (4) Belassen Sie den **Dienst** als *Benutzerdefiniert*.
- (5) Belassen Sie das **Protokoll** als *Beliebig*.
- (6) Geben Sie bei der Option **Neue Ziel-IP-Adresse/Netzmaske** = *Host* und die IPv4-Adresse *192.168.2.254* ein.
Durch diese Regel wird jeglicher auf der PPPoE-WAN-Schnittstelle ankommender IPv4-Verkehr auf die IP-Adresse 192.168.2.254 weitergeleitet.
- (7) Bestätigen Sie Ihre Einstellungen mit **OK**.

Nun müssen noch für den ausgehenden Verkehr bei sensiblen Diensten die ausgehenden Quellports eingestellt werden. Dies ist z. B. bei einigen Herstellern (LANCOM, Sophos UTM, ...) für den Aufbau der Phase 1 (IKE) einer IPSec-Verbindung notwendig. Bei einer **be.IP** oder einem Gerät der bintec elmeg GmbH ist dieser Schritt für IPSec nicht nötig.

Gehen Sie in das Menü **Netzwerk->NAT->NAT-Konfiguration ->Neu**.

Basisparameter		Ursprünglichen Datenverkehr angeben	
Beschreibung	<input type="text" value="IKE_Sourceport"/>	Dienst	<input type="text" value="Benutzerdefiniert"/>
Schnittstelle	<input type="text" value="WAN_GERMANY - TELEKOM ENTERTAIN"/>	Protokoll	<input type="text" value="UDP"/>
Art des Datenverkehrs	<input type="text" value="ausgehend (Quell-NAT)"/>	Originale Quell-IP-Adresse/Netzmaske	<input type="text" value="Beliebig"/>
NAT-Methode	<input type="text" value="symmetrisch"/>	Original Quell-Port/Bereich	<input type="text" value="Port angeben"/> 500 bis <input type="text" value=""/>
		Ziel-IP-Adresse/Netzmaske	<input type="text" value="Beliebig"/>
		Ziel-Port/Bereich	<input type="text" value="Port angeben"/> 500 bis <input type="text" value=""/>
Substitutionswerte			
Neue Quell-IP-Adresse/Netzmaske	<input type="text" value="Host"/> <input type="text" value="0.0.0.0"/>		
Neuer Quell-Port	<input checked="" type="radio" value="Original"/>		

Abb. 40: Netzwerk->NAT->NAT-Konfiguration ->Neu

Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine **Beschreibung** ein, z. B. *IKE_Sourceport*.
- (2) Wählen Sie eine **Schnittstelle** aus, z. B. *WAN_GERMANY - TELEKOM BUSINESS*.
- (3) Wählen Sie die Einstellung **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* aus.
- (4) Für die **NAT-Methode** wählen Sie *symmetrisch* aus.
- (5) Belassen Sie den **Dienst** als *Benutzerdefiniert*.
- (6) Wählen Sie unter **Protokoll** *UDP*.
- (7) Wählen Sie **Original Quell-Port/Bereich** = *Port angeben* und geben Sie *500* ein.
- (8) Wählen Sie **Ziel-Port/Bereich** = *Port angeben* und geben Sie *500* ein.
- (9) Die als **Neue Quell-IP-Adresse/Netzmaske** angegebene IP-Adresse *0.0.0.0* dient als Platzhalter für die dynamisch zugewiesene IP-Adresse der WAN-Schnittstelle. Sollte eine „feste“ offizielle IP-Adresse vorhanden sein, kann diese hier eingetragen werden.
- (10) Unter **Neuer Quell-Port** aktivieren Sie *Original*.
- (11) Bestätigen Sie Ihre Einstellungen mit **OK**.

Für weitere Dienste, die eine Beibehaltung des **Quell-Port** benötigen, verfahren Sie bitte analog zum obigen Beispiel. Wählen Sie das entsprechende **Protokoll** aus, und geben Sie den **Port** ein.

6.2.2 Stateful Inspection Firewall (SIF)

Das nächste Subsystem, das die jetzt von der NAT „durchgelassenen“ Pakete passieren, ist die Stateful Inspection Firewall. Durch den Status der WAN-Schnittstelle als „nicht vertrauenswürdig“ dürfen in der Standardeinstellung von dieser Schnittstelle keine initialen Anfragen gestellt werden, sondern nur entsprechende Anfragen von „vertrauenswürdig“ Schnittstellen (initial alle LAN-Schnittstellen) beantwortet werden. Die Anfragen werden also zunächst weiterhin blockiert, diesmal von der SIF.

Eine Regel, die diesen Zugriff als Ausnahme vom Ausgangsverhalten erlaubt, muss erst erstellt werden.

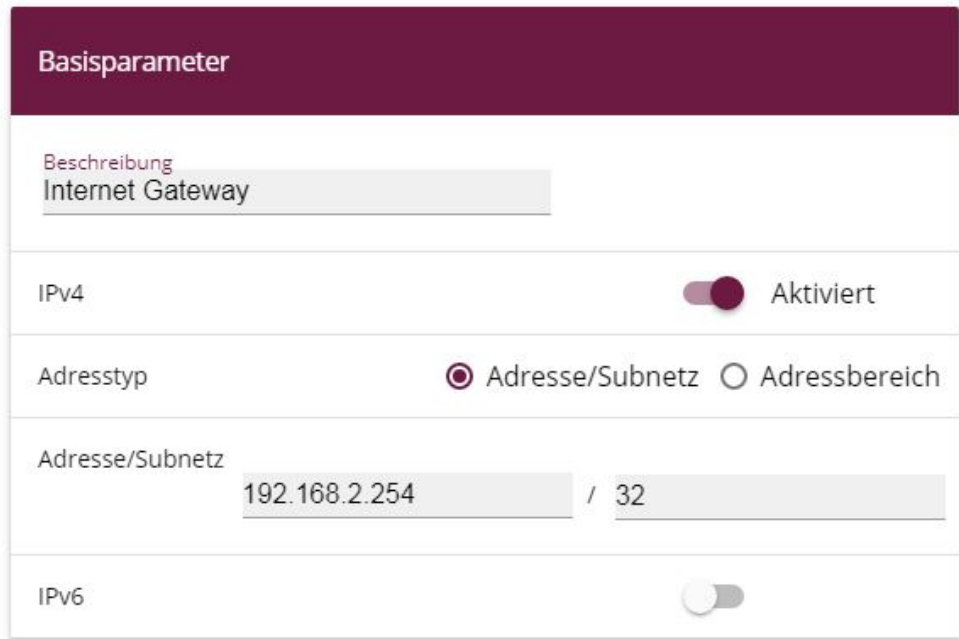


Hinweis

In der Stateful Inspection Firewall gilt die Regel, dass Pakete, die durch eine Regel erlaubt werden, später nicht mehr verboten werden können und umgekehrt. Ggf. ist also auch die Reihenfolge der durchlaufenen Regeln zu beachten!

In unserem Beispiel müssen alle Protokolle und alle Ports zum Zugriff aus dem WAN auf die IP-Adresse des Internet Gateways (192.168.2.254) freigegeben werden. Die benötigten Schnittstellen und die Diensteszusammenfassung „any“ sind bereits vordefiniert, es muss nur noch die IP-Adresse des Internet Gateways definiert werden.

Gehen Sie in das Menü **Firewall->Adressen->Adressliste->Neu**.



Basisparameter

Beschreibung
Internet Gateway

IPv4 Aktiviert

Adresstyp Adresse/Subnetz Adressbereich

Adresse/Subnetz
192.168.2.254 / 32

IPv6

Abb. 41: Firewall->Adressen->Adressliste->Neu

Gehen Sie folgendermaßen vor:

- Geben Sie eine **Beschreibung** ein, z. B. *Internet Gateway*.
- Geben Sie bei **Adresse/Subnetz** die IP-Adresse des Internet Gateways *192.168.2.254* und das Subnetz *32* ein.
- Bestätigen Sie Ihre Einstellungen mit **OK**.

Als neue Regel wird der Zugriff von der WAN-Schnittstelle auf die IPv4-Adresse des Internet Gateways für jeden Dienst und alle Protokolle definiert.

Gehen Sie in das Menü **Firewall->Richtlinien->IPv4-Filterregeln->Neu**.

Basisparameter

Quelle	WAN_GERMANY - TELEKOM ENTERTAIN ▼
Ziel	Internet Gateway ▼
Dienst	any ▼
Aktion	Zugriff ▼

Abb. 42: Firewall->Richtlinien->IPv4-Filterregeln->Neu

Gehen Sie folgendermaßen vor:

- (a) Wählen Sie eine **Quelle** z. B. *WAN_GERMANY - TELEKOM BUSINESS* aus.
- (b) Wählen Sie das **Ziel** = *Intern Gateway*.
- (c) Wählen Sie den **Dienst** *any* aus.
- (d) Belassen Sie **Aktion** *Zugriff*.
- (e) Bestätigen Sie Ihre Einstellungen mit **OK**.

Im Menü **Firewall->Richtlinien->IPv4-Filterregeln** wird eine Liste aller konfigurierten IPv4-Filterregeln angezeigt.

Filterregeln

Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv				
1	WAN_GERMANY - TELEKOM ENTERTAIN	Internet Gateway	any	Zugriff	● Aktiviert	↑↓	≡	🗑️	✎

Abb. 43: Firewall->Richtlinien->IPv4-Filterregeln

6.2.3 Änderungen am Internet Gateway

Am Internet Gateway müssen jetzt die Standardroute und ggf. der DNS-Server auf die IP-Adresse der **be.IP** umgestellt werden. Auch die Rolle des Zeitservers kann von der **be.IP** übernommen werden.

6.2.4 Schlussbemerkung

Das Szenario ist auch bedingt durch die Tatsache, dass eine Einwahl mehrerer PPPoE-Verbindungen an einem xDSL-Anschluss der DTAG seit Januar 2015 unterbunden wird. Auch könnte eine Routingverbindung der **be.IP** über die bisherige PPPoE-Einwahl des Internet Gateways konfiguriert werden, dann müssen aber Mechanismen, die die **be.IP** automatisch für VoIP vornimmt, vom Internet Gateway übernommen werden. Beispielhaft seien hier genannt:

- Quality of Service (Priorisierung) für die Telefoniepakete
- Freigaben in der Firewall für Telefonie
- NAT-Mechanismen für die nicht zusammenhängenden Ports von RTP Daten
- SRV-Abfragen via DNS (für tel.t-online.de) müssen adäquat aufgelöst werden.

Die sehr umfassenden Einstellungen in NAT und SIF zur Weiterleitung des gesamten Verkehrs aus dem Internet können natürlich bei Bedarf feiner angepasst und weiter eingeschränkt werden.

Diese Beschreibung basiert auf einem durchlaufenen Schnellstartassistenten, sollten schon vorhandene Portforwardings in der NAT existieren, ist ggf. die Reihenfolge zu beachten!

6.3 Konfigurationsschritte im Überblick

NAT-Konfiguration (Ziel-NAT)

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>All_to_Firewall</i>
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>WAN_GERMAN - TELEKOM BUSINESS</i>
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>eingehend (Ziel-NAT)</i>
Dienst	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Benutzerdefiniert</i>
Protokoll	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Beliebig</i>
Quell-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Beliebig</i>
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Beliebig</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Host: 192.168.2.254</i>

NAT-Konfiguration (Quell-NAT)

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>IKE_Sourceport</i>
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration-> Neu	z. B. <i>WAN_GERMAN - TELEKOM BUSINESS</i>
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>ausgehend (Quell-NAT)</i>
NAT-Methode	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>symmetrisch</i>
Protokoll	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>UDP</i>
Original Quell-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Port angeben: 500</i>
Ziel-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Port angeben: 500</i>

Feld	Menü	Wert
Neue Quell-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Host: 0.0.0.0</i>
Neuer Quell-Port	Netzwerk->NAT->NAT-Konfiguration-> Neu	<i>Original</i>

Stateful Inspection Firewall (SIF)

Feld	Menü	Wert
Beschreibung	Firewall->Adressen->Adressliste-> Neu	<i>z. B. Internet Gateway</i>
IPv4	Firewall->Adressen->Adressliste-> Neu	<i>Aktiviert</i>
Adresstyp	Firewall->Adressen->Adressliste-> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall->Adressen->Adressliste-> Neu	<i>z. B. 192.168.2.254 / 32</i>

IPv4-Filterregeln

Feld	Menü	Wert
Quelle	Firewall->Richtlinien-> IPv4-Filterregeln-> Neu	<i>WAN_GERMAN - TELEKOM BUSINESS</i>
Ziel	Firewall->Richtlinien-> IPv4-Filterregeln-> Neu	<i>Internet Gateway</i>
Dienst	Firewall->Richtlinien-> IPv4-Filterregeln-> Neu	<i>any</i>
Aktion	Firewall->Richtlinien-> IPv4-Filterregeln-> Neu	<i>Zugriff</i>

Kapitel 7 be.IP Secure Client: Konfiguration eines VPN Remote Zugriffs

7.1 Einleitung

Im Folgende konfigurieren Sie einen IPSec-Tunnel zwischen einem bintec be.IP Media- und VPN-Gateway (ab Software 10.1.5 Patch 3) und einem be.IP Secure Client (ab Version 3.0.4 Build 26471).

Zur Konfiguration wird das Graphical User Interface (**GUI**) verwendet. Hilfe zu den verfügbaren Konfigurationsoptionen erhalten Sie über das Online-Hilfe-System.

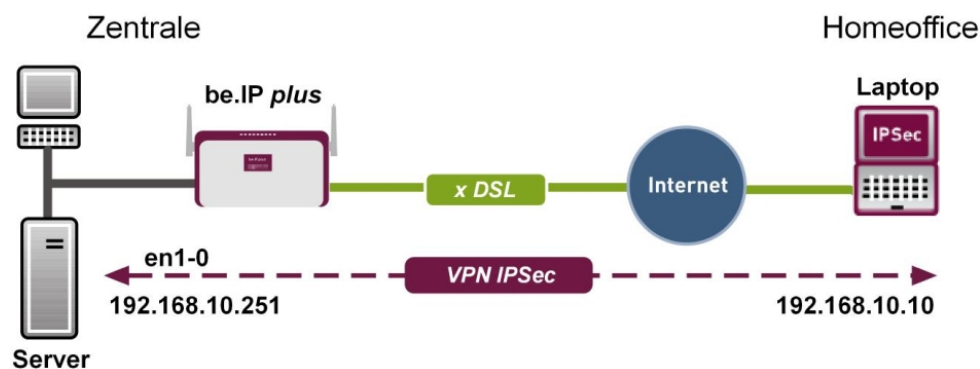


Abb. 44: Beispielszenario

Voraussetzungen

- Eine **be.IP** oder eine **be.IP plus**, erreichbar über eine offizielle IP-Adresse oder über DynDNS sowie mit aktiver Internetverbindung
- Ein PC oder ein Laptop mit aktiver Internetverbindung, auf dem der be.IP Secure Client installiert wird
- Lizenzschlüssel und Seriennummer für die Aktivierung des be.IP Secure Client

7.2 Konfiguration

7.2.1 Gateway starten

- (1) Öffnen Sie einen Web-Browser, geben Sie die IP-Adresse Ihres Geräts in das Adressfeld Ihres Web-Browsers ein und bestätigen Sie mit der Eingabetaste.
Das Fenster **Welcome** öffnet sich.
- (2) Geben Sie in die Felder **User** und **Password** Ihre Anmeldedaten ein und klicken Sie auf **Login**.
Die Statusseite der Benutzeroberfläche öffnet sich in der **Ansicht Benutzer**.

7.2.2 Tunnel mit dem Assistenten VPN konfigurieren

Verwenden Sie zur Konfiguration des Tunnels den **Assistenten VPN**.

- (1) Gehen Sie zu **Assistenten->VPN->VPN-Verbindungen->Neu**.
- (2) Wählen Sie **VPN-Szenario** *IPSec - Einwahl eines einzelnen Clients*.



The screenshot shows a web interface for selecting a VPN scenario. At the top, a dark purple header contains the text "Wählen Sie das VPN-Szenario aus:" and a question mark icon. Below the header, there is a white area with the label "VPN-Szenario" on the left and a dropdown menu on the right. The dropdown menu is currently open, showing the selected option "IPSec - Einwahl eines einzelnen Clients" with a downward-pointing arrow.

Abb. 45: **Assistenten->VPN->VPN-Verbindungen->Neu**

- (3) Klicken Sie auf **Weiter**, um Ihre Auswahl zu bestätigen.

Im nächsten Schritt geben Sie die erforderlichen Daten für das IPSec-Szenario ein.

The screenshot shows a configuration window with three main sections:

- Verbindungsdetails:** Fields for 'Beschreibung' (IPSec_Connection_1), 'Lokale IPsec ID' (be_ip_plus), 'Entfernte IPsec ID' (IPSec_Connection_1), and 'Preshared Key' (masked with dots).
- Entferntes Netzwerk:** A table of local networks and a dropdown for 'IP-Adresspool auswählen' (DHCP Adressbereich). Below, it shows 'IP-Adresspool für Einwahl-Clients' set to 192.168.0.10-192.168.0.30.
- Weitere Konfigurationsschritte auswählen:** A toggle switch for 'Konfigurationsdatei für bintec Secure IPSec Client exportieren' which is currently 'Aktiviert'.

Abb. 46: Assistenten->VPN->VPN-Verbindungen->Neu->Weiter

Gehen Sie folgendermaßen vor:

- (1) Bei **Beschreibung** geben Sie einen Namen für die Verbindung ein, z. B. *IP-Sec_Connection_1*.
- (2) Die **Lokale IPsec ID** lassen Sie unverändert.
- (3) Bei **Entfernte IPsec ID** geben Sie die ID des entfernten IPsec-Peers ein, z. B. *IP-Sec_Connection_1*.
- (4) Für die Authentifizierung wird ein **Preshared Key** verwendet.



Hinweis

Wir empfehlen, als **Preshared Key** eine Kombination aus Buchstaben, Zahlen und Sonderzeichen zu verwenden.

- (5) Unter **IP-Adresspool auswählen** wählen Sie einen geeigneten IP-Adressbereich aus, zum Beispiel *DHCP Adressbereich* oder konfigurieren Sie unter **WAN->Internet + Einwählen->IP Pools->Neu** einen neuen Adressbereich. Um einen neuen Adressbereich zu konfigurieren, müssen Sie die **Ansicht Vollzugriff** verwenden.



Hinweis

Wir empfehlen, einen IP-Pool mit Adressen aus dem internen Netz des Gateways zu verwenden.

- (6) Aktivieren Sie **Konfigurationsdatei für bintec Secure IPSec Client exportieren**.



Hinweis

Die exportierte Datei *.ini kann sowohl in einen be.IP Secure Client als auch in einen bintec elmeg IPsec Secure Client importiert werden.

- (7) Bestätigen Sie Ihre Angaben mit **OK**.
Folgendes Fenster öffnet sich:

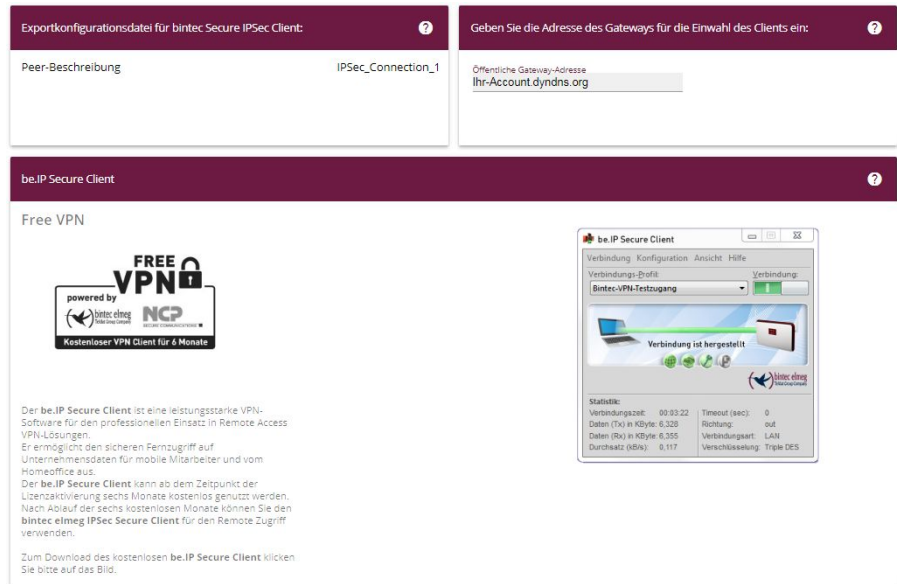


Abb. 47: Assistenten->VPN->VPN-Verbindungen->Neu->Weiter->OK

- (8) Klicken Sie auf **Exportieren**.
Ein zusätzliches Fenster öffnet sich.
- (9) Wählen Sie **Datei speichern** und klicken Sie auf **OK**.
Die ini-Datei wird gespeichert.

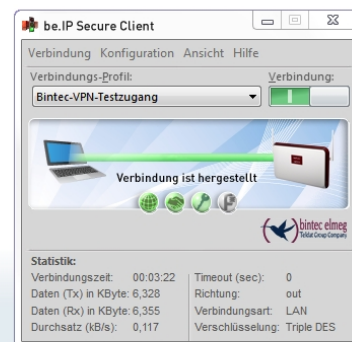
7.2.3 be.IP Secure Client herunterladen

- (1) Klicken Sie auf den Link **be.IP Secure Client** oder auf die Grafik.
Die bintec elmeg Homepage öffnet sich an der entsprechenden Stelle.

be.IP Secure Client

Der **be.IP Secure Client** ist eine leistungsstarke VPN-Software für den professionellen Einsatz in Remote Access VPN-Lösungen.

Er ermöglicht den sicheren Fernzugriff auf Unternehmensdaten für mobile Mitarbeiter und vom Homeoffice aus.



be.IP Secure Client

2 Download(s) verfügbar:

-  [beIP-Secure-Client-Win-x86-64-304-26471.exe](#) be.IP Secure Client 64bit
27,61 MB, 19.11.2015
-  [beIP-Secure-Client-Win-x86-304-26471.exe](#) be.IP Secure Client 32bit
23,80 MB, 19.11.2015

Abb. 48: Download-Seite für den be.IP Secure Client

- (2) Laden Sie die Installationsdatei für den be.IP Secure Client von dieser Homepage und speichern Sie die exe-Datei in der gewünschten Version (32-Bit-Version oder 64-Bit-Version, passend zu Ihrem Betriebssystem) auf Ihrem PC.
- (3) Sichern Sie die Konfiguration Ihres Gateways mit **Konfiguration speichern**.

7.2.4 be.IP Secure Client installieren und konfigurieren

Für die Installation des be.IP Secure Clients steht ein Assistent zur Verfügung.

- (1) Klicken Sie auf die exe-Datei, die Sie von der bintec-elmeg-Homepage heruntergeladen haben.
Das Fenster **be.IP Secure Client - InstallShield Wizard** öffnet sich.

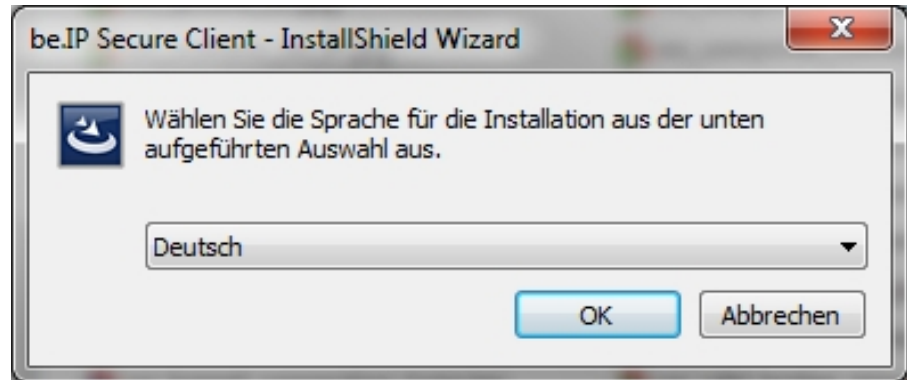


Abb. 49: Sprachauswahl im **InstallShield Wizard**

- (2) Wählen Sie die Sprache für die Installation, z. B. *Deutsch* und klicken Sie auf **OK**. Die Datei wird entpackt, Sie werden begrüßt.

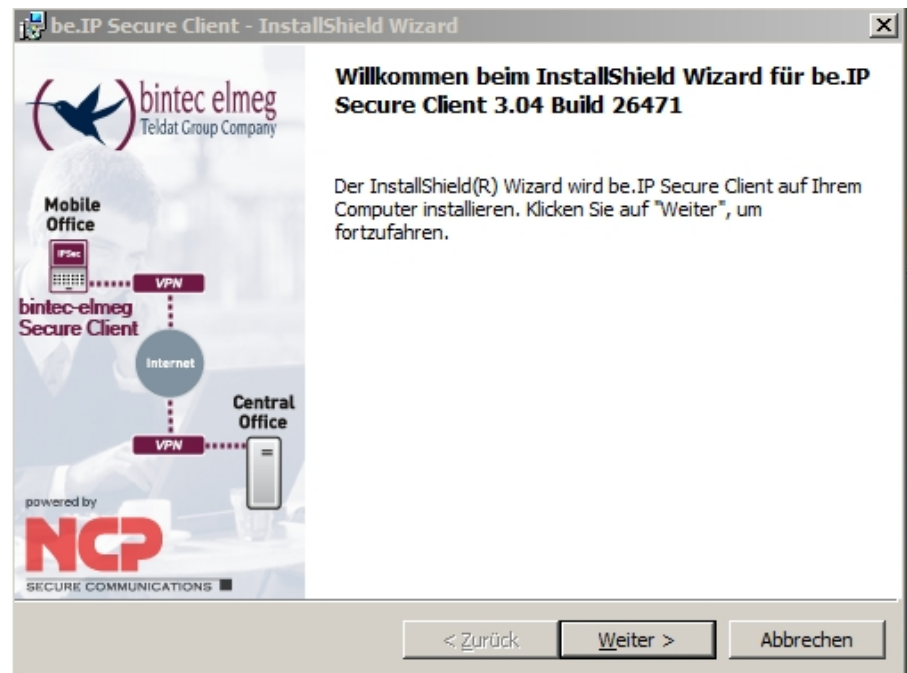


Abb. 50: Willkommen-Seite im **InstallShield Wizard**

- (3) Klicken Sie auf **Weiter**.

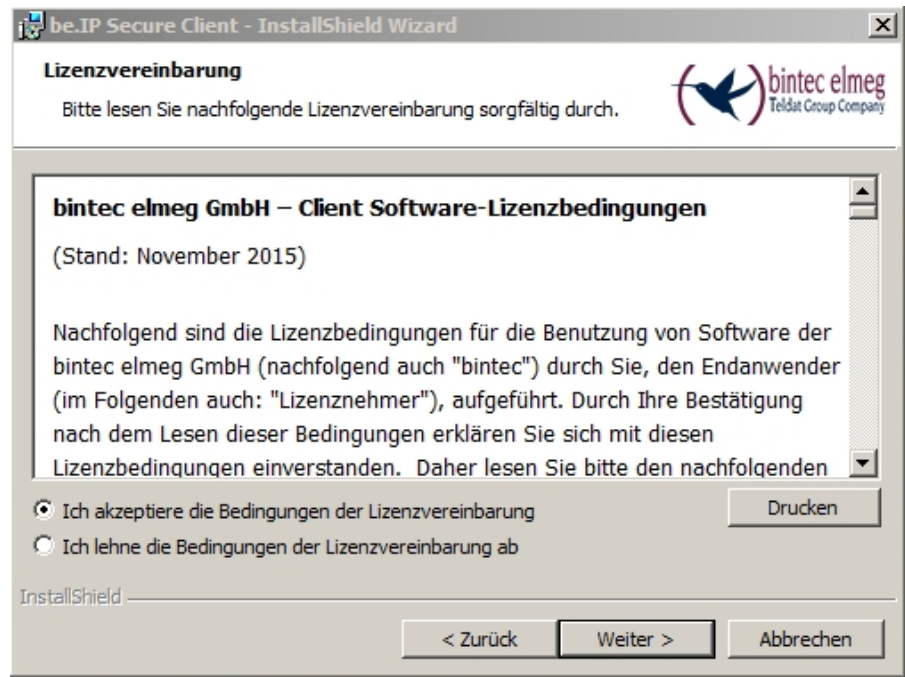


Abb. 51: Lizenzvereinbarung im **InstallShield Wizard**

- (4) Lesen Sie die Lizenzbedingungen. Aktivieren Sie *Ich akzeptiere die Bedingungen der Lizenzvereinbarung* und klicken Sie auf **Weiter**.

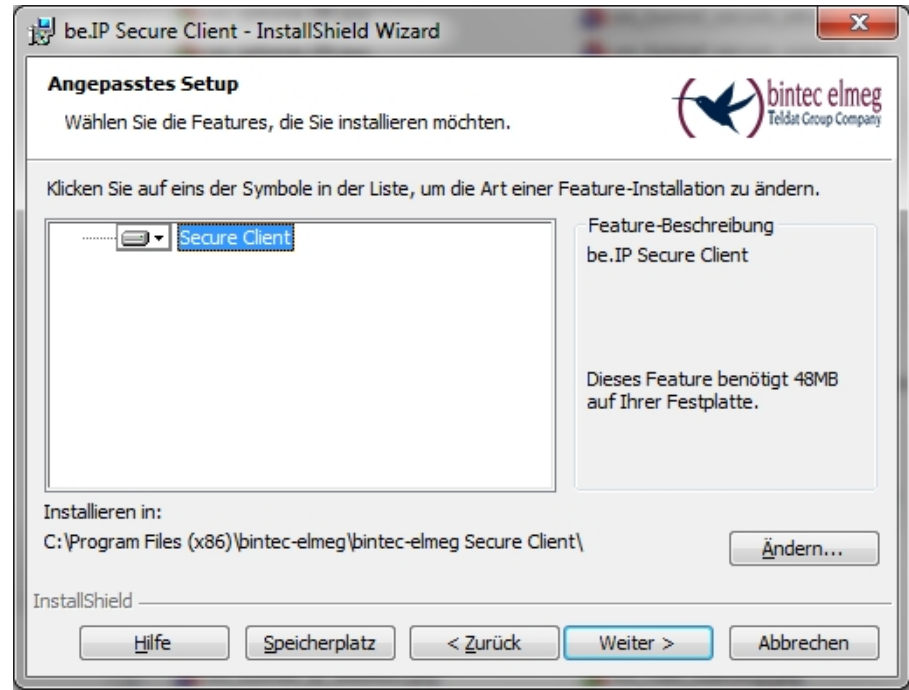


Abb. 52: Setup im **InstallShield Wizard**

- (5) Belassen Sie die Einstellung **Secure Client** und klicken Sie auf **Weiter**.

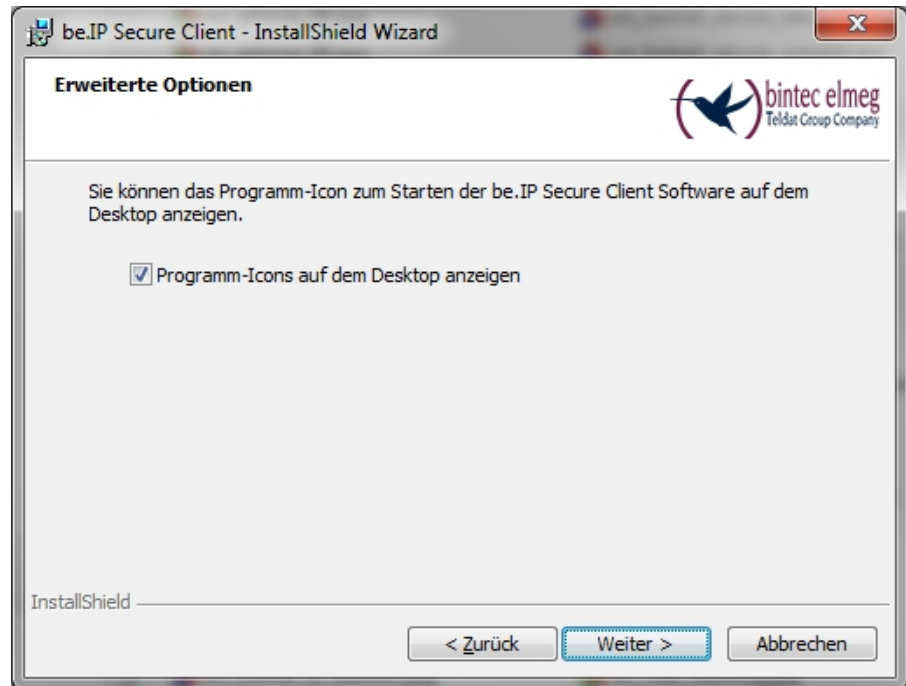


Abb. 53: Icon anzeigen lassen im **InstallShield Wizard**

- (6) Wenn Sie für den be.IP Secure Client ein Icon auf dem Desktop Ihres PC anzeigen lassen wollen, aktivieren Sie *Programm-Icons auf dem Desktop anzeigen* und klicken Sie auf **Weiter**.
Die Vorbereitungen für die Installation sind abgeschlossen.
- (7) Klicken Sie auf **Installieren**.

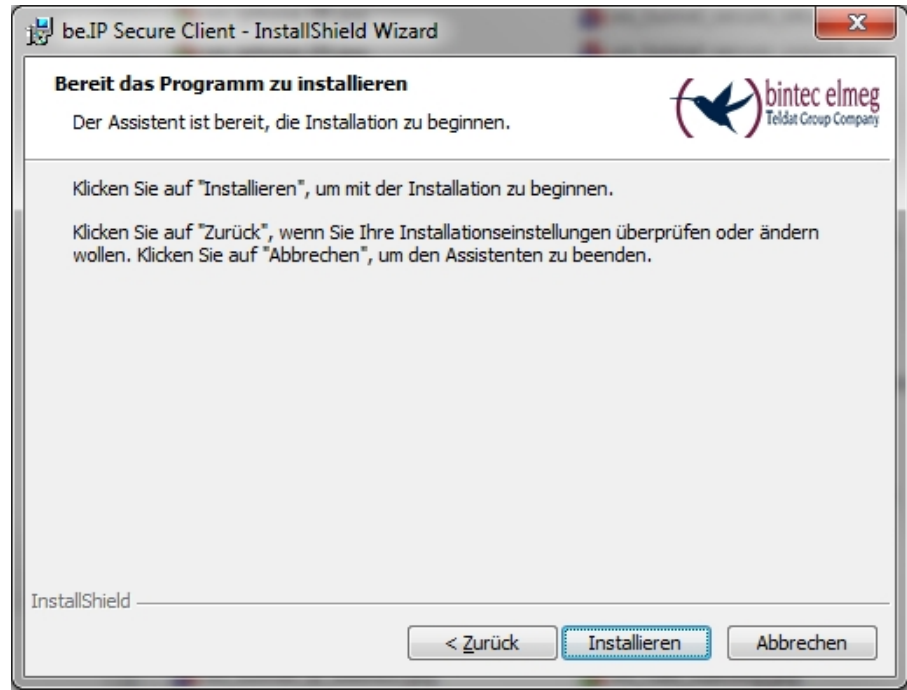


Abb. 54: Ende der Vorbereitungen im **InstallShield Wizards**
Der be.IP Secure Client wird installiert.

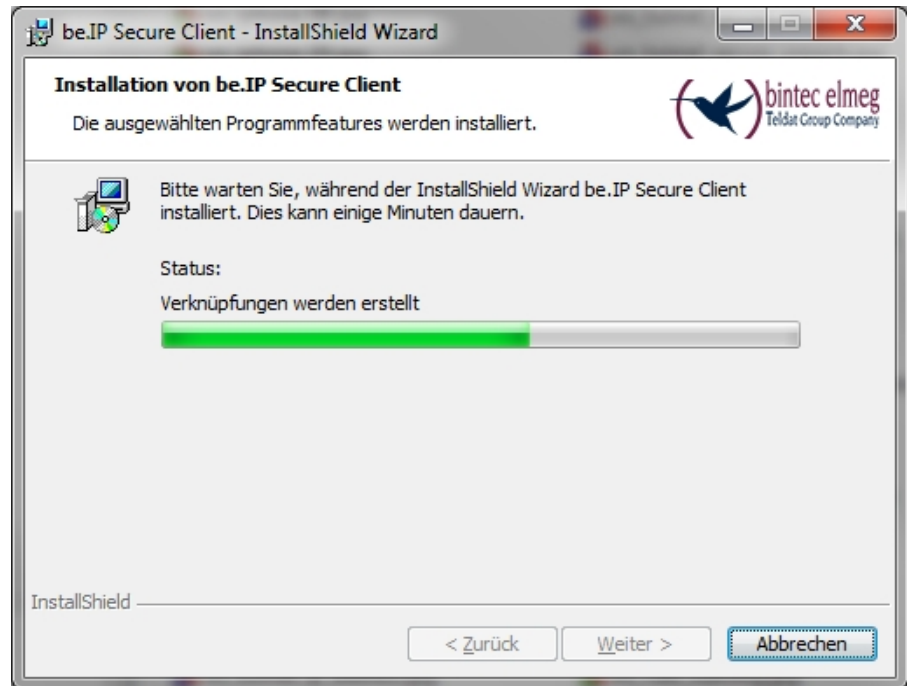


Abb. 55: be.IP Secure Client installieren im **InstallShield Wizard**



Abb. 56: be.IP Secure Client ist installiert
Die Installation ist abgeschlossen.

- (8) Klicken Sie auf **Fertig stellen**.

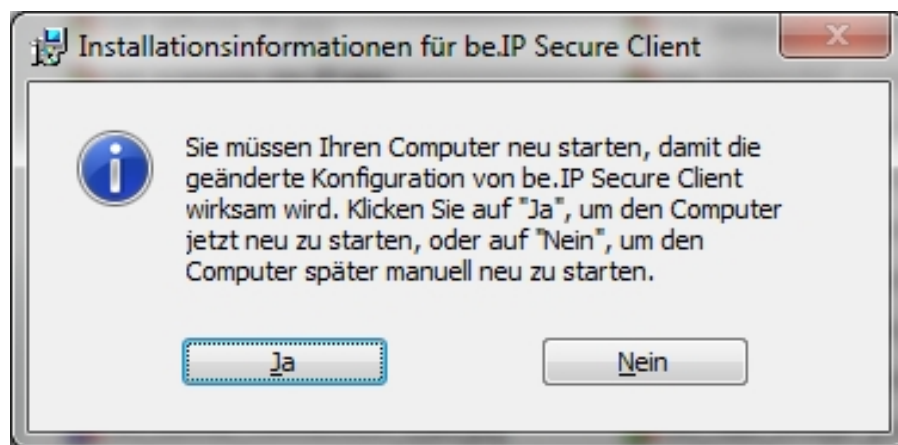


Abb. 57: Installationsinformationen für den **be.IP Secure Client**

- (9) Klicken Sie auf **Ja**, um Ihren PC neu zu starten.

7.2.5 Software aktivieren und Datei einlesen

Der be.IP.IPSecure Client und der Assistent für die Software-Aktivierung starten nach dem PC Neustart automatisch. Für die Software-Aktivierung benötigen Sie eine aktive Internet-Verbindung.

- (1) Geben Sie die Lizenzdaten ein.



Hinweis

Die Seriennummer einer be.IP Client Lizenz besteht aus acht Ziffern und beginnt mit der Zeichenfolge 300.

Assistent für Software-Aktivierung

Lizenzdaten
Wie lauten die Lizenzdaten?

Bitte geben Sie die Lizenzdaten der be.IP Secure Client Software ein.

Lizenzschlüssel:
3088 - 2210 - 5764 - xxxx - xxxx

Seriennummer:
[Redacted]

< Zurück Weiter > Abbrechen

Abb. 58: Assistent für Software-Aktivierung: Lizenzdaten eingeben

- (2) Klicken Sie auf **Weiter**.
Die Online-Aktivierung der Software wird durchgeführt.
- (3)

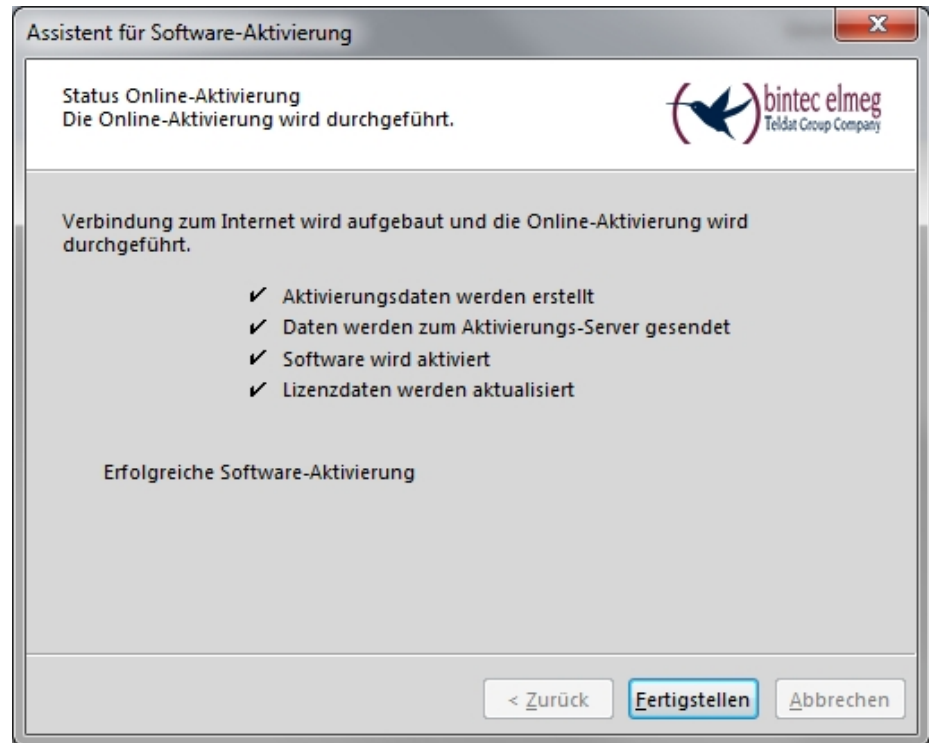


Abb. 59: Erfolgreiche Software-Aktivierung

Wenn die Software erfolgreich aktiviert ist, klicken Sie auf **Fertigstellen**.

- (4) Wenn Sie die Software aktiviert haben, können Sie die ini-Datei einlesen, die Sie mit Ihrem Gateway erzeugt haben.

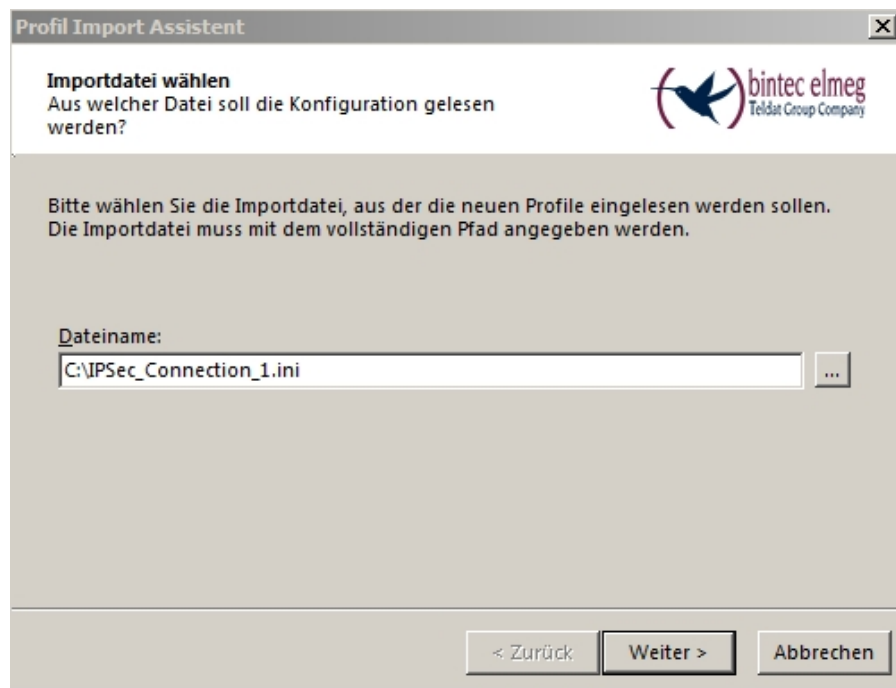


Abb. 60: ini-Datei einlesen

- (5) Wählen Sie die gewünschte Datei, z. B. *IPSec_Connection_1.ini* und klicken Sie auf **Weiter**.
- (6) Klicken Sie auf **Fertigstellen**.

7.2.6 IPSec-Verbindung aufbauen

Wenn die Aktivierung abgeschlossen und eine ini-Datei eingelesen ist, kann eine IPSec-Verbindung aufgebaut werden.

- (1) Wählen Sie dazu im **be.IP Secure Client** in der Liste **Verbindungs-Profil** das Profil, das Sie eingelesen haben, z. B. *IPSec_Connection_1*.
- (2) Klicken Sie in das Feld **Verbindung**.
Die Verbindung wird aufgebaut. Die Farbe des Feldes wechselt von rot zu grün.

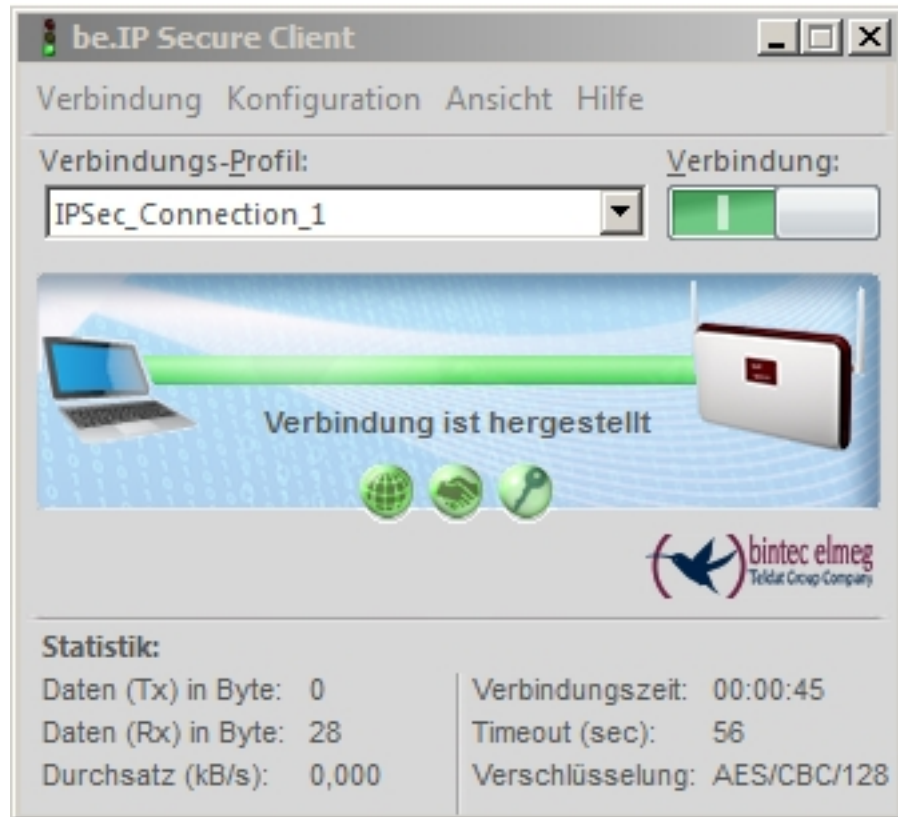


Abb. 61: IPsec-Verbindung ist hergestellt

7.2.7 Tunnel splitten

Standardmäßig sendet der Client alle Datenpakete in den aktiven Tunnel. Wenn Sie Zugriff auf ein bestimmtes Zielnetz haben wollen, müssen Sie die IP-Adresse dieses privaten Zielnetzes eintragen.

- (1) Gehen Sie dazu im **be.IP Secure Client** in das Menü **Konfiguration->Profile**. Das Fenster **Profile** öffnet sich.
- (2) Doppelklicken Sie auf das Profil, das Sie angelegt haben, z. B. *IP-Sec_Connection_1*. Das Fenster **Profil-Einstellungen IPSec_Connection_1** öffnet sich.
- (3) Klicken Sie auf **Split Tunneling** links in der Liste.

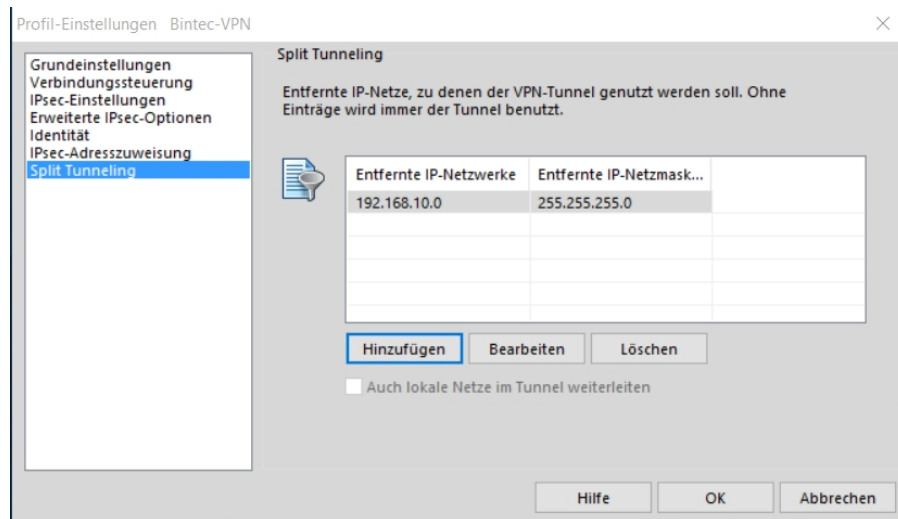


Abb. 62: Split Tunneling

- (4) Klicken Sie auf **Hinzufügen**.
Das Fenster **IP-Netze** öffnet sich.
- (5) Geben Sie die IP-Adresse sowie die Netzmaske Ihres privaten Netzes ein, z. B. *192.168.10.0* und *255.255.255.0* und klicken Sie auf **OK**.
Ihr Netzwerk wird in der Liste angezeigt.
- (6) Klicken Sie auf **OK**.
Das Fenster **IP-Netze** schließt sich.
- (7) Klicken Sie auf **OK**.
Das Fenster **Profile** schließt sich.

7.3 Konfigurationsschritte im Überblick

Gateway starten

Feld	Fenster	Wert
User	Welcome	z. B. <i>admin</i>
Password	Welcome	z. B. <i>User</i>

Tunnel mit dem Assistenten VPN konfigurieren

Feld	Menü	Wert
VPN-Szenario	Assistenten->VPN->VPN-Verbindungen->Neu	z. B. <i>IPSec - Einwahl eines einzelnen Clients</i>

Feld	Menü	Wert
Beschreibung	Assistenten->VPN->VPN-Verbindungen->Neu->>Weiter	z. B. <i>IP-Sec_Connection_1</i>
Lokale IPsec ID	Assistenten->VPN->VPN-Verbindungen->Neu->>Weiter	Angezeigten Wert unverändert belassen, z. B. <i>be.IP+</i>
Entfernte IPsec ID	Assistenten->VPN->VPN-Verbindungen->Neu->>Weiter	z. B. <i>IP-Sec_Connection_1</i>
Preshared Key	Assistenten->VPN->VPN-Verbindungen->Neu->>Weiter	z. B. <i>Secret_1</i>
IP-Adresspool auswählen	Assistenten->VPN->VPN-Verbindungen->Neu->>Weiter	z. B. <i>DHCP Adressbereich</i>
Konfigurationsdatei für bintec Secure IPsec Client exportieren	Assistenten->VPN->VPN-Verbindungen->Neu->>Weiter->OK	<i>Aktiviert</i>

bintec-elmeg Secure Client - InstallShield Wizard

Feld	Menü	Wert
Sprache	OK	z. B. <i>Deutsch</i>
Ich akzeptiere die Bedingungen der Lizenzvereinbarung	OK->Weiter	<i>Aktiviert</i>
Secure Client	OK->Weiter->Weiter	<i>Aktiviert</i>
Programm-Icons auf dem Desktop anzeigen	OK ->Weiter ->Weiter ->Weiter ->Installieren ->Fertig stellen->Ja	z. B. <i>Aktiviert</i>

Assistent für die Software-Aktivierung

Feld	Menü	Wert
Online-Aktivierung	Aktivierung	Aktiviert
Lizenzschlüssel	Aktivierung ->Aktivierung ->Weiter	z. B. <i>3088 - 2210 - 5764 - 6789 - 1234</i>
Seriennummer	Aktivierung ->Aktivierung ->Weiter	z. B. <i>30001234</i>
Importdatei wählen	Aktivierung ->Aktivierung -	z. B.

Feld	Menü	Wert
	>Weiter ->Weiter	C:\IPSec_Connection_1.ini

be.IP Secure Client: IPSec-Verbindung aufbauen

Feld	Menü	Wert
Verbindungs-Profil	Fenster be.IP Secure Client	z. B. IP-Sec_Connection_1

be.IP Secure Client: Tunnel teilen

Feld	Menü	Wert
Verfügbare Profile	Konfiguration ->Profile	z. B. auf IP-Sec_Connection_1 doppelklicken
Liste links	Konfiguration ->Profile ->Hinzufügen	Split Tunneling
IP-Netz	Konfiguration ->Profile ->Hinzufügen	z. B. 192.168.10.0
Netz-Maske	Konfiguration ->Profile ->Hinzufügen ->OK->OK->OK	z. B. 255.255.255.0

Kapitel 8 be.IP plus als PBX mit zwei xDSL-Anschlüssen

8.1 Vorbemerkung

Im folgenden Workshop wird die Konfiguration einer **be.IP plus** als Telefonanlage mit zwei xDSL-Anschlüssen mittels Lastverteilung und fest zugeteilten SIP-Leitungen (keine nomadische Nutzung) beschrieben.

Ab dem Firmwarestand 10.1.5 Patch 6 ist es möglich einzelne VoIP-Verbindungen fest auf eine bestimmte WAN-Verbindung zu binden. Ermöglicht wird dies über den bereits für Registrierungen eingesetzten Mechanismus der **Standorte**, der jetzt auch die ausgehende Schnittstelle für VoIP-Pakete einer SIP-Verbindung definiert.

Notwendig wird dieser Umstand durch das Fehlen von weiteren Unterscheidungskriterien, da die Registrar-IP-Adresse, Ports und DSCP-Werte identisch sind. Weiterhin ist darauf zu achten, dass nur bei einer der WAN-Verbindungen IPv6 aktiviert ist, da etliche Betriebssysteme und deren Applikation wie z. B. MS Windows nicht in der Lage sind, mehrere IPv6-Präfixe in Lastverteilungs-Szenarien zu verwenden und diese Aufgabe aufgrund des Fehlens einer NAT auch nicht von der **be.IP** übernommen werden kann.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

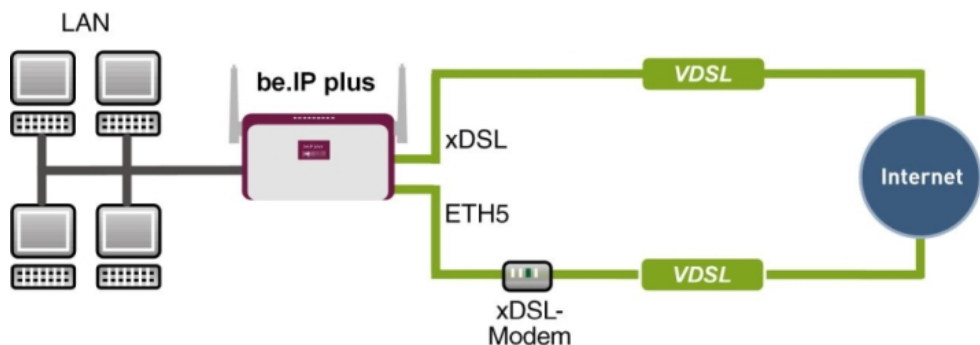


Abb. 63: Beispielszenario

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:


- Eine **be.IP plus** mit Systemsoftware 10.1.5 Patch 6
- Zwei unabhängige VDSL-Internetverbindungen
- Ein externes VDSL-Modem welches an eth1-4 (physischer Port LAN5) der **be.IP** angeschlossen ist

8.2 Konfiguration

8.2.1 Einrichtung der WAN-Verbindung

Zuerst müssen die beiden WAN-Verbindungen eingerichtet werden. Für die WAN-Verbindung über das interne VDSL-Modem (für ein Anschluss der Deutschen Telekom) folgen Sie den Schritten **Ersteinrichtung Telekom**. Mit der Schaltfläche **Weiter** können Sie die einzelnen Schritte durchlaufen.

WAN-Verbindung über das interne Modem der be.IP

Den über den Schnellstart-Assistenten konfigurierten Anschluss der Deutschen Telekom sehen Sie im Menü **WAN->Internet + Einwählen->PPPoE->Germany - Telekom Entertainment ->** . Die Option **IPv6** ist aktiviert.

Basisparameter

Beschreibung
Germany - Telekom Entertain

PPPoE-Modus Standard Mehrfachverbindung

PPPoE-Ethernet-Schnittstelle Automatisch

Benutzername
#0001@t-online.c

Passwort *****

Immer aktiv Aktiviert

IPv4-Einstellungen

Sicherheitsrichtlinie Nicht Vertrauenswürdig Vertrauenswürdig

IP-Adressmodus Statisch IP-Adresse abrufen

Standardroute Aktiviert

NAT-Eintrag erstellen Aktiviert

IPv6-Einstellungen

IPv6 Aktiviert

Sicherheitsrichtlinie Nicht Vertrauenswürdig Vertrauenswürdig

IPv6-Modus Host

Router Advertisement annehmen Aktiviert

DHCP-Client Aktiviert

IPv6-Adressen

Link-Präfix	Host-Adresse

HINZUFÜGEN

Abb. 64: WAN->Internet + Einwählen->PPPoE->Germany - Telekom Entertain ->

Um Störungen der bestehenden ersten VDSL-WAN-Strecke über das interne Modem zu vermeiden muss zuerst die **Metrik** der Standardroute über die entsprechende WAN-Schnittstelle auf *0* gesetzt werden. Da die **be.IP** über die zweite xDSL-Strecke zusammen mit der WAN-IP ebenfalls eine Standardroute erhält - allerdings mit Metrik *1* - ist dieser Schritt (insbesondere bei Fernkonfiguration) sinnvoll.

- (1) Gehen Sie in das Menü **Netzwerk->Routen->Konfiguration von IPv4-Routen** .

Routen						
Ziel-IP-Adresse	Netzmaske	Gateway	Schnittstelle	Metrik	Routentyp	Erweiterte Route
0.0.0.0	0.0.0.0	0.0.0.0	WAN_GERMANY - TELEKOM ENTERTAIN	1	Standardroute über Gateway	<input type="checkbox"/>

Abb. 65: Netzwerk->Routen->Konfiguration von IPv4-Routen

- (2) Wählen Sie das Symbol , um den Eintrag *WAN_GERMANY - TELEKOM ENTERTAIN* zu bearbeiten.

Basisparameter	Routenparameter
Routentyp: Standardroute über Gateway	Gateway-IP-Adresse: 0.0.0.0
Schnittstelle: WAN_GERMANY-TELEKOM-ENTERTAIN	Metrik: 0
Routenklasse: <input checked="" type="radio"/> Standard <input type="radio"/> Erweitert	

Abb. 66: Netzwerk->Routen->Konfiguration von IPv4-Routen 

- (3) Wählen Sie bei **Metrik** die Priorität der Route aus, in unserem Beispiel die 0.
- (4) Bestätigen Sie Ihre Angaben mit **OK**.

WAN-Verbindung über das externe Modem an en1-4 (physischer Port LAN5)

Der zweite Anschluss wird über das externe Modem an en1-4 mit Hilfe von **Assistenten** erstellt.

- (1) Gehen Sie dazu in das Menü **Assistenten->Internet->Internetverbindungen->Neu**.
- (2) Wählen Sie bei **Verbindungstyp** *Externes xDSL-Modem* aus.

Internetverbindungstyp auswählen: ?

Verbindungstyp Externes xDSL-Modem ▼

Abb. 67: **Assistenten->Internet->Internetverbindungen->Neu**

- (3) Klicken Sie **Weiter** um eine neue Internetverbindung zu konfigurieren.
- (4) Geben Sie die erforderlichen Daten für die Verbindung ein.

Beschreibung
Telekon_xDSL2

Wählen Sie den physischen Ethernet-Port aus, der mit dem externen xDSL-Modem verbunden ist:

Physischer Ethernet-Port ETH5

Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:

Typ Vordefiniert

Land Germany

Internet Service Provider Telekom

Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:

Anschlusskennung XXXXXXXXXX

Zugangsnummer
(vormals T-Online Nummer) XXXXXXXXXX

Mitbenutzernummer
0001 XXXXXXXXXX

Persönliches Kennwort
***** XXXXXXXXXX

Wählen Sie den Verbindungsmodus aus:

Immer aktiv Aktiviert

Die IPv6-Konfiguration auswählen

IPv6

Abb. 68: Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter



Hinweis


Die Hinweismeldung beim Anlegen der zweiten DSL-Verbindung kann ignoriert werden. Routingkonflikte aufgrund von mehreren Standardrouten werden durch die IP-Lastverteilung verhindert!

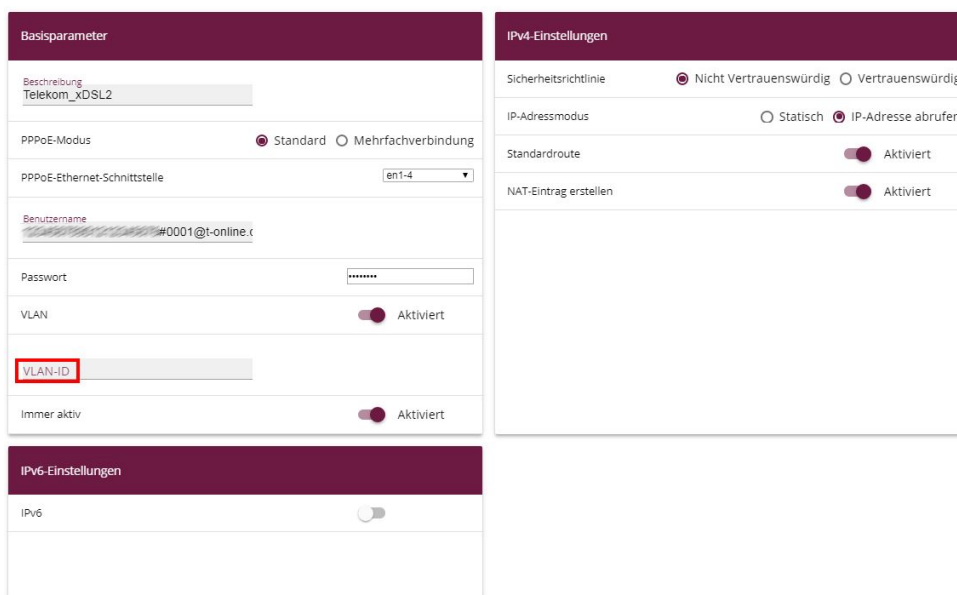
Gehen Sie folgendermaßen vor:

- (1) Bei **Beschreibung** geben Sie eine beliebige Bezeichnung für die Internetverbindung ein, z. B. *Telekom_xDSL2* ein.
- (2) Im Menüpunkt **Physischer Ethernet-Port** wählen Sie den Port aus an dem das xDSL-Modem angeschlossen ist, hier *ETH5* (das entspricht dem Anschluss LAN5 des Geräts).
- (3) Bei **Typ** wählen Sie die Option *Vordefiniert* aus.
- (4) Wählen Sie das **Land** aus, in dem der Internetzugang eingerichtet werden soll, hier *Germany*.
- (5) Wählen Sie Ihren **Internet Service Provider** aus der Liste aus, hier z. B. *Telekom*.
- (6) Bei **Anschlusskennung** geben Sie die 12-stellige Anschlusskennung ein, die Sie von

Ihrem Provider erhalten haben, z. B. *123456789012*.

- (7) Geben Sie die meist 12-stellige **Zugangsnummer** ein, die Sie von Ihrem Provider erhalten haben, z. B. *123456789012*.
- (8) Geben Sie **Persönliches Kennwort** ein, das Sie von Ihrem Provider erhalten haben, z. B. *test12345*.
- (9) Im Feld **Immer aktiv** legen Sie fest, ob die Internetverbindung immer aktiv sein soll. Aktivieren Sie diese Option nur, wenn Sie über einen Internetzugang mit Flatrate verfügen.
- (10) Das Kontrollkästchen **IPv6** bleibt deaktiviert.
- (11) Bestätigen Sie Ihre Angaben mit **OK**.

Je nach Einstellung des vorgelagerten Modems muss eventuell noch die **VLAN-ID 7** im Menü **WAN->Internet + Einwählen->PPPoE ->  -> Telekom_xDSL2** entfernt werden.



The screenshot displays the configuration interface for a WAN connection. It is divided into three main sections: Basisparameter, IPv4-Einstellungen, and IPv6-Einstellungen.

- Basisparameter:**
 - Beschreibung: Telekom_xDSL2
 - PPPoE-Modus: Standard Mehrfachverbindung
 - PPPoE-Ethernet-Schnittstelle: en1-4
 - Benutzername: #0001@t-online.c
 - Passwort: [masked]
 - VLAN: Aktiviert
 - VLAN-ID: [highlighted with a red box]
 - Immer aktiv: Aktiviert
- IPv4-Einstellungen:**
 - Sicherheitsrichtlinie: Nicht Vertrauenswürdig Vertrauenswürdig
 - IP-Adressmodus: Statisch IP-Adresse abrufen
 - Standardroute: Aktiviert
 - NAT-Eintrag erstellen: Aktiviert
- IPv6-Einstellungen:**
 - IPv6: Deaktiviert

Abb. 69: **WAN->Internet + Einwählen->PPPoE ->  -> Telekom_xDSL2**

8.2.2 Einstellung der WAN-Schnittstelle für die SIP-Verbindung

Im nächsten Schritt müssen die SIP-Verbindungen noch fest auf die jeweiligen xDSL-WAN-Schnittstellen gebunden werden.

Für die Verbindung über das interne Modem der **be.IP**, gehen Sie in das Menü **VoIP->Einstellungen->Standorte**.

Registrierungsverhalten für VoIP-Teilnehmer ohne definierten Standort

Standardverhalten

Keine Registrierung
 Registrierung nur in privaten Netzwerken
 Uneingeschränkte Registrierung

Standorte

Beschreibung	URLs/IP-Adressen / Schnittstellen	Max. Upstream-Bandbreite	Max. Downstream-Bandbreite
LAN	BRIDGE_BRO	-	-

Abb. 70: VoIP->Einstellungen->Standorte

Gehen Sie folgendermaßen vor:

- (1) Belassen Sie bei **Standardverhalten** die Einstellung *Registrierung nur in privaten Netzwerk*.
- (2) Klicken Sie auf **Neu** um neue Einträge hinzuzufügen.

Grundeinstellungen

Beschreibung
WAN_xDSL

Beinhalteter Standort (Parent) Keiner ▾

Typ Adressen Schnittstellen

Schnittstellen

Schnittstelle

WAN_GERMANY - TELEKOM ENTERTAIN ▾ 🗑️

HINZUFÜGEN

Bandbreitenbegrenzung Upstream

Bandbreitenbegrenzung Downstream

Abb. 71: VoIP-> Einstellungen-> Standorte-> Neu

- (3) Geben Sie eine **Beschreibung** für den Eintrag ein, hier z. B. *WAN_xDSL*.

- (4) Wählen Sie bei **Typ** die Option *Schnittstelle* aus. Der SIP-Standort wird über die verfügbaren Schnittstellen definiert.
- (5) Bei **Schnittstellen** klicken Sie auf **Hinzufügen** und wählen Sie die gewünschte Schnittstelle aus, hier *WAN_GERMANY - TELEKOM ENTERTAIN*.
- (6) Bestätigen Sie Ihre Angaben mit **OK**.

Die Konfiguration muss für **beide** xDSL-WAN-Verbindungen und die zugehörigen SIP-Verbindungen vorgenommen werden. Konfigurieren Sie das externe xDSL-Modem analog zur Konfiguration des internen Modems.

- (1) Geben Sie eine **Beschreibung** für den Eintrag ein, hier z. B. *Telekom_xDSL2*.
- (2) Wählen Sie bei **Typ** die Option *Schnittstelle* aus.
- (3) Bei **Schnittstellen** klicken Sie auf **Hinzufügen** und wählen Sie die gewünschte Schnittstelle aus, hier *WAN_TELEKOM_xDSL2*.
- (4) Bestätigen Sie Ihre Angaben mit **OK**.

Wählen Sie nun zu dem Anschluss der Deutschen Telekom den neu definierten **Standort** aus.

Gehen Sie dazu in das Menü **VoIP->Einstellungen->SIP-Provider**.



Nr.	Beschreibung	Registrar	Anschlussart	Status	Aktion
1	+49911...	tel.c-online.de	Einzelrufnummer	🕒	⌆ ⌵ 🗑️ ✎

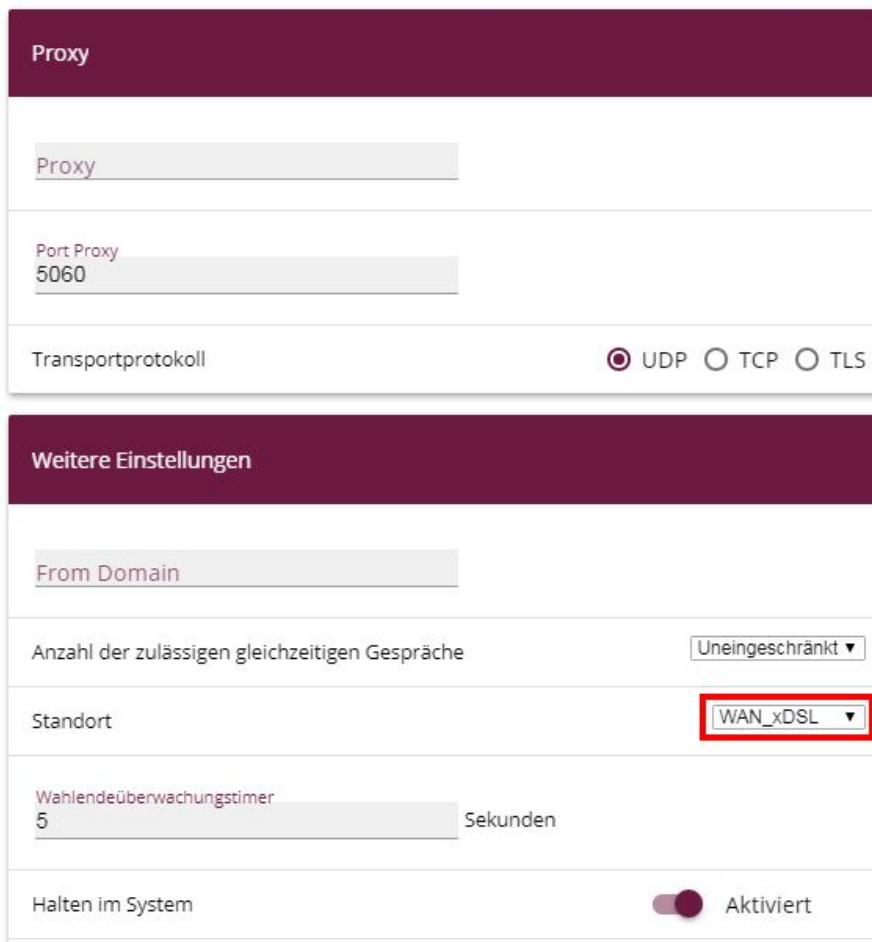
Seite: 1, Objekte: 1 - 1, Max. Anzahl 25

Abb. 72: **VoIP->Einstellungen->SIP-Provider**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie das Symbol **✎**, um den SIP-Provider zu bearbeiten.
- (2) Klicken Sie auf **Erweiterte Einstellungen**.

Erweiterte E



Proxy

Proxy

Port Proxy
5060

Transportprotokoll UDP TCP TLS

Weitere Einstellungen

From Domain

Anzahl der zulässigen gleichzeitigen Gespräche

Standort

Wahlendeüberwachungstimer
5 Sekunden

Halten im System Aktiviert

Abb. 73: VoIP -> Einstellungen -> SIP-Provider -> Neu+ Erweiterte Einstellungen

- (3) Wählen Sie den neu definierten **Standort** des SIP-Providers aus, hier *WAN_xDSL*.
- (4) Bestätigen Sie Ihre Angaben mit **OK**.

8.2.3 Einrichtung der Lastverteilung

Zur Einrichtung der Lastverteilung muss zunächst eine **Lastverteilungsgruppe** angelegt werden.

Gehen Sie in das Menü **Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu**.

The image shows two screenshots from a web interface. The top screenshot is titled 'Basisparameter' and contains the following fields: 'Gruppenbeschreibung' with the value 'xDSL1/xDSL2', 'Verteilungsrichtlinie' with a dropdown menu set to 'Sitzungs-Round-Robin', and 'Verteilungsmodus' with radio buttons for 'Immer' (unselected) and 'Nur aktive Schnittstellen verwenden' (selected). The bottom screenshot is titled 'Schnittstellenauswahl für Verteilung' and shows a table with columns: 'Schnittstelle', 'Verteilungsverhältnis', 'Routenselektor', and 'IP-Adresse zur Nachverfolgung'. Below the table is a 'HINZUFÜGEN' button and a horizontal scrollbar.

Abb. 74: **Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine beliebige **Gruppenbeschreibung** ein, z. B. *xDSL1/xDSL2*.
- (2) Bei **Verteilungsrichtlinie** wählen Sie das Verfahren aus, nach dem die Daten verteilt werden, hier *Sitzungs-Round-Robin* .
Anschließend können die beiden xDSL-Internetzugänge zu dieser Lastverteilungsgruppe hinzugefügt werden.
- (3) Klicken Sie dazu auf **Hinzufügen**.

The image shows two screenshots from a web interface. The top screenshot is titled 'Basisparameter' and contains the following fields: 'Gruppenbeschreibung' with the value 'xDSL1/xDSL2', 'Verteilungsrichtlinie' with the value 'Sitzungs-Round-Robin'. The bottom screenshot is titled 'Schnittstellenauswahl für Verteilung' and shows a table with columns: 'Schnittstelle', 'Verteilungsverhältnis', 'Routenselektor', and 'IP-Adresse zur Nachverfolgung'. Below the table is a 'HINZUFÜGEN' button and a horizontal scrollbar. The 'Schnittstelle' dropdown is set to 'WAN_GERMANY - TELEKOM ENTERTAIN' and the 'Verteilungsverhältnis' is set to '50 %'.

Abb. 75: **Netzwerk-> Lastverteilung-> Lastverteilungsgruppen ->Neu ->Hinzufügen**

- (4) Wählen Sie bei **Schnittstelle** den ersten xDSL-Zugang *WAN_GERMANY - TELEKOM ENTERTAIN* aus.
- (5) Unter **Verteilungsverhältnis** geben Sie an, welchen Prozentsatz des Datenverkehrs eine Schnittstelle übernehmen soll. In unserem Beispiel sind das *50 %*.
- (6) Klicken Sie auf **Übernehmen**.
- (7) Fügen Sie mit **Hinzufügen** die zweite xDSL-Leitung hinzu.

The image shows two screenshots of a network configuration interface. The first screenshot, titled 'Basisparameter', shows a table with two rows: 'Gruppenbeschreibung' with the value 'xDSL1/xDSL2' and 'Verteilungsrichtlinie' with the value 'Sitzungs-Round-Robin'. The second screenshot, titled 'Schnittstellenauswahl für Verteilung', shows a dropdown menu for 'Schnittstelle' set to 'WAN_TELEKOM_XDSL2' and a percentage input field for 'Verteilungsverhältnis' set to '50 %'.

Abb. 76: **Netzwerk-> Lastverteilung-> Lastverteilungsgruppen ->Neu ->Hinzufügen**

- (8) Wählen Sie bei **Schnittstelle** den zweiten xDSL-Zugang *WAN_TELEKOM_XDSL2* aus.
- (9) Und bei **Verteilungsverhältnis** geben Sie *50 %* ein.
- (10) Klicken Sie auf **Übernehmen**.

Nach diesem Konfigurationsschritt sind bereits beide Internetverbindungen mit Hilfe der Lastverteilung verwendbar.





Schnittstellenauswahl für Verteilung			
Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung
WAN_GERMANY - TELEKOM ENTERTAIN	50 %		 
WAN_TELEKOM_XDSL2	50 %		 
HINZUFÜGEN			

Abb. 77: **Netzwerk->Lastverteilung->Lastverteilungsgruppen**

Bei unterschiedlichen Geschwindigkeiten der WAN-Strecken oder bei einer höheren Anzahl der an der Lastverteilung beteiligten WAN-Strecken sind die Verteilungsverhältnisse entsprechend anzupassen.

8.2.4 Spezielle Lastverteilungs-Behandlung von verschlüsselten Verbindungen

Mit der bis jetzt abgeschlossenen Konfiguration werden IP-Sitzungen jeweils zur Hälfte auf die beiden xDSL-Leitungen verteilt. Dadurch kann es bei bestimmten Protokollen (z. B. verschlüsselten HTTPS-Verbindungen) zu Problemen und Verbindungsabbrüchen kommen. Die Ursache dieser Verbindungsprobleme liegt an der unterschiedlichen Internet IP-Adresse der beiden xDSL-Verbindungen. Bei parallelen Verbindungen zum gleichen Server würden beide xDSL-Leitungen wechselseitig verwendet werden. Zur Umgehung dieser Schwierigkeit können zusammengehörige IP-Sitzungen vorübergehend auf eine der Internet-Verbindungen gebunden werden. Im Menü **Special Session Handling** wird die spezielle Behandlung solcher kritischer Verbindungen konfiguriert.

Gehen Sie in das Menü **Netzwerk->Lastverteilung->Special Session Handling->Neu**.

Basisparameter	
Admin-Status	<input checked="" type="checkbox"/> Aktiviert
Beschreibung	<input type="text" value="https"/>
Dienst	<input type="text" value="http (SSL)"/>
Ziel-IP-Adresse/Netzmaske	<input type="text" value="Beliebig"/>
Quellschnittstelle	<input type="text" value="Beliebig"/>
Quell-IP-Adresse/Netzmaske	<input type="text" value="Beliebig"/>
Special Handling Timer	<input type="text" value="900"/> Sekunden

Abb. 78: **Netzwerk->Lastverteilung->Special Session Handling->Neu**

Gehen Sie folgendermaßen vor:

- (1) Bei **Beschreibung** geben Sie eine Bezeichnung für den Eintrag, z. B. *https* ein.
- (2) Bei **Dienst** wählen Sie *http (SSL)* aus.
- (3) Den **Special Handling Timer** stellen Sie auf *900* Sekunden.
- (4) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.
- (5) Klicken Sie erneut auf **Neu**.

Basisparameter	
Admin-Status	<input checked="" type="checkbox"/> Aktiviert
Beschreibung	ssh
Dienst	ssh ▼
Ziel-IP-Adresse/Netzmaske	Beliebig ▼
Quellschnittstelle	Beliebig ▼
Quell-IP-Adresse/Netzmaske	Beliebig ▼
Special Handling Timer	900 Sekunden

Abb. 79: **Netzwerk->Lastverteilung->Special Session Handling->Neu**

- (1) Geben Sie eine **Beschreibung** für den Eintrag ein, z. B. *ssh*.
- (2) Wählen Sie den **Dienst** *ssh* aus.
- (3) Den **Special Handling Timer** stellen Sie auf *900* Sekunden.
- (4) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.


8.2.5 Anpassen der Metrik

Da eine Lastverteilungsgruppe nur dann aktiv wird, wenn die zu den WAN-Verbindungen gehörenden Standardrouten die gleiche Metrik aufweisen, muss die in einem früheren Schritt auf *0* geänderte Metrik der WAN-Verbindung nun zurück auf die Metrik *1* gesetzt werden.

Gehen Sie in das Menü **Netzwerk->Routen->Konfiguration von IPv4-Routen** .

Routen							Erweiterte Route
Ziel-IP-Adresse	Netzmaske	Gateway	Schnittstelle	Metrik	Routentyp		
0.0.0.0	0.0.0.0	0.0.0.0	WAN_GERMANY - TELEKOM ENTERTAIN	0	Standardroute über Gateway	<input type="checkbox"/>	
0.0.0.0	0.0.0.0	0.0.0.0	WAN_TELEKOM_XDSL2	1	Standardroute über Gateway	<input type="checkbox"/>	

Abb. 80: Netzwerk->Routen->Konfiguration von IPv4-Routen

(1) Klicken Sie auf das -Symbol um den Eintrag zu bearbeiten.

Basisparameter		Routenparameter	
Routentyp	Standardroute über Gateway	Gateway-IP-Adresse	0.0.0.0
Schnittstelle	WAN_GERMANY - TELEKOM ENTERTAIN	Metrik	1
Routenklasse	<input checked="" type="radio"/> Standard <input type="radio"/> Erweitert		

Abb. 81: Netzwerk ->Routen ->Konfiguration von IPv4-Routen -> 

- (2) Wählen Sie bei **Metrik** die Priorität der Route aus, in unserem Beispiel die 1.
- (3) Bestätigen Sie mit **OK**.

Die Lastverteilung zwischen den beiden xDSL-Verbindungen ist jetzt aktiv.

8.3 Abschließende Bemerkungen

Sollen IPSec-Tunnel von einer bestimmten Schnittstelle der in der Lastverteilungsgruppe beteiligten Schnittstellen initiiert werden, so ist das in den **Erweiterten Einstellungen** des jeweiligen Tunnels im IPSec-Menü anzugeben.



Für eine per NAT/PAT eingetragene Weiterleitung wird in der Antwort automatisch wieder die identische WAN-Schnittstelle gewählt, über die die Anfrage gestellt wurde. Es sind keine weiteren Konfigurationsschritte notwendig.

IPv6-Datenverkehr wird im Beispiel nur über die erste xDSL-WAN-Verbindung geroutet, aber in die Auslastung der Schnittstelle mit einberechnet.

Beherrschen beide WAN-Verbindungen einer Lastverteilungsgruppe IPv6, muss es auf einem der beiden deaktiviert werden. In IPv6 gibt es keinen NAT-Mechanismus und ein proprietäres sog. „Prefix Masking“ ist nicht implementiert. Da die Auswahl der Quell-IP aber Sache des Netzwerk-Clients hinter der **be.IP** ist, kann ansonsten keine einwandfreie Funktion von Diensten garantiert werden.

8.4 Konfigurationsschritte im Überblick

WAN-Verbindung über das interne Modem einrichten

Feld	Menü	Wert
IPv6	WAN-> Internet + Einwählen ->PP-PoE ->Germany - Telekom Entertainment -> 	Aktiviert
Metrik	Netzwerk ->Routen ->Konfiguration von IPv4-Routen -> 	0

WAN-Verbindung über das externe Modem einrichten

Feld	Menü	Wert
Verbindungstyp	Assistenten ->Internetzugang ->Internetverbindungen ->Neu	Externes xDSL-Modem
Beschreibung	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	z. B. Telekom_xDSL2
Physischer Ethernet-Port	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	z. B. ETH5
Typ	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	Vordefiniert
Land	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	Germany
Internet Service Provider	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	z. B. Telekom
Anschlusskennung	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	z. B. 123456789012
Zugangsnummer	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	z. B. 123456789012
Mitbenutzernummer	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	0001
Persönliches Kennwort	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	z. B. test12345
Immer aktiv	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	Aktiviert
IPv6	Assistenten ->Internetzugang ->Internetverbindungen ->Neu ->Weiter	Deaktiviert

WAN-Verbindung über das externe Modem einrichten


Feld	Menü	Wert
Standardverhalten	VoIP-> Einstellungen-> Standorte	<i>Registrierung nur in privaten Netzwerk</i>
Beschreibung	VoIP-> Einstellungen-> Standorte-> Neu	z. B. <i>WAN_xDSL</i>
Typ	VoIP-> Einstellungen-> Standorte-> Neu	<i>Schnittstellen</i>
Schnittstellen	VoIP-> Einstellungen-> Standorte-> Neu	Hinzufügen und <i>WAN_GERMANY - TELEKOM ENTERTAIN</i>
Standort	VoIP-> Einstellungen-> SIP-Provider -> Neu+ Erweiterte Einstellungen	<i>WAN_xDSL</i>
Beschreibung	VoIP-> Einstellungen-> Standorte-> Neu	z. B. <i>Telekom_xDSL2</i>
Typ	VoIP-> Einstellungen-> Standorte-> Neu	<i>Schnittstellen</i>
Schnittstellen	VoIP-> Einstellungen-> Standorte-> Neu	Hinzufügen und <i>WAN_TELEKOM_XDSL2</i>

Einrichtung der Lastverteilung

Feld	Menü	Wert
Gruppenbeschreibung	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	z. B. <i>xDSL1 / xDSL2</i>
Verteilungsrichtlinie	Netzwerk-> Lastverteilung-> Lastverteilungsgruppen-> Neu	<i>Sitzungs-Round-Robin</i>
Schnittstelle	Netzwerk-> Lastverteilung-> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>WAN_GERMANY - TELEKOM ENTERTAIN</i>
Verteilungsverhältnis	Netzwerk-> Lastverteilung-> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>50 %</i>
Schnittstelle	Netzwerk-> Lastverteilung-> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>WAN_TELEKOM_XDSL2</i>
Verteilungsverhältnis	Netzwerk-> Lastverteilung-> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>50 %</i>

Feld	Menü	Wert
	fügen	
Beschreibung	Netzwerk-> Lastverteilung-> Special Session Handling ->Neu	z. B. <i>https</i>
Dienst	Netzwerk-> Lastverteilung-> Special Session Handling ->Neu	<i>http (SSL)</i>
Special Handling Timer	Netzwerk-> Lastverteilung-> Special Session Handling ->Neu	900 Sekunden
Beschreibung	Netzwerk-> Lastverteilung-> Special Session Handling ->Neu	z. B. <i>ssh</i>
Dienst	Netzwerk-> Lastverteilung-> Special Session Handling ->Neu	<i>ssh</i>
Special Handling Timer	Netzwerk-> Lastverteilung-> Special Session Handling ->Neu	900 Sekunden

Anpassen der Metrik

Feld	Menü	Wert
Metrik	Netzwerk ->Routen ->Konfiguration von IPv4-Routen -> 	1

Kapitel 9 Telefonieren über einen SIP-Provider mithilfe der be.IP plus

9.1 Einleitung

Im Folgenden wird die Einrichtung eines SIP-Providers in der **be.IP plus** beschrieben.



Hinweis

Die Angaben auf den Bildern dienen nur als Beispiel. Bitte verwenden Sie die Daten, die Sie von Ihrem SIP-Provider erhalten haben.

Eine Übersicht der bisher getesteten SIP-Provider finden Sie im Internet unter http://faq.bintec-elmeg.com/index.php/Konfiguration_SIP_Provider.

Bei Benutzung eines Inland-SIP-Providers sind einige Voreinstellungen von Bedeutung, um z. B. bei einem Ortsgespräch nicht die gesamte Vorwahl und Rufnummer einzugeben, sondern nur die Rufnummer.

Variante 1

In diesem Beispiel ist die **be.IP plus** durch ihr internes DSL-Modem direkt mit dem Internet verbunden.

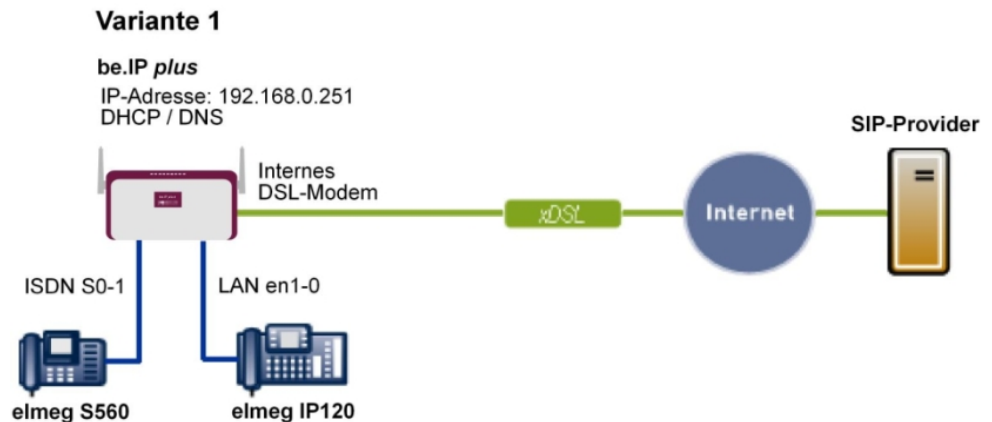


Abb. 82: Beispielszenario

Voraussetzungen

- Ein Internetzugang über das integrierte ADSL/ADSL2+-Modem
- Eine **be.IP plus** mit Systemsoftware-Version 10.1 Rev. 5 oder neuer wird als DHCP- und DNS-Server im Netzwerk verwendet.
- **elmeg IP120**-Telefone mit Firmware-Version 01.00.04 oder neuer
- **elmeg S560**-Telefone mit Firmware-Version 1.400 oder neuer
- Anbindung der **be.IP plus** an alle Endgeräte und Anschlüsse nach Anschaltplan

Variante 2

In diesem Beispiel wird die Integration einer **be.IP plus** in ein vorhandenes Netzwerk mit einem Gateway, z. B. **bintec RS353jw**, beschrieben.

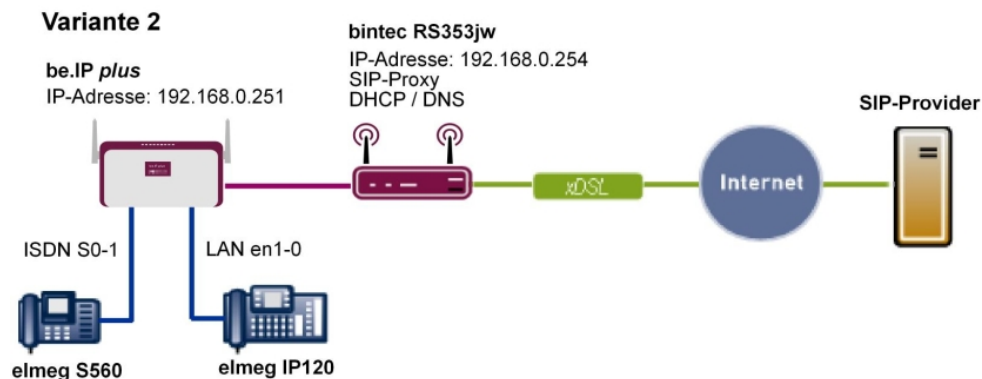


Abb. 83: Beispielszenario

Voraussetzungen

- Ein vorhandenes Netzwerk mit einem **bintec RS353jw** Gateway mit Systemsoftware-Version 10.1 Rev. 4 oder neuer. Das **bintec RS353jw** Gateway wird als DHCP- und DNS-Server im Netzwerk verwendet.
- Eine **be.IP plus** mit Systemsoftware-Version 10.1 Rev. 5 oder neuer
- **elmeg IP120** Telefone mit Firmware-Version 01.00.04 oder neuer
- **elmeg S560** Telefone mit Firmware-Version 1.400 oder neuer
- Anbindung der **be.IP plus** an alle Endgeräte und Anschlüsse nach Anschaltplan

9.2 Vorbereitende Konfiguration



Hinweis

Für die allgemeine Netzwerkkonfiguration folgen Sie den Assistenten **Erste Schritte** und **Internetzugang**.

9.2.1 Variante 1: Netzwerkkonfiguration mit direktem Internetanschluss

9.2.1.1 Konfiguration der be.IP plus

Sie müssen Ihre **be.IP plus** als DHCP-Server konfigurieren.



Hinweis

Für die Konfiguration der **be.IP plus** als DHCP-Server lesen Sie bitte die Kapitel zur Variante 3 des Telefonie-Workshops "Anbindung von **elmeg-Telefonen**".

9.2.2 Variante 2: Netzwerkkonfiguration mit Gateway

9.2.2.1 Konfiguration des Gateways (bintec RS353jw)

Sie müssen die VoIP-Einstellungen des Gateways anpassen. Die Konfiguration erfolgt über das GUI des Gateways. Zusätzlich muss ein DHCP-Server eingerichtet werden.



Hinweis

Für die Konfiguration des DHCP-Servers lesen Sie bitte die Kapitel zu den Varianten 1 und 2 des Telefonie-Workshops "Anbindung von **elmeg-Telefonen**".

- (1) Gehen Sie zu **Assistenten->VoIP PBX im LAN->Neu**.
- (2) Wählen Sie die **WAN-Schnittstelle für VoIP-Priorisierung** aus, über die die VoIP PBX in Ihrem LAN das Internet erreichen soll, hier *Internet-PPPoE*.
- (3) Klicken Sie auf **Weiter**.

Geben Sie die Einstellungen der VoIP PBX im LAN ein: ?

WAN-Schnittstelle für VoIP-Priorisierung efm35-60


Maximale Upload-Geschwindigkeit
 kbit/s

DSCP-Wert zur Priorisierung von RTP-Daten TOS-Binärwert ▼

DSCP-Wert zur Priorisierung von SIP-Protokoll-Meldungen TOS-Binärwert ▼

IP-Adresse der VoIP PBX im LAN

IP Adresse

HINZUFÜGEN

Port-STUN-Server

Port-SIP-Server

Abb. 84: VoIP->SIP->Options

Gehen Sie folgendermaßen vor, um die SIP-Einstellungen vorzunehmen:

- (1) Geben Sie die **Maximale Upload-Geschwindigkeit** Ihrer Internet-Verbindung ein, hier z. B. *2000* kbit/s.
- (2) Die Parameter **DSCP-Wert zur Priorisierung von RTP-Daten** und **DSCP-Wert zur Priorisierung von SIP-Protokoll-Meldungen** sind vom Hersteller der TK-Anlage bzw. des VoIP-Telefons zu erfahren.

- (3) Geben Sie die **IP-Adresse der VoIP PBX im LAN** ein, hier z. B. `192.168.0.251`.
- (4) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.



Hinweis

Nehmen Sie obige Einstellungen in jedem Fall vor, da es sonst zu Problemen bei Gesprächen über einen SIP-Provider kommen kann.

9.2.2.2 Konfiguration der be.IP plus

Sie müssen die Gateway- und den DNS-Server-Einstellungen der **be.IP plus** konfigurieren. Die Konfiguration erfolgt über das GUI der **be.IP plus**.

- (1) Gehen Sie zu **Assistenten->Erste Schritte->Grundeinstellungen**.

<p>Geben Sie die Grundeinstellungen des Systems ein: ?</p> <p>Systemname be_ip_plus</p> <p>Standort</p> <p>Kontakt BINTECELMG</p>	<p>Geben Sie das Kennwort für den Systemadministrator ein: ?</p> <p>Systemadministrator-Kennwort *****</p> <p>Systemadministrator-Kennwort bestätigen *****</p>
<p>Wählen Sie den physikalischen Ethernet-Port für die LAN-Verbindung aus: ?</p> <p>Physikalischer Ethernet-Port (LAN) ETH1 ▾</p>	<p>Geben Sie die IPv4-LAN-Konfiguration ein: ?</p> <p>Logische Ethernet-/Bridge-Schnittstelle br0</p> <p>Adressmodus <input checked="" type="radio"/> Statisch <input type="radio"/> DHCP-Client</p> <p>IP-Adresse 192.168.0.251</p> <p>Netzmaske 255.255.255.0</p> <p>Standard-Gateway-IP-Adresse 192.168.0.254</p> <p>Feste DNS-Server-Adresse <input checked="" type="checkbox"/> Aktiviert</p> <p>DNS-Server 1 192.168.0.254</p> <p>DNS-Server 2 0.0.0.0</p> <p>⚠ Warnung! Konfigurationsverbindung geht möglicherweise beim Ändern der IP-Adresse verloren! Klicken Sie auf "OK", und melden Sie sich erneut an, um fortzufahren!</p>
<p>Wird dieses Gerät als DHCPv4-Server verwendet? ?</p> <p>Dieses Gerät als DHCPv4-Server verwenden <input type="checkbox"/></p>	<p>IPv6-Konfiguration eingeben ?</p> <p>IPv6 <input type="checkbox"/></p>

Abb. 85: Assistenten->Erste Schritte->Grundeinstellungen

Gehen Sie folgendermaßen vor, um die Gateway- und DNS-Einstellungen vorzunehmen:

- (1) Geben Sie unter **Standard-Gateway-IP-Adresse** die IP-Adresse Ihres Gateways ein,

das den Internetzugang bereitstellt, z. B. *192.168.0.254*.

- (2) Aktivieren Sie **Feste DNS-Server-Adresse**.
- (3) Geben Sie unter **DNS-Server 1** die IP-Adresse des Name-Servers für die Namensauflösung von Internet-Adressen ein, hier *192.168.0.254*.
- (4) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

9.2.3 Variante 1 + 2: Konfiguration der Ländereinstellungen in der be.IP plus

Durch die Einstellung der Parameter **Internationaler Präfix / Länderkennzahl** und **Nationaler Präfix / Ortsnetzkenzahl** werden bei der Wahl über den SIP-Provider die internationale und nationale Rufnummer automatisch und ohne zusätzliche Eingaben erzeugt. Die Konfiguration ermöglicht auch eine korrekte Rufverteilung bei ankommenden Anrufen über den SIP-Provider.

- (1) Gehen Sie zu **Systemverwaltung -> Globale Einstellungen -> System**.

The image shows a web-based configuration interface for a SIP system. It is divided into three main sections:

- Grundeinstellungen (Basic Settings):**
 - Systemname: be.ip_plus
 - Standort: (empty field)
 - Kontakt: BINTECELMEG
 - Maximale Anzahl der Syslog-Protokolleinträge: 50
 - Maximales Nachrichtenlevel von Systemprotokolleinträgen: Information (dropdown menu)
 - Maximale Anzahl der Accounting-Protokolleinträge: 20
 - Herstellernamen anzeigen: Aktiviert
 - Konfiguration der automatischen Speicherung:
- Systemeinstellungen (System Settings):**
 - Signalisierung der Übergabe: Mit Freiton Mit Wartemusik (Music On Hold, MoH)
 - Übergabe auf besetzten Teilnehmer: Deaktiviert
 - Abwurf auf Rufnummer: Kein Abwurf - Besetztton (dropdown menu)
 - Externe Verbindungen zusammenschalten:
- Ländereinstellungen (Country Settings):**
 - Ländereinstellung: Deutschland (dropdown menu)
 - Internationaler Präfix / Länderkennzahl: 00 / 49
 - Nationaler Präfix / Ortsnetzkenzahl: 0 / 911

Abb. 86: Systemverwaltung ->Globale Einstellungen->System

Gehen Sie folgendermaßen vor, um die Kennzahlen zu konfigurieren:

- (1) Bei **Internationaler Präfix / Länderkennzahl** tragen Sie die Länderkennzahl ein, z. B. für Deutschland die 49. Ohne den Eintrag muss bei SIP-Providern immer die vollständige Rufnummer mit Länderkennzahl gewählt werden.
- (2) Bei **Nationaler Präfix / Ortsnetzkenzahl** tragen Sie die Ortskennzahl für den Ort ein, an dem Ihr System installiert ist, z. B. 911 für Nürnberg. Ohne den Eintrag muss bei SIP-Providern für Ortsgespräche die Rufnummer mit nationalem Präfix / Ortskennzahl gewählt werden.
- (3) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

9.3 Variante 1 + 2: Konfiguration des SIP-Providers in der be.IP plus

Ein VoIP-Anschluss kann als Einzelrufnummer- oder Durchwahl-Anschluss konfiguriert werden. Diese Bezeichnungen entsprechen Mehrgeräte- bzw. Anlagenanschlüssen bei ISDN.

Bei einem Einzelrufnummer-Anschluss erhalten Sie vom SIP-Provider eine oder mehrere Rufnummern.

Bei einem Durchwahl-Anschluss erhalten Sie vom SIP-Provider eine Basisrufnummer mit mehreren Durchwahlrufnummern (Rufnummernplan). Beispiel: Basisrufnummer = 1234; Durchwahlrufnummern: 1, 2, ...; Rufnummern: 1234 - 1, 1234 - 2, ...

9.3.1 SIP-Provider (Einzelrufnummer)

Im Folgenden wird die Einrichtung eines SIP-Providers bei Verwendung eines Einzelrufnummer-Anschlusses beschrieben.

- (1) Gehen Sie zu **Assistenten->Telefonie->Anschlüsse->Neu**.
- (2) Wählen Sie unter **Verbindungstyp** *SIP-Einzelrufnummer*.
- (3) Bei **Typ** wählen Sie *Benutzerdefiniert*.
- (4) Klicken Sie auf **Weiter**.

SIP-Provider-Einstellungen ?

Name

Anschlussart Einzelrufnummer

Authentifizierungs-ID

Passwort

Benutzername

Registrar

Domäne

Rufnummern ?

Einzelrufnummer (MSN)	Beschreibung	
<input type="text" value="49911148797640"/>	<input type="text" value="Sipgate_1"/>	<input type="button" value="🗑"/>

HINZUFÜGEN

Die Amtsleitung der Berechtigungsklasse zuweisen ?

Berechtigungsklasse

HINZUFÜGEN

Erweiterte Einstellungen

Registrar ?

Port Registrar

Transportprotokoll UDP TCP TLS

STUN-Server ?

STUN-Server

Port:STUN-Server

Weitere Einstellungen ?

Internationale Rufnummer erzeugen Aktiviert

Nationale Rufnummer erzeugen Aktiviert

SIP-Header-Feld: FROM Display

SIP-Header-Feld: FROM User

SIP-Header-Feld: P-Preferred

SIP-Header-Feld: P-Asserted

Abb. 88: **Assistenten->Telefonie->Anschlüsse->Neu-> <SIP-Provider>**

Gehen Sie folgendermaßen vor, um die Anmeldedaten des SIP-Providers zu hinterlegen:



Hinweis

Bei einem Gateway mit eingerichteten VoIP PBX im LAN-Assistenten muss bei einigen SIP-Providern ein **STUN-Server** konfiguriert werden.

- (1) Geben Sie unter **Name** eine Bezeichnung für den SIP-Provider ein, z. B. *Sipgate_Plus_1*.
- (2) Geben Sie die **Authentifizierungs-ID** (SIP-ID) Ihres Providers ein, z. B. *1527861e0*.
- (3) Geben Sie das **Passwort** ein, das Sie von Ihrem VoIP-Provider erhalten haben.
- (4) Geben Sie unter **Benutzername** den Namen ein, den Sie von Ihrem VoIP-Provider erhalten haben, z. B. *1527861e0*. Dieser entspricht bei den Providern Sipgate, 1&1, QSC und Toplink der SIP-ID.
- (5) Geben Sie als SIP **Registrar** eine IP-Adresse oder einen Domänennamen an.
 - Für Sipgate Basic / Plus: *sipgate.de*
 - Für 1&1: *sip.lund1.de*
 - Für QSC-IPfonie basic: *sip.qsc.de*
 - Für die Anbindung des Call & Surf Comfort IP-Anschlusses der Deutschen Telekom: *tel.t-online.de*
 - Für Toplink: *toplink-voice.de*
- (6) Legen Sie unter **Einzelrufnummer (MSN)** mit **Hinzufügen** einen neuen Eintrag an. Geben Sie unter **Einzelrufnummer (MSN)** die Rufnummer ein, die Sie von Ihrem VoIP-Provider erhalten haben, z. B. *4911148797640*. Geben Sie unter **Angezeigter Name** eine Bezeichnung für den Anschluss ein, z. B. *Sipgate_1*. Diese wird für ankommende Anrufe am Systemtelefon angezeigt.




Hinweis

Für die Provider QSC-IPfonie basic und Toplink können hier mehrere Rufnummern konfiguriert werden.

Bei den Providern Sipgate Basic / Plus, 1&1 und Deutsche Telekom muss für jede weitere Rufnummer des SIP-Providers ein weiterer SIP-Anschluss mit eigenen SIP-Accountdaten angelegt werden. Um abgehende Telefonate über weitere Rufnummern bzw. SIP-Anschlüsse zu ermöglichen, sollten unter **Nummerierung->Benutzereinstellungen->Berechtigungsklassen** zusätzliche Berechtigungsklassen konfiguriert werden.

- (7) Die **Berechtigungsklasse** belassen Sie bei *Uneingeschränkt*.
- (8) Aktivieren Sie **Internationale Rufnummer erzeugen** und **Nationale Rufnummer er-**

zeugen.


- (9) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.
Nach erfolgreicher Registrierung der Anlage beim SIP-Provider wechselt die Statusanzeige des jeweiligen SIP-Anschlusses auf .

9.3.1.1 1&1

Beim SIP-Provider 1&1 muss bei der eingehenden Nummer das Präfix *49* durch *0* ersetzt werden. Damit werden bei ankommenden Anrufen die Rufnummern bzw. Namen aus dem Systemtelefonbuch korrekt angezeigt.

- (1) Gehen Sie zu **VoIP->Einstellungen->SIP-Provider-> <1und1> ->** .

<div style="background-color: #4b0032; color: white; padding: 5px;">Grundeinstellungen</div> <div style="padding: 5px;"> <p>Beschreibung 1und1_1</p> <p>Provider-Status <input checked="" type="radio"/> Aktiv <input type="radio"/> Inaktiv</p> <p>Anschlussart <input checked="" type="radio"/> Einzelrufnummer <input type="radio"/> Durchwahl</p> <p>Authentifizierungs-ID 4991198067344</p> <p>Passwort *****</p> <p>Benutzername 4991198067344</p> <p>Domäne</p> </div>	<div style="background-color: #4b0032; color: white; padding: 5px;">Einstellungen für Gehende Rufnummer</div> <div style="padding: 5px;"> <p>Gehende Rufnummer Standard</p> </div>
<div style="background-color: #4b0032; color: white; padding: 5px;">Registrar</div> <div style="padding: 5px;"> <p>Registrar sip.1und1.de</p> <p>Port Registrar 5060</p> <p>Transportprotokoll <input checked="" type="radio"/> UDP <input type="radio"/> TCP <input type="radio"/> TLS</p> </div>	<div style="background-color: #4b0032; color: white; padding: 5px;">STUN</div> <div style="padding: 5px;"> <p>STUN-Server</p> <p>Port-STUN-Server 3478</p> </div>
<div style="background-color: #4b0032; color: white; padding: 5px;">Timer</div> <div style="padding: 5px;"> <p>Registrierungstimer 600 Sekunden</p> </div>	

Abb. 89: **VoIP->Einstellungen->SIP-Provider-> <1und1> ->** .

	<input type="checkbox"/> Privacy User
	<input checked="" type="checkbox"/> Privacy ID
SIP-Header-Feld: FROM Display	Keiner
SIP-Header-Feld: FROM User	Benutzername
SIP-Header-Feld: P-Preferred	Keiner
SIP-Header-Feld: P-Asserted	Keiner
Ersetzen des internationalen Präfix durch "+"	<input type="checkbox"/>
Anmeldung eines Proxys erlauben	<input type="checkbox"/>
SIP-Bindungen nach Neustart löschen	<input checked="" type="checkbox"/> Aktiviert
Vorgeschaltetes Gerät mit NAT	<input type="checkbox"/>
Early-Media-Unterstützung	<input checked="" type="checkbox"/> Aktiviert
Art der Registrierung	<input checked="" type="radio"/> Einzel <input type="radio"/> Bulk (BNC) <input type="radio"/> Keine Registrierung
T.38 FAX Unterstützung	<input checked="" type="checkbox"/> Aktiviert
Ersetzen des Präfix der eingehenden Nummer	49 ersetzen durch 0
SIP Update senden	<input type="checkbox"/>
Anfrage-URI	<input type="checkbox"/>
Quell-IP-Adresse überprüfen	<input type="checkbox"/>
Überprüfung des TLS-Zertifikats	<input type="checkbox"/>

Abb. 90: VoIP->Einstellungen->SIP-Provider-> <1und1> ->  ->Erweiterte Einstellung

Gehen Sie folgendermaßen vor:

- (1) Geben Sie unter **Ersetzen des Präfix der eingehenden Nummer** 49 ein.
- (2) Geben Sie unter **ersetzen durch** 0 ein.
- (3) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.




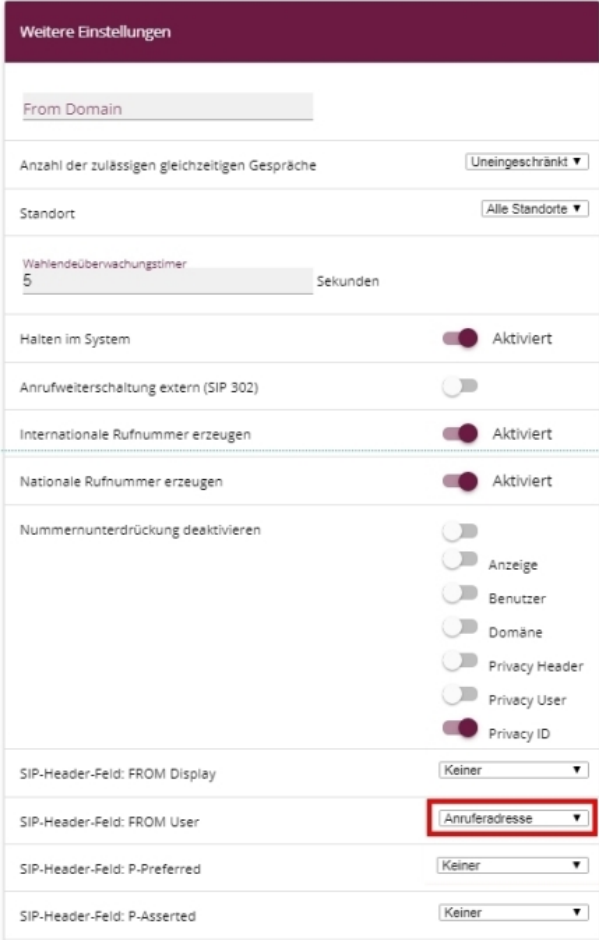
Hinweis

Wird der PBX-Assistent erneut für diesen Anschluss verwendet, werden alle Einstellungen im Menü **VoIP->Einstellungen->SIP-Provider** zurückgesetzt.


9.3.1.2 QSC-IPfonie basic

Beim SIP-Provider QSC-IPfonie basic muss für den **SIP-Header-Feld: FROM User** die Option *Anruferadresse* aktiviert werden. Damit wird es möglich, bei abgehenden Telefonaten unterschiedliche Rufnummern zu verwenden.

- (1) Gehen Sie zu **VoIP->Einstellungen->SIP-Provider-> <qsc_ipfonie_basic>** ->  -> **Erweiterte Einstellungen**.



Weitere Einstellungen	
From Domain	
Anzahl der zulässigen gleichzeitigen Gespräche	Uneingeschränkt ▼
Standort	Alle Standorte ▼
Wahlendeüberwachungstimer	5 Sekunden
Halten im System	<input checked="" type="checkbox"/> Aktiviert
Anrufweilerschaltung extern (SIP 302)	<input type="checkbox"/>
Internationale Rufnummer erzeugen	<input checked="" type="checkbox"/> Aktiviert
Nationale Rufnummer erzeugen	<input checked="" type="checkbox"/> Aktiviert
Nummernunterdrückung deaktivieren	<input type="checkbox"/> <input type="checkbox"/> Anzeige <input type="checkbox"/> Benutzer <input type="checkbox"/> Domäne <input type="checkbox"/> Privacy Header <input type="checkbox"/> Privacy User <input checked="" type="checkbox"/> Privacy ID
SIP-Header-Feld: FROM Display	Keiner ▼
SIP-Header-Feld: FROM User	Anruferadresse ▼
SIP-Header-Feld: P-Preferred	Keiner ▼
SIP-Header-Feld: P-Asserted	Keiner ▼

Abb. 91: **VoIP->Einstellungen->SIP-Provider-> <qsc_ipfonie_basic>** ->  -> **Erweiterte Einstellungen**

Gehen Sie folgendermaßen vor, um den SIP-Header zu erweitern:

- (1) Aktivieren Sie unter **SIP-Header-Feld: FROM User** die Option *Anruferadresse*.

- (2) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.




Hinweis

Wird der PBX-Assistent erneut für diesen Anschluss verwendet, werden alle Einstellungen im Menü **VoIP->Einstellungen->SIP-Provider** zurückgesetzt.

9.3.1.3 Toplink

Beim SIP-Provider Toplink muss für den **SIP-Header-Feld: FROM User** die Option *Anruferadresse* aktiviert werden.

- (1) Gehen Sie zu **VoIP->Einstellungen->SIP-Provider-> <toplink>->**  **-> Erweiterte Einstellungen.**

Weitere Einstellungen	
From Domain	
Anzahl der zulässigen gleichzeitigen Gespräche	Uneingeschränkt ▼
Standort	Alle Standorte ▼
Wahlendeüberwachungstimer	5 Sekunden
Halten im System	<input checked="" type="checkbox"/> Aktiviert
Anrufweilerschaltung extern (SIP 302)	<input type="checkbox"/>
Internationale Rufnummer erzeugen	<input checked="" type="checkbox"/> Aktiviert
Nationale Rufnummer erzeugen	<input checked="" type="checkbox"/> Aktiviert
Nummernunterdrückung deaktivieren	<input type="checkbox"/> <input type="checkbox"/> Anzeige <input type="checkbox"/> Benutzer <input type="checkbox"/> Domäne <input type="checkbox"/> Privacy Header <input type="checkbox"/> Privacy User <input checked="" type="checkbox"/> Privacy ID
SIP-Header-Feld: FROM Display	Keiner ▼
SIP-Header-Feld: FROM User	Benutzername ▼
SIP-Header-Feld: P-Preferred	Anruferadresse ▼
SIP-Header-Feld: P-Asserted	Keiner ▼

Abb. 92: VoIP->Einstellungen->SIP-Provider-> <toplink> -> Erweiterte Einstellungen

Gehen Sie folgendermaßen vor, um den SIP-Header zu erweitern:

- (1) Aktivieren Sie unter **SIP-Header-Feld: P-Preferred** die Option *Anruferadresse*.
- (2) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.



Hinweis

Wird der PBX-Assistent erneut für diesen Anschluss verwendet, werden alle Einstellungen im Menü **VoIP->Einstellungen->SIP-Provider** zurückgesetzt.

9.3.2 SIP-Provider (Durchwahl)

Voraussetzung

Im Folgenden wird die Einrichtung eines SIP-Providers bei Verwendung eines Durchwahl-Anschlusses beschrieben.

- (1) Gehen Sie zu **Assistenten->Telefonie->Anschlüsse->Neu**.
- (2) Wählen Sie unter **Verbindungstyp** *SIP-Durchwahl*.
- (3) Bei **Typ** wählen Sie *Benutzerdefiniert*.
- (4) Klicken Sie auf **Weiter**.

SIP-Provider-Einstellungen
?

Name	<input type="text" value="Sipgate_trunking"/>
Anschlussart	Durchwahl
Authentifizierungs-ID	<input type="text" value="152850710"/>
Passwort	<input type="password" value="*****"/>
Benutzername	<input type="text" value="152850710"/>
Registrar	<input type="text" value="sipconnect.sipgate.de"/>
Domäne	<input type="text"/>

Die Amtsleitung der Berechtigungsklasse zuweisen
?

Berechtigungsklasse	<input type="text" value="Uneingeschränkt"/> ▼ 🗑️
HINZUFÜGEN	

Rufnummern
?

Bestrufnummer	<input type="text" value="4991149522701"/>
---------------	--

Erweiterte Einstellungen

<div style="background-color: #4b2c2c; color: white; padding: 5px; margin-bottom: 5px;">Registrar ?</div> <div style="border: 1px solid #ccc; padding: 5px;"> Port Registrar 5060 </div> <div style="border: 1px solid #ccc; padding: 5px;"> Transportprotokoll <input checked="" type="radio"/> UDP <input type="radio"/> TCP <input type="radio"/> TLS </div>	<div style="background-color: #4b2c2c; color: white; padding: 5px; margin-bottom: 5px;">STUN-Server ?</div> <div style="border: 1px solid #ccc; padding: 5px;"> STUN-Server </div> <div style="border: 1px solid #ccc; padding: 5px;"> Port STUN-Server 3478 </div>				
<div style="background-color: #4b2c2c; color: white; padding: 5px; margin-bottom: 5px;">Durchwahlausnahme (P-P) ?</div> <div style="border: 1px solid #ccc; padding: 5px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Durchwahlausnahme (P-P)</td> <td style="width: 50%;">Angezeigter Name</td> </tr> <tr> <td style="border-bottom: 1px solid #ccc; text-align: center;">0</td> <td style="border-bottom: 1px solid #ccc; text-align: center;">Zentrale-0 🗑️</td> </tr> </table> </div> <div style="border: 1px solid #ccc; padding: 5px;"> HINZUFÜGEN <div style="border: 1px solid #ccc; height: 20px; margin-top: 5px;"></div> </div>	Durchwahlausnahme (P-P)	Angezeigter Name	0	Zentrale-0 🗑️	<div style="background-color: #4b2c2c; color: white; padding: 5px; margin-bottom: 5px;">Weitere Einstellungen ?</div> <div style="border: 1px solid #ccc; padding: 5px;"> Internationale Rufnummer erzeugen <input checked="" type="checkbox"/> Aktiviert </div> <div style="border: 1px solid #ccc; padding: 5px;"> Nationale Rufnummer erzeugen <input checked="" type="checkbox"/> Aktiviert </div> <div style="border: 1px solid #ccc; padding: 5px;"> SIP-Header-Feld: FROM Display Keiner ▼ </div> <div style="border: 1px solid #ccc; padding: 5px;"> SIP-Header-Feld: FROM User Benutzername ▼ </div> <div style="border: 1px solid #ccc; padding: 5px;"> SIP-Header-Feld: P-Preferred Keiner ▼ </div> <div style="border: 1px solid #ccc; padding: 5px;"> SIP-Header-Feld: P-Asserted Keiner ▼ </div>
Durchwahlausnahme (P-P)	Angezeigter Name				
0	Zentrale-0 🗑️				

Abb. 94: Assistenten->Telefonie->Anschlüsse->Neu-> <SIP-Provider (Durchwahl)>

Gehen Sie folgendermaßen vor, um die Anmeldedaten des SIP-Providers zu hinterlegen:




Hinweis

Bei einem Gateway mit eingerichteten VoIP PBX im LAN-Assistenten muss bei einigen SIP-Providern ein **STUN-Server** konfiguriert werden.

- (1) Geben Sie unter **Name** eine Bezeichnung für den SIP-Provider ein, z. B. *Sipgate-Trunking*.
- (2) Geben Sie die **Authentifizierungs-ID** (SIP-ID) Ihres Providers ein, z. B. *1528507t0*.
- (3) Geben Sie das **Passwort** ein, das Sie von Ihrem VoIP-Provider erhalten haben.
- (4) Geben Sie unter **Benutzername** den Namen ein, den Sie von Ihrem VoIP-Provider erhalten haben, z. B. *1528507t0*. Dieser entspricht bei den Providern Sipgate und QSC der SIP-ID.
- (5) Geben Sie als SIP **Registrar** eine IP-Adresse oder einen Domännennamen an.
 - Für Sipgate Trunking: *sipconnect.sipgate.de*
 - Für QSC-IPfonie extended: *sip.qsc.de*
- (6) Geben Sie eine **Basisrufnummer** ein, z. B. *4911149522701*.
- (7) Legen Sie unter **Berechtigungsklasse** mit **Hinzufügen** einen neuen Eintrag an und wählen Sie eine Berechtigungsklasse aus, z. B. *Uneingeschränkt*.
- (8) Legen Sie unter **Durchwahlausnahme (P-P)** mit **Hinzufügen** einen neuen Eintrag an.


Geben Sie unter **Durchwahlausnahme (P-P)** die Durchwahlrufnummer ein, die Sie von Ihrem VoIP-Provider erhalten haben, z. B. *0*.

Geben Sie unter **Angezeigter Name** eine Bezeichnung für den Anschluss ein, z. B. *Zentrale-0*. Diese wird für ankommende Anrufe am Systemtelefon angezeigt.

- (9) Aktivieren Sie **Internationale Rufnummer erzeugen** und **Nationale Rufnummer erzeugen**.
- (10) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.
Nach erfolgreicher Registrierung der Anlage beim SIP-Provider wechselt die Statusanzeige des jeweiligen SIP-Anschlusses auf .

9.3.2.1 Sipgate Trunking

Beim SIP-Provider Sipgate Trunking muss für den **SIP-Header-Feld: P-Preferred** die Option *Anruferadresse* aktiviert werden.

- (1) Gehen Sie zu **VoIP->Einstellungen->SIP-Provider-> <sipgate_trunking>** ->**Erweiterte Einstellungen**.

Weitere Einstellungen	
From Domain	
Anzahl der zulässigen gleichzeitigen Gespräche	Uneingeschränkt ▼
Standort	Alle Standorte ▼
Wahlendeüberwachungstimer	5 Sekunden
Halten im System	<input checked="" type="checkbox"/> Aktiviert
Anrufweilerschaltung extern (SIP 302)	<input type="checkbox"/>
Internationale Rufnummer erzeugen	<input checked="" type="checkbox"/> Aktiviert
Nationale Rufnummer erzeugen	<input checked="" type="checkbox"/> Aktiviert
Nummernunterdrückung deaktivieren	<input type="checkbox"/> <input type="checkbox"/> Anzeige <input type="checkbox"/> Benutzer <input type="checkbox"/> Domäne <input type="checkbox"/> Privacy Header <input type="checkbox"/> Privacy User <input checked="" type="checkbox"/> Privacy ID
SIP-Header-Feld: FROM Display	Keiner ▼
SIP-Header-Feld: FROM User	Benutzername ▼
SIP-Header-Feld: P-Preferred	Anruferadresse ▼
SIP-Header-Feld: P-Asserted	Keiner ▼

Abb. 95: VoIP->Einstellungen->SIP-Provider-> <sipgate_trunking> ↗->Erweiterte Einstellungen

Gehen Sie folgendermaßen vor, um den SIP-Header zu erweitern:

- (1) Aktivieren Sie unter **SIP-Header-Feld: P-Preferred** die Option *Anruferadresse*.
- (2) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.




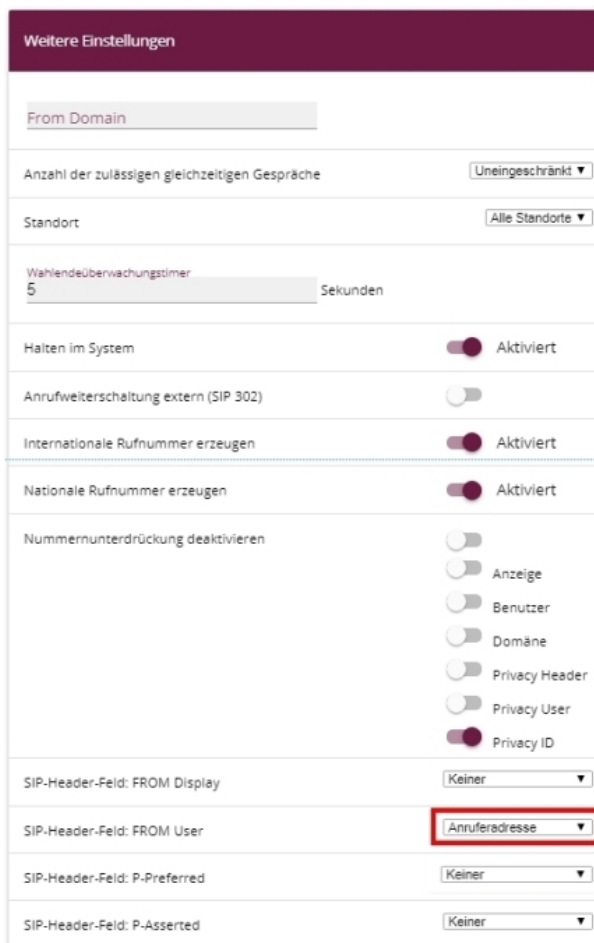
Hinweis

Wird der PBX-Assistent erneut für diesen Anschluss verwendet, werden alle Einstellungen im Menü **VoIP->Einstellungen->SIP-Provider** zurückgesetzt.


9.3.2.2 QSC-IPfonie extended

Beim SIP-Provider QSC-IPfonie extended muss für den unter **SIP-Header-Feld: FROM User** die Option *Anruferadresse* aktiviert werden.

- (1) Gehen Sie zu **VoIP->Einstellungen->SIP-Provider-> <qsc_ipfonie_extended>**  **->Erweiterte Einstellungen.**



Weitere Einstellungen	
From Domain	
Anzahl der zulässigen gleichzeitigen Gespräche	Uneingeschränkt ▼
Standort	Alle Standorte ▼
Wahlendeüberwachungstimer	5 Sekunden
Halten im System	<input checked="" type="checkbox"/> Aktiviert
Anrufweiterleitung extern (SIP 302)	<input type="checkbox"/>
Internationale Rufnummer erzeugen	<input checked="" type="checkbox"/> Aktiviert
Nationale Rufnummer erzeugen	<input checked="" type="checkbox"/> Aktiviert
Nummernunterdrückung deaktivieren	<input type="checkbox"/> <input type="checkbox"/> Anzeige <input type="checkbox"/> Benutzer <input type="checkbox"/> Domäne <input type="checkbox"/> Privacy Header <input type="checkbox"/> Privacy User <input checked="" type="checkbox"/> Privacy ID
SIP-Header-Feld: FROM Display	Keiner ▼
SIP-Header-Feld: FROM User	Anruferadresse ▼
SIP-Header-Feld: P-Preferred	Keiner ▼
SIP-Header-Feld: P-Asserted	Keiner ▼

Abb. 96: **VoIP->Einstellungen->SIP-Provider-> <qsc_ipfonie_extended>**  **->Erweiterte Einstellungen**

Gehen Sie folgendermaßen vor, um den SIP-Header zu erweitern:

- (1) Aktivieren Sie unter **SIP-Header-Feld: FROM User** die Option *Anruferadresse*.
- (2) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.



Hinweis

Wird der PBX-Assistent erneut für diesen Anschluss verwendet, werden alle Einstellungen im Menü **VoIP->Einstellungen->SIP-Provider** zurückgesetzt.

9.4 Variante 1 + 2: Konfiguration der Berechtigungs-klasse (Optional)

Für gehende Telefonate über einen SIP-Provider muss dem Benutzer eine passende Berechtigungsklasse zugeordnet sein.



Hinweis

Einen Benutzer legen Sie unter **Nummerierung->Benutzereinstellungen->Benutzer** an.

Sie können für den Benutzer dieselbe Berechtigungsklasse wie bei der Konfiguration des SIP-Providers verwenden, z. B. *Uneingeschränkt*.

Andernfalls müssen Sie die Berechtigungsklasse, die dem Benutzer zugeordnet ist, folgendermaßen anpassen.

- (1) Gehen Sie zu **Nummerierung->Benutzereinstellungen->Berechtigungsklassen-><Benutzerberechtigungsklasse>**  **->Grundeinstellungen**.

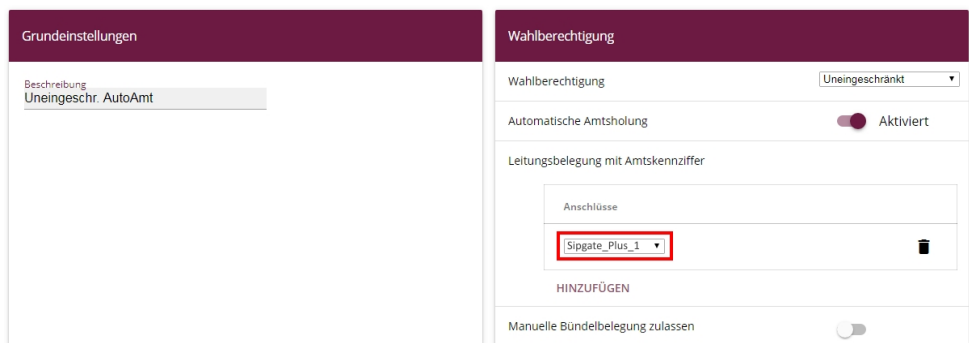


Abb. 97: **Nummerierung->Benutzereinstellungen->Berechtigungsklassen-><Benutzerberechtigungsklasse>**  **->Grundeinstellungen**

Gehen Sie folgendermaßen vor, um die Berechtigungsklasse anzupassen:

- (1) Legen Sie unter **Leitungsbelegung mit Amtskennziffer** mit **Hinzufügen** einen neuen Eintrag an und wählen Sie Ihren VoIP-Anschluss aus, z. B. *Sipgate_Plus_1*.
- (2) Bestätigen Sie mit **Übernehmen**.

9.5 Variante 1 + 2: Konfiguration der Rufnummern in der be.IP plus

9.5.1 Zuordnung der kommenden Anrufe

Im Folgenden legen Sie fest, welche internen Teilnehmer bzw. Teams über die externe Rufnummer des SIP-Providers erreicht werden.




Hinweis


Für den folgenden Schritt muss bereits ein Benutzer angelegt sein.

Einen Benutzer legen Sie unter **Nummerierung->Benutzereinstellungen->Benutzer** an. Ordnen Sie dem Benutzer eine entsprechende Berechtigungsklasse zu (siehe [Variante 1 + 2: Konfiguration der Berechtigungsklasse \(Optional\)](#) auf Seite 111).

Ein Telefon weisen Sie dem Benutzer im Menü **Endgeräte** zu.

- (1) Gehen Sie zu **Nummerierung->Rufverteilung->Anrufzuordnung-><49911148797640>** .

Grundeinstellungen	Einstellungen interne Rufnummer und Abwurf
Sipgate_1	49911148797640
Externer Anschluss	Sipgate_Plus_1
Zuordnung	Interne Nummer
	Interne Rufnummer: 30 (Mustermann-30)

Abb. 98: **Nummerierung->Rufverteilung->Anrufzuordnung-><49911148797640>** 

Gehen Sie folgendermaßen vor, um die externe einer internen Rufnummer zuzuordnen:

- (1) Wählen Sie unter **Zuordnung** *Interne Nummer*.
- (2) Wählen Sie unter **Interne Rufnummer** die interne Rufnummer des entsprechenden Benutzers aus, z. B. *30 (Mustermann-30)*.
- (3) Bestätigen Sie mit **OK**.
- (4) Wiederholen Sie den Vorgang für alle weiteren Rufnummern des SIP-Providers.

9.5.2 Konfiguration der gehenden Rufnummern

9.5.2.1 SIP-Provider (Einzelrufnummer) QSC-IPfonie basic und Toplink

Falls für einen SIP-Provider mehrere Rufnummern konfiguriert sind, kann für den Teilnehmer eingestellt werden, welche Rufnummer bei abgehenden Gesprächen mitgesendet wird.

- (1) Gehen Sie zu **Nummerierung->Benutzereinstellungen->Benutzer-><Mustermann-30>** ->**Gehende Rufnummer-><30>** .

Gehende Rufnummer				
Priorität	Externer Anschluss	Gehende Rufnummer	Nummer verbergen	
1	Toplink	00495171773052	<input type="checkbox"/>	↑↓

Abb. 99: **Nummerierung->Benutzereinstellungen->Benutzer-><Mustermann-30>** ->**Gehende Rufnummer -><30>** 

Gehen Sie folgendermaßen vor, um einer internen Rufnummer eine gehende Rufnummer zuzuordnen:

- (1) Wählen Sie unter der Bezeichnung des SIP-Providers, z. B. **Toplink**, eine Rufnummer, z. B. *00495171773052*, aus.
- (2) Bestätigen Sie mit **Übernehmen**.

9.5.2.2 SIP-Provider (Durchwahl) Sipgate Trunking und QSC-IPfonie extended

Standardmäßig wird bei einem abgehenden Gespräch die Basisrufnummer mit der Durchwahlrufnummer des Benutzers gesendet. Dies entspricht der Einstellung *Standard, eigene DDI-Signale*. Abgehende Gespräche des Anlagenteilnehmers können aber auch mit anderen konfigurierten Rufnummern des Rufnummernplans gesendet werden.

- (1) Gehen Sie zu **Nummerierung->Benutzereinstellungen->Benutzer-><Mustermann-30>** ->**Gehende Rufnummer -><30>** .

Gehende Rufnummer			
Priorität	Externer Anschluss	Gehende Rufnummer	Nummer verbergen
1	Sipgate_trunking	4991149522701-0	<input type="checkbox"/>

Abb. 100: Nummerierung->Benutzereinstellungen->Benutzer-> <Mustermann-30> ->Gehende Rufnummer -> <30>

Gehen Sie folgendermaßen vor, um die gehende Rufnummer auszuwählen:

- Wählen Sie unter der Bezeichnung des SIP-Providers, z. B. **Sipgate_trunking**, eine konfigurierte Rufnummer, z. B. *004991149522701-0*, aus, die dem anderen Gesprächsteilnehmer übermittelt wird.
Wenn Sie *Standard, eigene DDI-Signale* wählen, wird die Basisrufnummer mit der eigenen Durchwahlrufnummer übermittelt.
- Bestätigen Sie mit **Übernehmen**.

9.6 Konfigurationsschritte im Überblick

Variante 2: Konfiguration des Gateways (z. B. bintec RS353jw)

Feld	Menü	Wert
WAN-Schnittstelle für VoIP-Priorisierung	VoIP ->VoIP PBX im LAN ->Neu	Internet-PPPoE
Maximale Upload-Geschwindigkeit	VoIP ->VoIP PBX im LAN ->Neu ->Weiter	z. B. 2000 kbit/s
IP-Adresse der VoIP PBX im LAN	VoIP ->VoIP PBX im LAN ->Neu ->Weiter	z. B. 192.168.0.251
Port-SIP-Server	VoIP ->VoIP PBX im LAN ->Neu ->Weiter	5060

Variante 2: Konfiguration der be.IP plus

Feld	Menü	Wert
Standard-Gateway-IP-Adresse	Assistenten ->Erste Schritte-> Grundeinstellungen	z. B. 192.168.0.254
Feste DNS-Server-Adresse	Assistenten ->Erste Schritte-> Grundeinstellungen	Aktiviert

Feld	Menü	Wert
DNS-Server 1	Assistenten-> Erste Schritte -> Grundeinstellungen	z. B. 192.168.0.254

Variante 1 + 2: Konfiguration der Ländereinstellungen



Feld	Menü	Wert
Internationaler Präfix / Länderkennzahl	Systemverwaltung-> Globale Einstellungen-> System	z. B. 49
Nationaler Präfix/ Ortsnetzkennzahl	Systemverwaltung-> Globale Einstellungen-> System	z. B. 911

SIP-Provider (Einzelrufnummer)


Feld	Menü	Wert
Name	Assistenten ->Telefonie-> Anschlüsse-> Neu-> <SIP-Provider>	z. B. Sipgate_Plus_1
Authentifizierungs-ID	Assistenten-> Telefonie ->Anschlüsse ->Neu-> <SIP-Provider>	z. B. 1527861e0
Passwort	Assistenten ->Telefonie-> Anschlüsse-> Neu-> <SIP-Provider>	z. B. Supersecret
Benutzername	Assistenten-> Telefonie ->Anschlüsse ->Neu-> <SIP-Provider>	z. B. 1527861e0
Registrar	Assistenten ->Telefonie-> Anschlüsse-> Neu-> <SIP-Provider>	z. B. sipgate.de
Einzelrufnummer	Assistenten-> Telefonie ->Anschlüsse ->Neu-> <SIP-Provider>	z. B. 4911148797640
Angezeigter Name	Assistenten ->Telefonie-> Anschlüsse-> Neu-> <SIP-Provider>	z. B. Sipgate_1
Berechtigungsklasse	Assistenten-> Telefonie ->Anschlüsse ->Neu-> <SIP-Provider>	z. B. Uneingeschränkt
Internationale Rufnummer	Assistenten ->Telefonie->	Aktiviert

Feld	Menü	Wert
erzeugen	Anschlüsse-> Neu-> <SIP-Provider>	
Nationale Rufnummer erzeugen	Assistenten-> Telefonie ->Anschlüsse ->Neu-> <SIP-Provider>	Aktiviert


1&1

Feld	Menü	Wert
Ersetzen des Präfix der eingehenden Nummer	VoIP ->Einstellungen-> SIP-Provider-> <1und1> ->  -> Erweiterte Einstellungen	49
ersetzen durch	VoIP ->Einstellungen-> SIP-Provider-> <1und1> ->  -> Erweiterte Einstellungen	0

QSC-IPfonie basic

Feld	Menü	Wert
SIP-Header-Feld: FROM User	VoIP-> Einstellungen-> SIP-Provider-> <qsc_ipfonie_basic> ->  -> Erweiterte Einstellungen	Anruferadresse

Toplink


Feld	Menü	Wert
SIP-Header-Feld: P-Preferred	VoIP-> Einstellungen-> SIP-Provider-> <toplink> ->  -> Erweiterte Einstellungen	Anruferadresse

SIP-Provider (Durchwahl)

Feld	Menü	Wert
Name	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>Sipgate_Trunking</i>
Authentifizierungs-ID	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>1528507t0</i>

Feld	Menü	Wert
Passwort	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>Supersecret</i>
Benutzername	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>1528507t0</i>
Registrar	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>sip- connect.sipgate.de</i>
Basisrufnummer	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>4911149522701</i>
Berechtigungsklasse	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>Uneingeschränkt</i>
Durchwahlausnahme (P-P)	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>0</i>
Angezeigter Name	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	z. B. <i>Zentrale-0</i>
Internationale Rufnummer erzeugen	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	<i>Aktiviert</i>
Nationale Rufnummer erzeugen	Assistenten ->Telefonie ->Neu -> <SIP-Provider (Durchwahl)>	<i>Aktiviert</i>

Sipgate Trunking

Feld	Menü	Wert
SIP-Header-Feld: P-Preferred	VoIP-> Einstellungen ->SIP-Provider-> <sipgate_trunking> ->  - > Erweiterte Einstellungen	<i>Anruferadresse</i>

QSC-IPfonie extended

Feld	Menü	Wert
SIP-Header-Feld: FROM User	VoIP ->Einstellungen-> SIP-Provider->	<i>Anruferadresse</i>

Feld	Menü	Wert
	<qsc_ipfonie_extended> -> ✎ -> Erweiterte Einstellungen	

Variante 1 + 2: Konfiguration der Berechtigungsklasse (Optional)

Feld	Menü	Wert
Leitungsbelegung mit Amtskennziffer	Nummerierung ->Benutzer-einstellungen ->Berechtigungsklassen -> <Benutzerberechtigungsklasse> ✎ -> Grundeinstellungen	z. B. <i>Sipgate_Plus_1</i>

Zuordnung der kommenden Anrufe

Feld	Menü	Wert
Zuordnung	Nummerierung ->Rufverteilung ->Anrufzuordnung -> <49911148797640> -> ✎	<i>Interne Nummer</i>
Interne Rufnummer	Nummerierung ->Rufverteilung ->Anrufzuordnung -> <49911148797640> -> ✎	z. B. <i>30</i> <i>(Mustermann-30)</i>

Konfiguration der gehenden Rufnummern - SIP-Provider (Einzelrufnummer) QSC-IPfonie basic und Toplink

Feld	Menü	Wert
z. B. Toplink	Nummerierung ->Benutzer-einstellungen ->Benutzer-> <Mustermann-30> ✎ -> Gehende Rufnummer -> <30> ✎	z. B. <i>00495171773052</i>

Konfiguration der gehenden Rufnummern - SIP-Provider (Durchwahl) Sipgate Trunking und QSC-IPfonie extended

Feld	Menü	Wert
z. B. Sipgate_Trunking	Nummerierung ->Benutzer-einstellungen ->Benutzer-> <Mustermann-30> ✎ -> Gehende Rufnummer -> <30> ✎	z. B. <i>004991149522401-0</i>

Kapitel 10 bintec 4Ge-LE als WAN-Strecke an einer be.IP

10.1 Einleitung

Die **be.IP** startet nach der Anmeldung in der Ansicht **Schnellstart**.

Nach vollständigem Durchlaufen dieses Assistenten startet die **be.IP** in der Ansicht **Benutzer**. Um alle angeführten Menüpunkte zu erreichen, wechseln Sie in die Ansicht **Vollzugriff**.

Im Folgenden wird die Anbindung einer **bintec 4Ge-LE** als Backup-WAN-Strecke an einer **be.IP** beschrieben.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

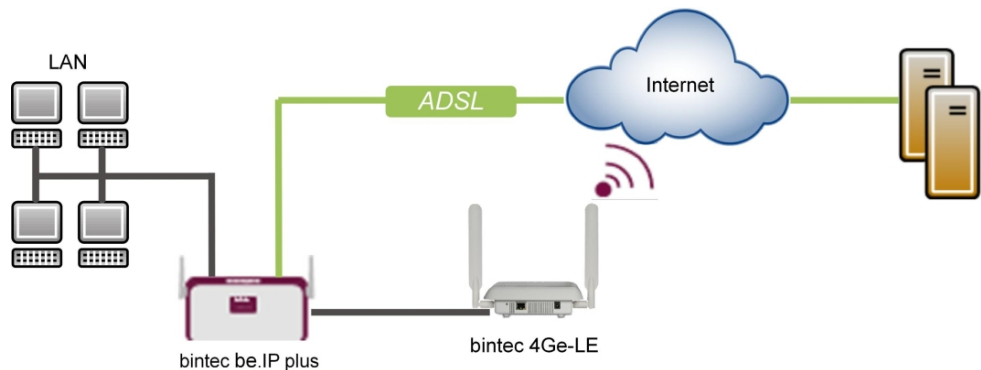


Abb. 101: Beispielszenario

Voraussetzungen

- Eine **bintec 4Ge-LE**
- Eine bintec **be.IP** oder eine **be.IP plus** mit aktueller Firmware. Die BOSS-Version Ihrer **be.IP** können Sie im Menü **Systemverwaltung** -> **Status** überprüfen.
- Eine bestehende Konfiguration wie sie von einem durchlaufenen **Schnellstartassistenten** angelegt wird.

10.2 Konfiguration

Anschluss der bintec 4Ge-LE

Die **bintec 4Ge-LE** läuft grundsätzlich als DHCP-Client und bekommt vom Gateway den Namen sowie die PIN für die SIM-Karte mittels der Option 43 (Vendor specific) übermittelt. Mit diesen Daten stellt das Gerät eine LTE (UMTS/GPRS)-Verbindung her und stellt die empfangene IP-Adresse, das Gateway und die DNS-Server seinerseits als DHCP-Server auf einer mit VLAN 463 getaggten Ethernet-Verbindung der **be.IP** zur Verfügung. Das führt dazu, dass die **be.IP** an der eigentlichen Schnittstelle DHCP-Server ist, an einem darauf aufsetzenden virtuellen Port mit VLAN 463 dagegen DHCP-Client!

Im Beispiel wird hierfür en1-4 (der blaue DMZ/WAN Port) verwendet, es kann aber auch auf jedem abgetrennten Port analog konfiguriert werden.

Im ersten Schritt werden nun die Schnittstellen angepasst/erstellt.

- (1) Gehen Sie in das Menü **LAN->IP-Konfiguration->Schnittstellen-> en1-4** .



Basisparameter	
Schnittstellenmodus	<input checked="" type="radio"/> Untagged <input type="radio"/> Tagged (VLAN)
MAC-Adresse	00:09:4f:6f:5e:80 <input type="checkbox"/> Voreingestellte verwenden

Grundlegende IPv4-Parameter	
Sicherheitsrichtlinie	<input type="radio"/> Nicht Vertrauenswürdig <input checked="" type="radio"/> Vertrauenswürdig
Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> DHCP
IP-Adresse / Netzmaske	
IP-Adresse	Netzmaske
192.168.43.41	255.255.255.252 
HINZUFÜGEN	

Abb. 102: **LAN->IP-Konfiguration->Schnittstellen-> en1-4** 

Gehen Sie folgendermaßen vor:

- (2) Belassen Sie den **Schnittstellenmodus** auf *Untagged*. Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet.
- (3) Die **Sicherheitsrichtlinie** belassen Sie auf *Vertrauenswürdig*. Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.
- (4) Geben Sie die **IP-Adresse / Netzmaske** der virtuellen Schnittstelle ein, hier z. B. *192.168.43.41* und *255.255.255.252*.
- (5) Bestätigen Sie Ihre Angaben mit **OK**.
Im nächsten Schritt erstellen Sie eine neue Schnittstelle.

- (1) Gehen Sie zu **LAN->IP-Konfiguration->Schnittstellen ->Neu**.

Basisparameter	Grundlegende IPv4-Parameter
Basierend auf Ethernet-Schnittstelle en1-4	Sicherheitsrichtlinie <input checked="" type="radio"/> Nicht Vertrauenswürdig <input type="radio"/> Vertrauenswürdig
Schnittstellenmodus <input type="radio"/> Untagged <input checked="" type="radio"/> Tagged (VLAN)	Adressmodus <input type="radio"/> Statisch <input checked="" type="radio"/> DHCP
VLAN-ID 463	DHCP-Metrik 5
MAC-Adresse 00:a0:f9 <input type="checkbox"/> Voreingestellte verwenden	IP-Adresse / Netzmaske <div style="display: flex; justify-content: space-between; border: 1px solid #ccc; padding: 2px;"> <input style="width: 40%; border: none;" type="text"/> <input style="width: 40%; border: none;" type="text"/> </div> <div style="text-align: center; font-size: small; margin-top: 2px;">HINZUFÜGEN</div>

Abb. 103: LAN->IP-Konfiguration->Schnittstellen ->Neu

Gehen Sie folgendermaßen vor:

- (2) Bei **Basierend auf Ethernet-Schnittstelle** wählen Sie die virtuelle Schnittstelle *en1-4* aus.
- (3) Den **Schnittstellenmodus** stellen Sie auf *Tagged (VLAN)*.
- (4) Weisen Sie die Schnittstelle einen VLAN zu. Geben Sie dazu die **VLAN-ID 463** ein.
- (5) Wählen Sie bei **Sicherheitsrichtlinie** *Nicht Vertrauenswürdig* aus.
- (6) Wählen Sie den **Adressmodus** *DHCP* aus. Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
- (7) Geben Sie bei **DHCP-Metrik** die Priorität der Route ein, in unserem Beispiel die 5.
- (8) Bestätigen Sie Ihre Angaben mit **OK**.

Die Netzwerkmaste für en1-4 wurde bewusst mit /30 gewählt, da nur ein IP-Bereich von 2 Adressen benötigt wird:

- **be.IP** (192.168.43.41)

- **bintec 4Ge-LE** (192.168.43.42)

Netzwerkadresse ist damit die 192.168.43.40, Broadcastadresse 192.168.43.43.

Die fertige Konfiguration sieht nun folgendermaßen aus:

Ethernet-/VLAN-Ports					
Schnittstelle	IPv4-Adresse/Netzmaske	IPv6-Adresse/Länge	Status	Aktion	
en1-4	192.168.43.41/255.255.255.252	-	✓	↑ ↓	✎ 🔍
efm35-60	Nicht konfiguriert/Nicht konfiguriert	-	✗	↑ ↓	✎ 🔍
ethoa35-5	Nicht konfiguriert/Nicht konfiguriert	-	✗	↑ ↓	✎ 🔍
br0	192.168.0.251/255.255.255.0	Präfix: Germany - Telekom Entertain:0 Host: eui64	✓	↑ ↓	✎ 🔍
ethoa35-5-1(VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✗	↑ ↓	🗑️ ✎ 🔍
efm35-60-1(VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✗	↑ ↓	🗑️ ✎ 🔍
en1-4-1(VLAN-ID463)	0.0.0/255.255.255.255 (DHCP)	-	✓	↑ ↓	🗑️ ✎ 🔍

Abb. 104: LAN->IP-Konfiguration->Schnittstellen

Nun muss für die virtuelle Schnittstelle `en1-4-1` als IPv4-WAN-Schnittstelle **NAT** aktiviert werden.

- (1) Gehen Sie zu **Netzwerk->NAT->NAT-Schnittstellen** .

NAT-Schnittstellen					
Schnittstelle	NAT aktiv	Loopback aktiv	Verwerfen ohne Rückmeldung	PPTP-Passthrough	Portweiterleitungen
BRIDGE_BR0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
efm35-60	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-4-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
WAN_EFM35-60-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
WAN_ETHOA35-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
WAN_ETHOA35-5-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
WAN_GERMANY - TELEKOM ENTERTAIN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0

Abb. 105: Netzwerk->NAT->NAT-Schnittstellen

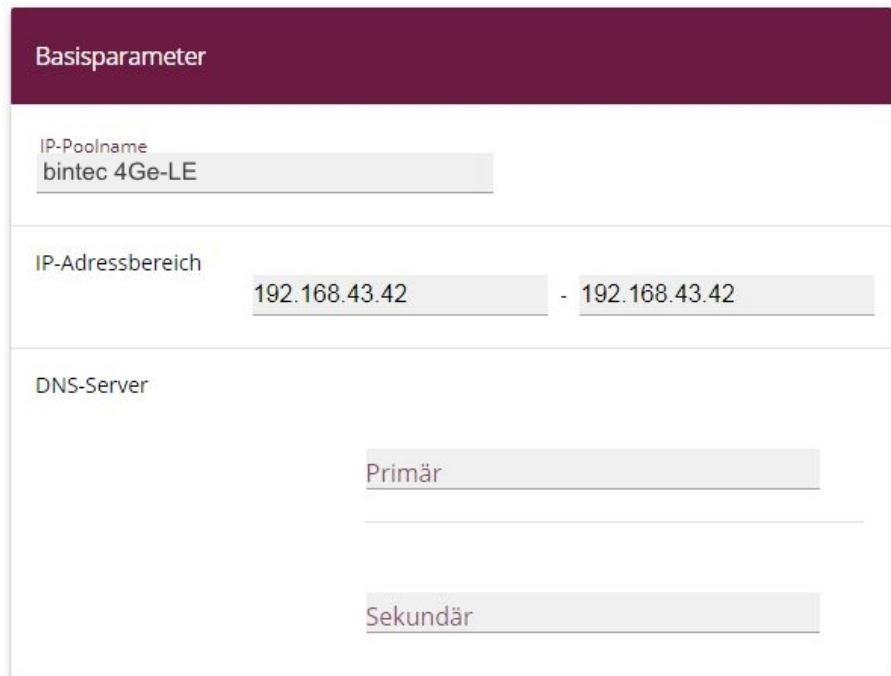
- (2) Aktivieren Sie für die **Schnittstelle** `LAN_EN1-4-1` die Optionen *NAT aktiv* und *Verwerfen ohne Rückmeldung*.
- (3) Bestätigen Sie Ihre Angaben mit **OK**.

Letzter Konfigurationsschritt ist nun die Einrichtung des DHCP-Servers mit der entspre-

chenden DHCP-Option 43 an der Schnittstelle *en1-4*. Aus Sicherheitsgründen wird eine statische Bindung der IP-Adresse an die MAC-Adresse des **bintec 4Ge-LE** vorgenommen, so dass nur dieser hier eine IP-Adresse vermittelt bekommt (und damit auch nur ihm die Option 43 mit der enthaltenen PIN übermittelt wird).

Um das Gerät als DHCP-Server zu aktivieren, muss erst der IP-Adress-Pool definiert werden.

- (1) Gehen Sie dazu in das Menü **Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration ->Neu**.



The screenshot shows a configuration window titled "Basisparameter" for a new IP pool. It contains three main sections:

- IP-Poolname:** A text field containing "bintec 4Ge-LE".
- IP-Adressbereich:** Two text fields containing "192.168.43.42" and "192.168.43.42", separated by a hyphen.
- DNS-Server:** Two text fields labeled "Primär" and "Sekundär", both currently empty.

Abb. 106: **Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration ->Neu**

- (2) Geben Sie bei **IP-Poolname** eine beliebige Beschreibung ein, hier z. B. *bintec 4Ge-LE* .
- (3) Geben Sie im **IP-Adressbereich** die IP-Adresse des IP-Adress-Pools ein, hier *192.168.43.42 - 192.168.43.42* .
- (4) Bestätigen Sie mit **OK**.

Im Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration ->Neu** können Sie jetzt den DHCP-Pool einrichten.

Basisparameter	
Schnittstelle	en1-4
IP-Poolname	bintec 4Ge-LE
Pool-Verwendung	Lokal
description	

Erweiterte Einstellungen:

Erweiterte Einstellung	
Gateway	Router als Gateway verwenden
Lease Time	120 Minuten
DHCP-Optionen	
Option	Wert
HINZUFÜGEN	
Herstellerspezifische Informationen (DHCP-Option 43)	
Hersteller-ID	Herstellerspezifische Informationen
HERSTELLER-STRING HINZUFÜGEN	HERSTELLERGRUPPE HINZUFÜGEN

Abb. 107: Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie die **Schnittstelle** *en1-4* aus.
- (2) Wählen Sie bei **IP-Poolname** den konfigurierten IP-Poolnamen *bintec 4Ge-LE* aus.
- (3) Klicken Sie auf **Erweiterte Einstellungen**.
- (4) Klicken Sie im Feld **Herstellerspezifische Informationen (DHCP-Option 43)** auf die Schaltfläche **Hersteller-String hinzufügen**.

Basisparameter

Hersteller auswählen - bintec - ▼

APN internet telekom

PIN 1234

Abb. 108: **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu->Erweiterte Einstellungen**

- (5) Unter **Hersteller auswählen** wählen Sie *-bintec-* aus.
- (6) Geben Sie den **APN** (Access Point Namen) des Providers Ihrer SIM-Karte ein, hier z. B. *internet.telekom*.
- (7) Geben Sie die **PIN** der SIM-Karte ein, z. B. *1234*.
- (8) Klicken Sie auf **Übernehmen**.

Im letzten Schritt wird nun die statische Bindung der IP-Adresse an die MAC-Adresse des Gerätes vorgenommen.

- (1) Gehen Sie in das Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung**.

IP/MAC-Bindung:

IP-Adresse	Beschreibung	MAC-Adresse	Verbleibende Lease Time	Statische Bindung
192.168.43.42				<input checked="" type="checkbox"/> Aktiviert

Abb. 109: **Lokale Dienste->DHCP-Server->IP/MAC-Bindung**




- (2) Aktivieren Sie die Option **Statische Bindung**.
- (3) Bestätigen Sie Ihre Angabe mit **OK**.

Mit dieser Konfiguration bekommt jetzt nur noch der **bintec 4Ge-LE** auf der Schnittstelle *en1-4* eine IP-Adresse mit der in der Option 43 enthaltenen PIN der SIM-Karte angeboten.

Die Konfiguration ist hiermit abgeschlossen. Sichern Sie die aktuelle Konfiguration mit der Schaltfläche **Konfiguration speichern**.

10.3 Konfigurationsschritte im Überblick

Anpassen der Schnittstelle

Feld	Menü	Wert
Schnittstellenmodus	LAN ->IP-Konfiguration ->Schnittstellen -> en1-4 	Untagged
Sicherheitsrichtlinie	LAN ->IP-Konfiguration ->Schnittstellen -> en1-4 	Vertrauenswürdig
IP-Adresse / Netzmaske	LAN ->IP-Konfiguration ->Schnittstellen -> en1-4 	z. B. 192.168.43.41 / 255.255.255.252

Neue Schnittstelle konfigurieren

Feld	Menü	Wert
Basierend auf Ethernet-Schnittstelle	LAN ->IP-Konfiguration ->Schnittstellen ->Neu	en1-4
Schnittstellenmodus	LAN ->IP-Konfiguration ->Schnittstellen ->Neu	Tagged (VLAN)
VLAN-ID	LAN ->IP-Konfiguration ->Schnittstellen ->Neu	463
Sicherheitsrichtlinie	LAN ->IP-Konfiguration ->Schnittstellen ->Neu	Nicht Vertrauenswürdig
Adressmodus	LAN ->IP-Konfiguration ->Schnittstellen ->Neu	DHCP
DHCP-Metrik	LAN ->IP-Konfiguration ->Schnittstellen ->Neu	z. B. 5

NAT aktivieren

Feld	Menü	Wert
NAT aktiv	Netzwerk-> NAT ->NAT-Schnittstellen	Aktiviert
Verwerfen ohne Rückmeldung	Netzwerk ->NAT-> NAT-Schnittstellen	Aktiviert

IP-Pool konfigurieren

Feld	Menü	Wert
IP-Poolname	Lokale Dienste ->DHCP-Server ->IP-Pool-Konfiguration ->Neu	z. B. bintec 4Ge-LE

Feld	Menü	Wert
IP-Adressbereich	Lokale Dienste ->DHCP-Server ->IP-Pool-Konfiguration ->Neu	z. B. 192.168.43.42 - 192.168.43.42

DHCP-Konfiguration

Feld	Menü	Wert
Schnittstelle	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu	en1-4
IP-Poolname	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu	bintec 4Ge-LE
Herstellerspezifische Informationen (DHCP-Option 43)	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu ->Erweiterte Einstellungen	Hersteller-String hinzufügen
Hersteller auswählen	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu ->Erweiterte Einstellungen ->Hersteller-String hinzufügen	-bintec-
APN	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu ->Erweiterte Einstellungen ->Hersteller-String hinzufügen	z. B. inter- net.telekom
PIN	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu ->Erweiterte Einstellungen ->Hersteller-String hinzufügen	z. B. 1234

IP/MAC-Bindung

Feld	Menü	Wert
Statische Bindung	Lokale Dienste ->DHCP-Server ->IP/MAC-Bindung	Aktiviert

Kapitel 11 Zwei gekoppelte be.IP 4isdn an einem Telekom VoIP Durchwahl-Anschluss

11.1 Einleitung

Damit Sie Ihre vorhandene ISDN-TK-Anlage an einem Voice-over-IP-Anschluss weiterverwenden können, benötigen Sie ein Media Gateway. Mit zwei gekoppelten **be.IP 4isdn** Media Gateways (sogenanntes Double Play) können Sie eine ISDN-TK-Anlage mit bis zu acht ISDN-Amtszugängen an einem Voice-over-IP DDI-Anschluss (Direct Dial In, Durchwahl) der Deutschen Telekom betreiben.

Eines der beiden Media Gateways wird als Master eingesetzt, das andere als Slave.

Der Master terminiert den Internetanschluss, verwaltet die SIP-Konten des Providers und dient für den Slave als Internet-Standard-Gateway.

Der Slave befindet sich im lokalen Netzwerk des Masters. Er dient im vorliegenden Szenario als nachgeschaltetes Media Gateway, das die Gesamtzahl der verwendbaren ISDN Ports auf bis zu acht erhöht.

Aufgrund der Arbeitsteilung der beiden Geräte unterscheiden sie sich auch in ihrer Konfiguration.

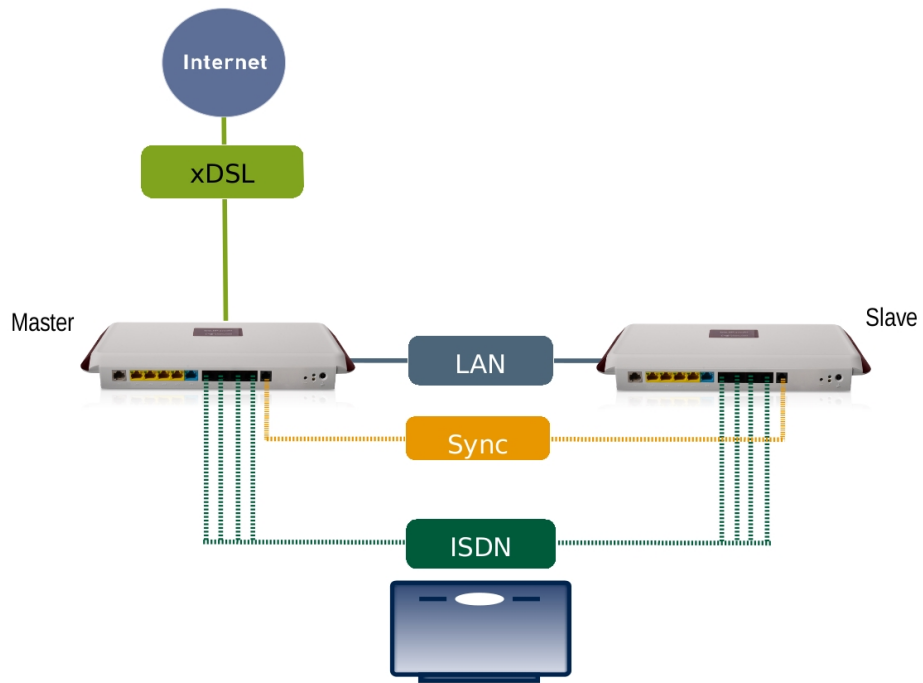


Abb. 110: Beispielszenario

Voraussetzungen

- Zwei **be.IP 4isdn** Geräte Im Media-Gateway-Modus, verbunden durch ein Synchronisationskabel zur Takt-Synchronisation der ISDN-Ports beider Geräte; (Das ISDN-Sync-Kabel kann als Zubehör erworben werden.)
- Systemsoftware-Version 10.1. Rev. 27 Patch 6 oder höher.

11.2 Konfiguration

- (1) Verbinden Sie das Gerät **be.IP 4isdn**, das als Slave dienen soll, mit Ihrem LAN.
- (2) Öffnen Sie einen Browser, geben Sie `192.168.0.251` in die Adresszeile des Browsers ein und bestätigen Sie mit der Eingabetaste.
- (3) Geben Sie **Benutzername** sowie **Kennwort** ein und klicken Sie auf **Anmelden**.

11.2.1 SYNC-Anschluss Einstellungen

Zum störungsfreien Betrieb der TK-Anlage an den ISDN Ports der beiden gekoppelten be.IP4isdn müssen die beiden be.IP4isdn taktsynchron laufen. Hierzu verbinden Sie bitte die beiden be.IP4isdn über die SYNC-Schnittstelle miteinander und konfigurieren beide Geräte gemäß Ihrer zugeordneten Rolle (Standard bzw. Slave).

Zur Konfiguration der Taktsynchronisierung der be.IP4isdn Standard, gehen Sie in das Menü **Physikalische Schnittstellen ->ISDN-Ports->ISDN-Konfiguration**.

Aktivieren Sie unter **SYNC-Anschluss Modus** die Option *Standard*.

The screenshot shows two sections of a web interface. The top section is titled "SYNC-Anschluss Einstellungen" and contains the "SYNC-Anschluss Modus" settings. Below this is a table titled "ISDN-Konfiguration" with columns for "Port" and "ISDN-Switch-Typ".

SYNC-Anschluss Modus
Der SYNC-Anschluss erlaubt den Anschluss einer zweiten be.IP 4isdn mit Hilfe eines SYNC-Kabels.
Im "Standard"-Modus arbeitet das Gerät als Taktgeber für ein Gerät im "Slave"-Modus. Stellen Sie sicher, dass Sie ein Gerät als "Standard" und eins als "Slave" konfigurieren. Standard Slave
Achtung: Für die Auswahl von "Slave" müssen alle ISDN-Ports auf "intern" geschaltet sein.

Port	ISDN-Switch-Typ	
bri-0 (NT)	Dialup (Euro-ISDN),Punkt-zu-Punkt	
bri-1 (NT)	Dialup (Euro-ISDN),Punkt-zu-Punkt	
bri-2 (NT)	Dialup (Euro-ISDN),Punkt-zu-Punkt	
bri-3 (NT)	Dialup (Euro-ISDN),Punkt-zu-Punkt	

Abb. 111: **Physikalische Schnittstellen ->ISDN-Ports->ISDN-Konfiguration**

Zur Konfiguration der Taktsynchronisierung der be.IP4isdn Slave, gehen Sie in das Menü **Physikalische Schnittstellen ->ISDN-Ports->ISDN-Konfiguration**.

Aktivieren Sie unter **SYNC-Anschluss Modus** die Option *Slave*.

SYNC-Anschluss Einstellungen

SYNC-Anschluss Modus

Der SYNC-Anschluss erlaubt den Anschluss einer zweiten be.IP 4isdn mit Hilfe eines SYNC-Kabels.
Im "Standard"-Modus arbeitet das Gerät als Taktgeber für ein Gerät im "Slave"-Modus. Stellen Sie sicher, dass Sie ein Gerät als "Standard" und eins als "Slave" konfigurieren.

Standard Slave

Achtung: Für die Auswahl von "Slave" müssen alle ISDN-Ports auf "Intern" geschaltet sein.

ISDN-Konfiguration





Port	ISDN-Switch-Typ	
bri-0 (NT)	Dialup (Euro-ISDN),Punkt-zu-Punkt	
bri-1 (NT)	Dialup (Euro-ISDN),Punkt-zu-Punkt	
bri-2 (NT)	Dialup (Euro-ISDN),Punkt-zu-Punkt	
bri-3 (NT)	Dialup (Euro-ISDN),Punkt-zu-Punkt	

Abb. 112: **Physikalische Schnittstellen ->ISDN-Ports->ISDN-Konfiguration**

11.2.2 be.IP 4isdn Slave konfigurieren (Teil 1)

IP-Adresse ändern

Um einen Adresskonflikt mit dem Master (der später konfiguriert wird) zu vermeiden, wird die IP-Adresse des Slaves geändert.

- (1) Gehen Sie in das Menü **Assistenten->Erste Schritte->Grundeinstellungen**.

Wählen Sie den physikalischen Ethernet Port für die LAN-Verbindung aus:

Physikalischer Ethernet-Port (LAN)

Geben Sie die IPv4-LAN-Konfiguration ein:

Logische Ethernet-/Bridge-Schnittstelle

Adressmodus Statisch DHCP-Client

IP-Adresse

Netzmaske

Standard-Gateway-IP-Adresse

Feste DNS-Server-Adresse Aktiviert

DNS-Server 1

DNS-Server 2

⚠️ Warnung! Konfigurationsverbindung geht möglicherweise beim Ändern der IP-Adresse verloren! Klicken Sie auf "OK", und melden Sie sich erneut an, um fortzufahren!

Wird dieses Gerät als DHCPv4-Server verwendet?

Dieses Gerät als DHCPv4-Server verwenden

IPv6-Konfiguration eingeben

IPv6

Abb. 113: Slave Konfiguration - IPv4-LAN-Konfiguration

- (2) Ändern Sie die **IP-Adresse** auf den Wert `192.168.0.252`.
- (3) Geben Sie unter **Standard-Gateway-IP-Adresse** die IP-Adresse des Masters ein, nämlich `192.168.0.251`.
- (4) Geben Sie unter **DNS-Server 1** ebenfalls die IP-Adresse des Masters ein, `192.168.0.251`.
- (5) Deaktivieren Sie die Option **Dieses Gerät als DHCPv4-Server verwenden**.
- (6) Klicken Sie auf **Erweiterte Einstellungen**.

Erweiterte Einstellungen

<p>Geben Sie die Einstellungen der Systemzeit ein: ?</p> <p>Manuelle Zeiteinstellung <input type="checkbox"/></p> <p>Systemzeit über Zeitserver aktualisieren <input checked="" type="checkbox"/> Aktiviert</p> <p>Primärer NTP-Zeitserver <input type="text" value="192.168.0.251"/></p> <p>Sekundärer NTP-Zeitserver <input type="text"/></p>	<p>Wählen Sie eine Zeitzone aus: ?</p> <p>Zeitzone <input type="text" value="Europe/Berlin"/></p>
<p>Wird das Gateway als Zeitserver für LAN-Clients verwendet? ?</p> <p>System als Zeitserver <input checked="" type="checkbox"/> Aktiviert</p>	<p>Möchten Sie sich zu dem Gateway über SSH verbinden? ?</p> <p>SSH-Dienst aktiv <input checked="" type="checkbox"/> Aktiviert</p>

Abb. 114: Slave Konfiguration - Systemzeit

- (7) Aktivieren Sie **Systemzeit über Zeitserver aktualisieren**.
- (8) Geben Sie unter **Primärer NTP-Zeitserver** die IP-Adresse des Masters ein, nämlich `192.168.0.251`.



Hinweis

Wenn Sie den Assistenten **Erste Schritte** mit **OK** verlassen, verlieren Sie die Verbindung zum Graphical User Interface (GUI) des Slaves, da sich die IP-Adresse des Geräts geändert hat. Sie müssen sich bei Bedarf mit der neuen IP-Adresse auf dem Gerät einloggen.

- (9) Bestätigen Sie Ihre Eingaben mit **OK**.

11.2.3 be.IP 4isdn Master konfigurieren

Als Nächstes wird der Master in Betrieb genommen und mit dem **Assistenten Ersteinrichtung Telekom** eine Grundkonfiguration des Geräts durchgeführt, sodass die Internetwahl funktionsfähig ist und das Gerät bereit ist, sich beim Provider anzumelden.

- (1) Verbinden Sie das Gerät **be.IP 4isdn**, das als Master dienen soll, mit Ihrem LAN.
- (2) Öffnen Sie einen Browser, geben Sie `192.168.0.251` in die Adresszeile ein und bestätigen Sie mit der Eingabetaste.
- (3) Geben Sie **Benutzername** sowie **Kennwort** ein und klicken Sie auf **Anmelden**.

- (4) Wählen Sie **Ansicht** *Vollzugriff*.

Grundkonfiguration

Mit Hilfe des **Assistenten Ersteinrichtung Telekom** wird eine Grundkonfiguration des Geräts vorgenommen.

- (1) Gehen Sie in das Menü **Assistenten->Ersteinrichtung Telekom** und durchlaufen Sie den Assistenten vollständig. Falls Sie Hilfe benötigen, steht Ihnen eine Hilfe zu jedem Schritt und zusätzlich die Online-Hilfe zur Verfügung.
- (2) Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

DDI Account anlegen

Als Nächstes wird mit dem **Assistenten Telefonie** einen DDI Account angelegt.

- (1) Gehen Sie in das Menü **Assistenten->Telefonie->Erste Schritte**.
- (2) Geben Sie die **Ortsnetzkenzahl** ein, z. B. *911* für Nürnberg.
- (3) Wählen Sie unter **ISDN-Port-Konfiguration** für alle ISDN-Ports *Punkt-zu-Punkt (Anlagenanschluss)*.
- (4) Bestätigen Sie Ihre Einstellungen mit **OK**.
- (5) Gehen Sie in das Menü **Assistenten->Telefonie->SIP-Provider->Neu**.
- (6) Wählen Sie **Verbindungstyp** *SIP-Durchwahl*, belassen Sie die Einstellung **Typ** *DeutschlandLAN* und klicken Sie auf **Weiter**.
- (7) Geben Sie eine **Beschreibung** ein, z. B. *+49911xxxxxx*.
- (8)



Hinweis

Geben Sie unter **Telefonie-Benutzername**, **Telefonie-Passwort** und **Registrierungsrufnummer** die Informationen ein, die Sie von Ihrem Internet Service Provider (ISP) erhalten haben.

Geben Sie den **Telefonie-Benutzernamen** ein, z. B. *471187654321*.

- (9) Geben Sie das **Telefonie-Passwort** ein, z. B. *Scrt2E4E*.
- (10) Geben Sie die **Registrierungsrufnummer** ein, z. B. *+499119876*.
- (11) Aktivieren Sie alle **ISDN-Ports**.
- (12) Geben Sie die **Durchwahlnummer**, die Sie von der Telekom erhalten haben, für die Verbindung ein, z. B. *123456*.
- (13) Bestätigen Sie Ihre Einstellungen mit **OK**.

SIP Server Account anlegen

Als Nächstes wird auf dem Master ein SIP Account angelegt, an dem sich später der Client registrieren kann.


- (1) Gehen Sie in das Menü **VoIP->Einstellungen->SIP-Konten->Neu**,

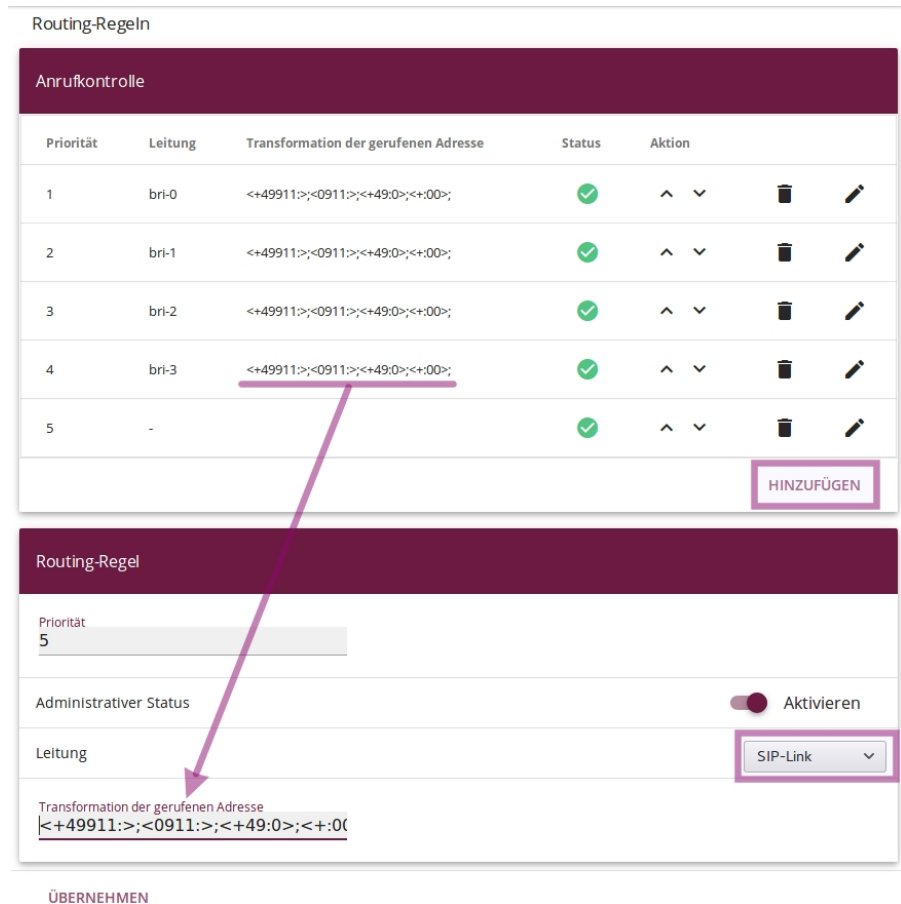
Abb. 115: SIP Account (Server)

- (2) Geben Sie eine **Beschreibung** ein, z. B. *SIP-Link*.
- (3) Wählen Sie **Trunk-Modus** *Server*.
- (4) Geben Sie einen **Benutzernamen** ein, z. B. *be.ip_4isdn*.
- (5) Geben Sie eine **Authentifizierungs-ID** ein, z. B. *be.ip_4isdn*.
- (6) Geben Sie ein **Passwort** ein, z. B. *beIP4secret*.
- (7) Bestätigen Sie Ihre Einstellungen mit **OK**.

Eingehende Rufe routen











Um eingehende Rufe auf den Slave zu routen, wenn alle ISDN-Ports des Masters belegt sind, wird die entsprechende Route editiert.

- (1) Gehen Sie in das Menü **VoIP->Media Gateway->Anrufkontrolle** und klicken Sie in der Zeile **<+49911xxxxx->bri>** auf das Symbol , um den Eintrag zu bearbeiten.
- (2) Klicken Sie auf **Hinzufügen**.



Routing-Regeln

Anrufkontrolle

Priorität	Leitung	Transformation der gerufenen Adresse	Status	Aktion
1	bri-0	<+49911:>;<0911:>;<+49:0>;<+:00>;	✓	^ v  
2	bri-1	<+49911:>;<0911:>;<+49:0>;<+:00>;	✓	^ v  
3	bri-2	<+49911:>;<0911:>;<+49:0>;<+:00>;	✓	^ v  
4	bri-3	<+49911:>;<0911:>;<+49:0>;<+:00>;	✓	^ v  
5	-		✓	^ v  

HINZUFÜGEN

Routing-Regel

Priorität
5

Administrativer Status Aktivieren

Leitung SIP-Link

Transformation der gerufenen Adresse
<+49911:>;<0911:>;<+49:0>;<+:00>;

ÜBERNEHMEN


Abb. 116: Call Route editieren

- (3) Aktivieren Sie **Administrativer Status**.
- (4) Wählen Sie unter **Leitung** *SIP-Link*.
- (5) Kopieren Sie im Abschnitt **Anrufkontrolle** den Wert unter **Transformation der gerufenen Adresse** `<+49911:>;<0911:>;<+49:0>;<+:00>;` und fügen Sie diesen Wert unter **Routing-Regel** in das Feld **Transformation der gerufenen Adresse** ein.
- (6) Klicken Sie auf **Übernehmen** und auf **OK**.

ISDN-TK-Anlage mit CLIP no screening (optional)

Wenn Sie eine TK-Anlage mit CLIP no screening verwenden, ist ein zusätzlicher Konfigura-

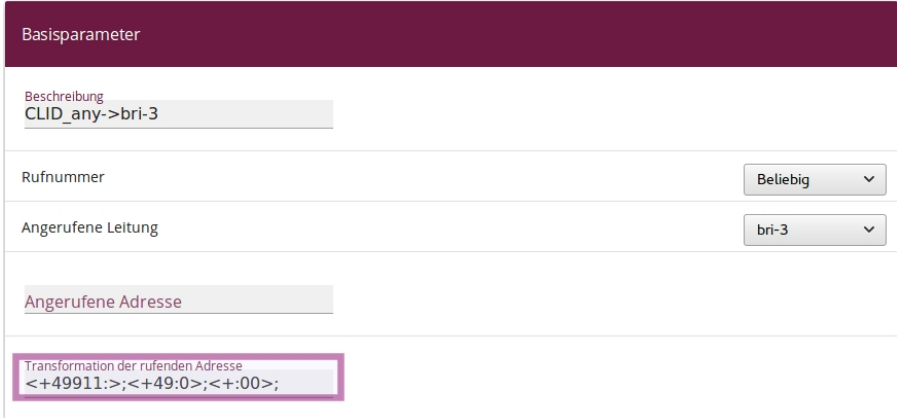
tionsschritt notwendig.

- (1) Gehen Sie in das Menü **VoIP->Media Gateway->Anrufkontrolle** und klicken Sie in der Zeile **<any->+49911xxxxxx>** auf das Symbol , um den Eintrag zu bearbeiten.
- (2) Löschen Sie den Eintrag unter **Anrufende Adresse**.
- (3) Bestätigen Sie die Einstellung mit **OK**.

Rufnummer umwandeln

Im nächsten Schritt wird die Rufnummer eines Anrufers ISDN-konform umgewandelt.

- (1) Gehen Sie in das Menü **VoIP->Media Gateway->CLID-Umwandlung** und öffnen Sie einen Eintrag, der in der **Beschreibung** *bri* enthält, z. B. *CLID_any->bri-3*.



Basisparameter	
Beschreibung	CLID_any->bri-3
Rufnummer	Beliebig
Angerufene Leitung	bri-3
Angerufene Adresse	
Transformation der rufenden Adresse	<+49911:>;<+49:0>;<+:00>;

Abb. 117: CLID- Umwandlung - Wert kopieren

- (2) Kopieren Sie den Wert unter **Transformation der rufenden Adresse** in den Zwischenspeicher und klicken Sie auf **Abbrechen**.
- (3) Gehen Sie in das Menü **VoIP->Media Gateway->CLID-Umwandlung->Neu**.

The screenshot shows a configuration interface with a dark red header 'Basisparameter'. Below the header, there are several input fields and dropdown menus:

- Beschreibung:** A text input field containing 'CLID_any->SIP-Link'.
- Rufnummer:** A dropdown menu with 'Beliebig' selected.
- Angerufene Leitung:** A dropdown menu with 'SIP-Link' selected.
- Angerufene Adresse:** A text input field (empty).
- Transformation der rufenden Adresse:** A text input field containing '<+49911:>;<+49:0>;<+:00>;'.

Abb. 118: CLID- Umwandlung

- (4) Geben Sie eine **Beschreibung** ein, z. B. *CLID_any->SIP-Link*
- (5) Belassen Sie **Rufnummer** *Beliebig*.
- (6) Wählen Sie **Angerufene Leitung** *SIP-Link*.
- (7) Fügen Sie in das Feld **Transformation der rufenden Adresse** den Wert aus der Zwischenablage *<+49911:>;<+49:0>;<+:00>;* ein und bestätigen Sie die Einstellung mit **OK**.
- (8) Klicken Sie auf **Konfiguration speichern**, um die Konfiguration zu speichern.
- (9) Klicken Sie auf **Ausloggen**, um sich vom Gerät abzumelden.

11.2.4 be.IP 4isdn Slave konfigurieren (Teil 2)

SIP Client Account

Als Nächstes wird ein SIP Client Account auf dem Slave angelegt.

- (1) Loggen Sie sich mit der IP-Adresse *192.168.0.252* auf dem Slave ein.
- (2) Gehen Sie in das Menü **VoIP ->Einstellungen->SIP-Konten->Neu**.

Basisparameter	Trunk-Einstellungen
Beschreibung SIP-Link	SIP-Header-Feld: FROM Display Keiner
Administrativer Status Aktiviert	SIP-Header-Feld: FROM User Anruferadresse
Trunk-Modus <input type="radio"/> Aus <input checked="" type="radio"/> Client <input type="radio"/> Server <input type="radio"/> Gateway	SIP-Header-Feld: P-Preferred Benutzername
Registrar 192.168.0.251	SIP-Header-Feld: P-Asserted Keiner
Ausgehender Proxy	Rufnummer
Realm	
Protokoll UDP Port: 5060	
Benutzername be.ip_4isdn	
Authentifizierungs-ID be.ip_4isdn	
Passwort ●●●●●●●●	
Standort Nicht definiert (Registrierung nur in privaten Netzwerken)	
Art der Registrierung <input checked="" type="radio"/> Einzel <input type="radio"/> Bulk (BNC) <input type="radio"/> Keine Registrierung	

Abb. 119: SIP Account (Slave)

- (3) Geben Sie eine **Beschreibung** ein, z. B. *SIP-Link*.
- (4) Wählen Sie **Trunk-Modus** *Client*.
- (5) Geben Sie unter **Registrar** die IP-Adresse des Masters ein, nämlich *192.168.0.251*.

**Hinweis**

Beachten Sie, dass die Parameter **Benutzername**, **Authentifizierungs-ID** und **Passwort** mit den Angaben im Master übereinstimmen müssen.

- (6) Geben Sie einen **Benutzernamen** ein, z. B. *be.IP_4isdn*.
- (7) Geben Sie eine **Authentifizierungs-ID** ein, z. B. *be.IP_4isdn*.
- (8) Geben Sie ein **Passwort** ein, z. B. *beIP4secret*.
- (9) Bestätigen Sie Ihre Eingaben mit **OK**.

Bidirektionales Routing konfigurieren

Für das bidirektionale Routing werden zwei Einträge angelegt, für jede Richtung ein Eintrag.

Eintrag 1

- (1) Gehen Sie in das Menü **VoIP ->Media Gateway->Anrufkontrolle->Neu**.

Basisparameter

Beschreibung
SIP-Link -> ISDN-Ports

Administrativer Status Aktivieren

Typ Erlauben ▾

Anrufende Leitung SIP-Link ▾

Anrufende Adresse
*

Angerufene Adresse
*

Anrufkontrolle

Priorität	Leitung	Transformation der gerufenen Adresse	Status	Aktion
1	bri-0		✓	^ ▾
2	bri-1		✓	^ ▾
3	bri-2		✓	^ ▾
4	bri-3		✓	^ ▾

Abb. 120: Call Routing (Eintrag 1)

- (2) Geben Sie eine **Beschreibung** ein, z. B. *SIP-Link->ISDN-Ports*.
- (3) Belassen Sie **Administrativer Status** *Aktivieren* und **Typ** *Erlauben*.
- (4) Wählen Sie unter **Anrufende Leitung** *SIP-Link*.
- (5) Geben Sie bei **Anrufende Adresse** und **Angerufene Adresse** jeweils * ein.
- (6) Klicken Sie auf **Hinzufügen**.
- (7) Wählen Sie unter **Routing-Regel** als **Leitung** *bri-0* und klicken Sie auf **Überneh-**

men.

- (8) Klicken Sie erneut auf **Hinzufügen** und wiederholen Sie den Vorgang für *bri-1* bis *bri-3* bis die oben abgebildete Liste auf Ihrem Gerät angezeigt wird.
- (9) Bestätigen Sie Ihre Einstellungen mit **OK**.

Eintrag 2

- (1) Gehen Sie in das Menü **VoIP->Media Gateway->Anrufkontrolle->Neu**.

Basisparameter

Beschreibung
ISDN-Ports -> SIP-Link

Administrativer Status Aktivieren

Typ Erlauben ▾

Anrufende Leitung Beliebig ▾

Anrufende Adresse
*

Angerufene Adresse
*

Anrufkontrolle

Priorität	Leitung	Transformation der gerufenen Adresse	Status	Aktion
1	SIP-Link		✔	^ ▾ 🗑️ ✎

Abb. 121: Call Routing (Eintrag 2)

- (2) Geben Sie eine **Beschreibung** ein, z. B. *ISDN-Ports -> SIP-Link*.
- (3) Belassen Sie **Administrativer Status** *Aktivieren* und **Typ** *Erlauben*.
- (4) Wählen Sie unter **Anrufende Leitung** *Beliebig*.
- (5) Geben Sie bei **Anrufende Adresse** und **Angerufene Adresse** jeweils * ein.
- (6) Klicken Sie auf **Hinzufügen**.
- (7) Wählen Sie **Leitung** *SIP-Link* und klicken Sie auf **Übernehmen**.
- (8) Bestätigen Sie Ihre Einstellungen mit **OK**.
Die Konfiguration des Slaves ist abgeschlossen.
Die Transformation der Rufnummern erfolgt im Master. Daher muss auf dem Slave keine Konfiguration zu diesem Zweck erfolgen.

- (9) Klicken Sie auf **Konfiguration speichern** und auf **Ausloggen**, um die Konfiguration zu speichern und das Gerät zu verlassen.

11.3 Konfigurationsschritte im Überblick

SYNC-Anschluss Einstellungen

Feld	Menü	Wert
SYNC-Anschluss Modus	Physikalische Schnittstellen->ISDN-Porst->ISDN-Konfiguration	<i>Standard</i> = Aktiviert
SYNC-Anschluss Modus	Physikalische Schnittstellen->ISDN-Porst->ISDN-Konfiguration	<i>Slave</i> = Aktiviert

IP-Adresse ändern (Slave)

Feld	Menü	Wert
IP-Adresse	Assistenten->Erste Schritte->Grundeinstellungen	<i>192.168.0.252</i>
Standard-Gateway-IP-Adresse	Assistenten->Erste Schritte->Grundeinstellungen	<i>192.168.0.251</i>
DNS-Server 1	Assistenten->Erste Schritte->Grundeinstellungen	<i>192.168.0.251</i>
Dieses Gerät als DHCPv4-Server verwenden	Assistenten->Erste Schritte->Grundeinstellungen	deaktiviert
Systemzeit über Zeitserver aktualisieren	Assistenten->Erste Schritte->Grundeinstellungen->Erweiterte Einstellungen	<i>Aktiviert</i>
Primärer NTP-Zeitserver	Assistenten->Erste Schritte->Grundeinstellungen->Erweiterte Einstellungen	<i>192.168.0.251</i>

DDI Account (Master)


Feld	Menü	Wert
Status des Media Gateways	Assistenten->Telefonie->Erste Schritte	<i>Aktiviert</i>
Ortsnetzkenzahl	Assistenten->Telefonie->Erste Schritte	<i>z. B. 911</i>
ISDN x + 1 (bri-x)	Assistenten->Telefonie->Erste Schritte	<i>Punkt-zu-Punkt</i>

Feld	Menü	Wert
	Schritte	<i>(Anlagenanschluss)</i>
Verbindungstyp	Assistenten->Telefonie->SIP-Provider->Neu	<i>SIP-Durchwahl</i>
Typ	Assistenten->Telefonie->SIP-Provider->Neu	<i>DeutschlandLAN</i>
Beschreibung	Assistenten ->Telefonie ->SIP-Provider ->Neu ->Weiter	z. B. <i>+49911xxxxxx</i>
Telefonie-Benutzername	Assistenten ->Telefonie ->SIP-Provider ->Neu ->Weiter	z. B. <i>471187654321</i>
Telefonie-Passwort	Assistenten ->Telefonie ->SIP-Provider ->Neu ->Weiter	z. B. <i>Scrt2E4E</i>
Registrierungsrufnummer	Assistenten ->Telefonie ->SIP-Provider ->Neu ->Weiter	z. B. <i>+499119876</i>
Durchwahlnummer	Assistenten ->Telefonie ->SIP-Provider ->Neu ->Weiter	z. B. <i>123456</i>
ISDN-Ports	Assistenten ->Telefonie ->SIP-Provider ->Neu ->Weiter	Aktiviert

SIP Server Account (Master)


Feld	Menü	Wert
Beschreibung	VoIP->Einstellungen ->SIP-Konten->Neu	z. B. <i>SIP-Link</i>
Trunk-Modus	VoIP->Einstellungen ->SIP-Konten->Neu	<i>Server</i>
Benutzername	VoIP->Einstellungen ->SIP-Konten->Neu	z. B. <i>be.ip_4isdn</i>
Authentifizierungs-ID	VoIP->Einstellungen ->SIP-Konten->Neu	z. B. <i>be.ip_4isdn</i>
Passwort	VoIP->Einstellungen ->SIP-Konten->Neu	z. B. <i>beIP4secret</i>

Eingehende Rufe routen (Master)

Feld	Menü	Wert
Administrativer Status	VoIP->Media Gateway->Anrufkontrolle-><+49911xxxxxx->bri>  Hinzufügen	<i>Aktivieren</i>
Leitung	VoIP->Media Gateway->Anrufkon-	<i>SIP-Link</i>

Feld	Menü	Wert
	trolle-><+49911xxxxxx->bri>  Hinzufügen	
Transformation der gerufenen Adresse	VoIP->Media Gateway->Anrufkontrolle-><+49911xxxxxx->bri>  Hinzufügen	<+49911:>;<0911:>;<+49:0>;<+:00>;

ISDN-TK-Anlage mit CLID-no-screening (optional, Master)

Feld	Menü	Wert
Anrufende Adresse	VoIP->Media Gateway->Anrufkontrolle-><any->+49911xxxxxx> 	Vorhandenen Eintrag löschen

Rufnummer ISDN-konform umwandeln (Master)

Feld	Menü	Wert
Beschreibung	VoIP->Media Gateway->CLID-Umwandlung->Neu	<i>CLID_any->SIP-Link</i>
Rufnummer	VoIP->Media Gateway->CLID-Umwandlung->Neu	<i>Beliebig</i>
Angerufene Leitung	VoIP->Media Gateway->CLID-Umwandlung->Neu	z. B. <i>SIP-Link</i>
Transformation der rufenden Adresse	VoIP->Media Gateway->CLID-Umwandlung->Neu	<+49911:>;<+49:0>;<+:00>;

SIP Client Account (Slave)

Feld	Menü	Wert
Beschreibung	VoIP->Einstellungen->SIP-Konten->Neu	z. B. <i>SIP-Link</i>
Trunk-Modus	VoIP->Einstellungen->SIP-Konten->Neu	<i>Client</i>
Registrar	VoIP->Einstellungen->SIP-Konten->Neu	<i>192.168.0.251</i>
Benutzername	VoIP->Einstellungen->SIP-Konten->Neu	z. B. <i>be.ip_4isdn</i>
Authentifizierungs-ID	VoIP->Einstellungen->SIP-Konten->Neu	z. B. <i>be.ip_4isdn</i>
Passwort	VoIP->Einstellungen->SIP-Konten->Neu	z. B. <i>beIP4secret</i>

Bidirektionales Routing (Eintrag 1, Slave)

Feld	Menü	Wert
Beschreibung	VoIP->Media Gateway->Anrufkontrolle->Neu	SIP-Link->ISDN-Ports
Administrativer Status	VoIP->Media Gateway->Anrufkontrolle->Neu	Aktivieren
Typ	VoIP->Media Gateway->Anrufkontrolle->Neu	Erlauben
Anrufende Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu	SIP-Link
Anrufende Adresse	VoIP->Media Gateway->Anrufkontrolle->Neu	*
Angerufene Adresse	VoIP->Media Gateway->Anrufkontrolle->Neu	*
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	1
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	bri-0
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	2
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	bri-1
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	3
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	bri-2
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	4
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	bri-3

Bidirektionales Routing (Eintrag 2, Slave)

Feld	Menü	Wert
Beschreibung	VoIP->Media Gateway->Anrufkontrolle->Neu	ISDN-Ports->SIP-Link
Administrativer Status	VoIP->Media Gateway->Anrufkontrolle->Neu	Aktivieren
Typ	VoIP->Media Gateway->Anrufkontrolle->Neu	Erlauben

Feld	Menü	Wert
Anrufende Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu	<i>Beliebig</i>
Anrufende Adresse	VoIP->Media Gateway->Anrufkontrolle->Neu	*
Angerufene Adresse	VoIP->Media Gateway->Anrufkontrolle->Neu	*
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	1
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	<i>SIP-Link</i>

Kapitel 12 Zwei gekoppelte be.IP 4isdn an einem Telekom VoIP Einzelrufnummern-Anschluss

12.1 Einleitung

Damit Sie Ihre vorhandene ISDN-TK-Anlage an einem Voice-over-IP-Anschluss weiterverwenden können, benötigen Sie ein Media Gateway. Mit zwei gekoppelten **be.IP 4isdn** Media Gateways (sogenanntes Double Play) können Sie eine ISDN-TK-Anlage mit bis zu acht ISDN-Amtszugängen an einem Voice-over-IP Einzelrufnummern-Anschluss der Deutschen Telekom betreiben.

Eines der beiden Media Gateways wird als Master eingesetzt, das andere als Slave.

Der Master terminiert den Internetanschluss, verwaltet die SIP-Konten des Providers und dient für den Slave als Internet-Standard-Gateway.

Der Slave befindet sich im lokalen Netzwerk des Masters. Er dient im vorliegenden Szenario als nachgeschaltetes Media Gateway, das die Gesamtzahl der verwendbaren ISDN Ports auf bis zu acht erhöht.

Aufgrund der Arbeitsteilung der beiden Geräte unterscheiden sie sich auch in ihrer Konfiguration.

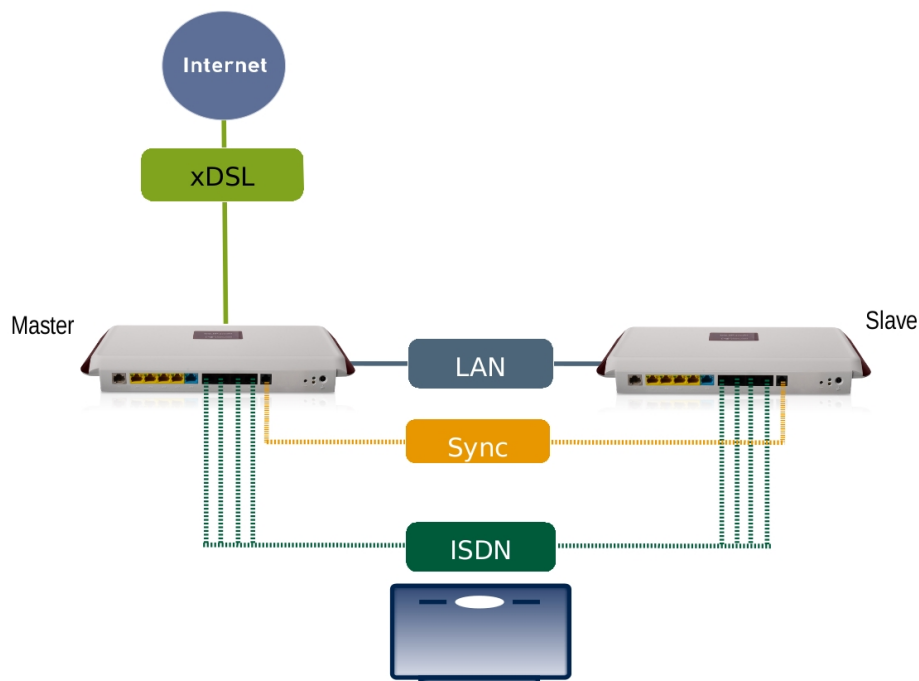


Abb. 122: Beispielszenario

Voraussetzungen

- Zwei **be.IP 4isdn** Geräte Im Media-Gateway-Modus, verbunden durch ein Synchronisationskabel zur Takt-Synchronisation der ISDN-Ports beider Geräte; (Das ISDN-Sync-Kabel kann als Zubehör erworben werden.)
- Systemsoftware-Version 10.1. Rev. 27 Patch 6 oder höher.

12.2 Konfiguration

- (1) Verbinden Sie das Gerät **be.IP 4isdn**, das als Slave dienen soll, mit Ihrem LAN.
- (2) Öffnen Sie einen Browser, geben Sie `192.168.0.251` in die Adresszeile des Browsers ein und bestätigen Sie mit der Eingabetaste.
- (3) Geben Sie **Benutzername** sowie **Kennwort** ein und klicken Sie auf **Anmelden**.

12.2.1 SYNC-Anschluss Einstellungen

Zum störungsfreien Betrieb der TK-Anlage an den ISDN Ports der beiden gekoppelten be.IP4isdn müssen die beiden be.IP4isdn taktsynchron laufen. Hierzu verbinden Sie bitte die beiden be.IP4isdn über die SYNC-Schnittstelle miteinander und konfigurieren beide Geräte gemäß Ihrer zugeordneten Rolle (Standard bzw. Slave).

Zur Konfiguration der Taktsynchronisierung der be.IP4isdn Standard, gehen Sie in das Menü **Physikalische Schnittstellen -> ISDN-Ports -> ISDN-Konfiguration**.

Aktivieren Sie unter **SYNC-Anschluss Modus** die Option *Standard*.

The screenshot shows two sections of a web interface. The top section is titled "SYNC-Anschluss Einstellungen" and contains the "SYNC-Anschluss Modus" settings. Below this is a table for "ISDN-Konfiguration" with columns for "Port" and "ISDN-Switch-Typ".

SYNC-Anschluss Modus
 Der SYNC-Anschluss erlaubt den Anschluss einer zweiten be.IP 4isdn mit Hilfe eines SYNC-Kabels.
 Im "Standard"-Modus arbeitet das Gerät als Taktgeber für ein Gerät im "Slave"-Modus. Stellen Sie sicher, dass Sie ein Gerät als "Standard" und eins als "Slave" konfigurieren. Standard Slave
 Achtung: Für die Auswahl von "Slave" müssen alle ISDN-Ports auf "Intern" geschaltet sein.

Port	ISDN-Switch-Typ	
bri-0 (NT)	Dialup (Euro-ISDN),Punkt-zu-Mehrpunkt	
bri-1 (NT)	Dialup (Euro-ISDN),Punkt-zu-Mehrpunkt	
bri-2 (NT)	Dialup (Euro-ISDN),Punkt-zu-Mehrpunkt	
bri-3 (NT)	Dialup (Euro-ISDN),Punkt-zu-Mehrpunkt	

Abb. 123: **Physikalische Schnittstellen -> ISDN-Ports -> ISDN-Konfiguration**

Zur Konfiguration der Taktsynchronisierung der be.IP4isdn Slave, gehen Sie in das Menü **Physikalische Schnittstellen -> ISDN-Ports -> ISDN-Konfiguration**.

Aktivieren Sie unter **SYNC-Anschluss Modus** die Option *Slave*.

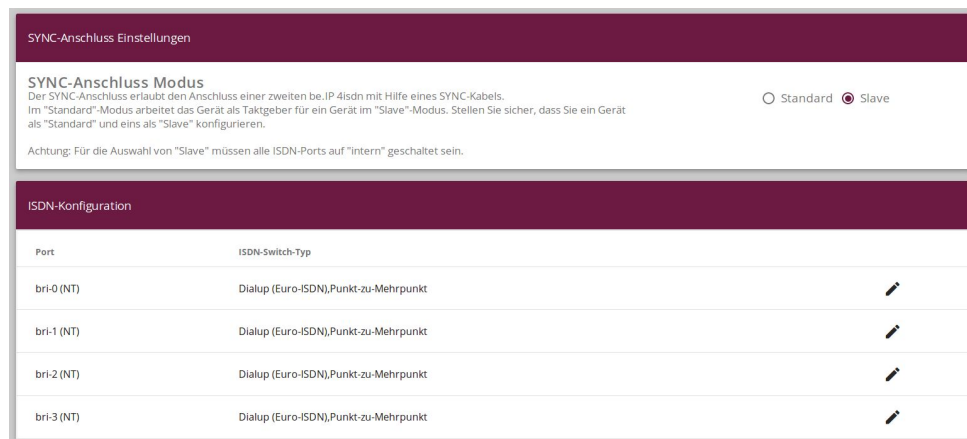


Abb. 124: Physikalische Schnittstellen ->ISDN-Ports->ISDN-Konfiguration

12.2.2 be.IP 4isdn Slave konfigurieren (Teil 1)

IP-Adresse ändern

Um einen Adresskonflikt mit dem Master (der später konfiguriert wird) zu vermeiden, wird die IP-Adresse des Slaves geändert.

- (1) Gehen Sie in das Menü **Assistenten->Erste Schritte->Grundeinstellungen**.

Wählen Sie den physikalischen Ethernet Port für die LAN-Verbindung aus:

Physikalischer Ethernet-Port (LAN)

Geben Sie die IPv4-LAN-Konfiguration ein:

Logische Ethernet-/Bridge-Schnittstelle

Adressmodus Statisch DHCP-Client

IP-Adresse

Netzmaske

Standard-Gateway-IP-Adresse

Feste DNS-Server-Adresse Aktiviert

DNS-Server 1

DNS-Server 2

⚠️ Warnung! Konfigurationsverbindung geht möglicherweise beim Ändern der IP-Adresse verloren! Klicken Sie auf "OK", und melden Sie sich erneut an, um fortzufahren!

Wird dieses Gerät als DHCPv4-Server verwendet?

Dieses Gerät als DHCPv4-Server verwenden

IPv6-Konfiguration eingeben

IPv6

Abb. 125: Slave Konfiguration - IPv4-LAN-Konfiguration

- (2) Ändern Sie die **IP-Adresse** auf den Wert `192.168.0.252`.
- (3) Geben Sie unter **Standard-Gateway-IP-Adresse** die IP-Adresse des Masters ein, nämlich `192.168.0.251`.
- (4) Geben Sie unter **DNS-Server 1** ebenfalls die IP-Adresse des Masters ein, `192.168.0.251`.
- (5) Deaktivieren Sie die Option **Dieses Gerät als DHCPv4-Server verwenden**.
- (6) Klicken Sie auf **Erweiterte Einstellungen**.

Erweiterte Einstellungen

<p>Geben Sie die Einstellungen der Systemzeit ein: ?</p> <p>Manuelle Zeiteinstellung <input type="checkbox"/></p> <p>Systemzeit über Zeitserver aktualisieren <input checked="" type="checkbox"/> Aktiviert</p> <p>Primärer NTP-Zeitserver <input type="text" value="192.168.0.251"/></p> <p>Sekundärer NTP-Zeitserver <input type="text"/></p>	<p>Wählen Sie eine Zeitzone aus: ?</p> <p>Zeitzone <input type="text" value="Europe/Berlin"/></p>
<p>Wird das Gateway als Zeitserver für LAN-Clients verwendet? ?</p> <p>System als Zeitserver <input checked="" type="checkbox"/> Aktiviert</p>	<p>Möchten Sie sich zu dem Gateway über SSH verbinden? ?</p> <p>SSH-Dienst aktiv <input checked="" type="checkbox"/> Aktiviert</p>

Abb. 126: Slave Konfiguration - Systemzeit

- (7) Aktivieren Sie **Systemzeit über Zeitserver aktualisieren**.
- (8) Geben Sie unter **Primärer NTP-Zeitserver** die IP-Adresse des Masters ein, nämlich `192.168.0.251`.



Hinweis

Wenn Sie den Assistenten **Erste Schritte** mit **OK** verlassen, verlieren Sie die Verbindung zum Graphical User Interface (GUI) des Slaves, da sich die IP-Adresse des Geräts geändert hat. Sie müssen sich bei Bedarf mit der neuen IP-Adresse auf dem Gerät einloggen.

- (9) Bestätigen Sie Ihre Eingaben mit **OK**.

12.2.3 be.IP 4isdn Master konfigurieren

Als Nächstes wird der Master in Betrieb genommen und mit dem **Assistenten Ersteinrichtung Telekom** eine Grundkonfiguration des Geräts durchgeführt, sodass die Internetwahl funktionsfähig ist und die Telekom SIP Accounts angelegt und registriert sind.



Hinweis

Der Einfachheit halber wird in dieser Anleitung nur ein SIP Account angelegt.

- (1) Verbinden Sie das Gerät **be.IP 4isdn**, das als Master dienen soll, mit Ihrem LAN.
- (2) Öffnen Sie einen Browser, geben Sie *192.168.0.251* in die Adresszeile ein und bestätigen Sie mit der Eingabetaste.
- (3) Geben Sie **Benutzername** sowie **Kennwort** ein und klicken Sie auf **Anmelden**.
- (4) Wählen Sie **Ansicht** *Vollzugriff*.

Grundkonfiguration

Mit Hilfe des **Assistenten Ersteinrichtung Telekom** wird eine Grundkonfiguration des Geräts vorgenommen.

- (1) Gehen Sie in das Menü **Assistenten->Ersteinrichtung Telekom** und durchlaufen Sie den Assistenten vollständig. Falls Sie Hilfe benötigen, steht Ihnen eine Hilfe zu jedem Schritt und zusätzlich die Online-Hilfe zur Verfügung.
- (2) Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

SIP Account anlegen

Als Nächstes wird mit dem **Assistenten Telefonie** einen SIP Account angelegt.

- (1) Gehen Sie in das Menü **Assistenten->Telefonie->Erste Schritte**.
- (2) Belassen Sie die Einstellung **Status des Media Gateways** *Aktiviert*.
- (3) Geben Sie die **Ortsnetzkenzahl** ein, z. B. *911* für Nürnberg.
- (4) Wählen Sie unter **ISDN-Port-Konfiguration** für alle ISDN-Ports *Punkt-zu-Mehrpunkt (Mehrgeräteanschluss)*.
- (5) Bestätigen Sie Ihre Einstellungen mit **OK**.
- (6) Gehen Sie in das Menü **Assistenten->Telefonie->SIP-Provider->Neu**.
- (7) Wählen Sie **Verbindungstyp** *SIP - Einzelrufnummer*, belassen Sie die Einstellung **Typ** *DeutschlandLAN* und klicken Sie auf **Weiter**.
- (8) Geben Sie eine **Beschreibung** ein, z. B. *+49911xxxxxx7*.
- (9)



Hinweis

Geben Sie unter **Authentifizierungsname / Weblogin** und **Passwort / Web Kennwort** die Informationen ein, die Sie von Ihrem Internet Service Provider (ISP) erhalten haben bzw. belassen Sie die Voreinstellungen.

Belassen Sie z. B. unter **Authentifizierungsname / Weblogin** die Voreinstellung *anonymous@t-online.de*.

- (10) Geben Sie das **Passwort / Web Kennwort** ein, z. B. *tele4Secret*.
- (11) Geben Sie den **Benutzernamen** ein, z. B. *+499119876*

- (12) Aktivieren Sie alle **ISDN-Ports**.
- (13) Geben Sie die **Einzelrufnummer (MSN)** für die Verbindung ein, z. B. *6543*.
- (14) Bestätigen Sie Ihre Einstellungen mit **OK**.

SIP Server Account anlegen

Als Nächstes wird auf dem Master ein SIP Account angelegt, an dem sich später der Client registrieren kann.

- (1) Gehen Sie in das Menü **VoIP->Einstellungen->SIP-Konten->Neu**,

Basisparameter	Trunk-Einstellungen
Beschreibung SIP-Link	SIP-Header-Feld: FROM Display Keiner
Administrativer Status Aktiviert	SIP-Header-Feld: FROM User Anruferadresse
Trunk-Modus Aus Client Server Gateway	SIP-Header-Feld: P-Preferred Benutzername
Realm	SIP-Header-Feld: P-Asserted Keiner
Protokoll UDP Port: 5060	Rufnummer
Benutzername be.ip_4isdn	
Authentifizierungs-ID be.ip_4isdn	
Passwort ●●●●●●●●	
Standort Nicht definiert (Registrierung nur in privaten Netzwerken)	
Art der Registrierung Einzel Bulk (BNC) Keine Registrierung	
Gültigkeit 600 Sekunden	
Angerufene Adresse Standard	
Quell-IP-Adresse überprüfen [Toggle]	
Überprüfung des TLS-Zertifikats [Toggle]	


Abb. 127: SIP Account (Server)

- (2) Geben Sie eine **Beschreibung** ein, z. B. *SIP-Link*.
- (3) Wählen Sie **Trunk-Modus** *Server*.
- (4) Geben Sie einen **Benutzernamen** ein, z. B. *be.ip_4isdn*.
- (5) Geben Sie eine **Authentifizierungs-ID** ein, z. B. *be.ip_4isdn*.
- (6) Geben Sie ein **Passwort** ein, z. B. *beIP4secret*.

- (7) Bestätigen Sie Ihre Einstellungen mit **OK**.











Eingehende Rufe routen

Um eingehende Rufe auf den Slave zu routen, wenn alle ISDN-Ports des Masters belegt sind, wird die entsprechende Route editiert.

- (1) Gehen Sie in das Menü **VoIP->Media Gateway->Anrufrkontrolle** und klicken Sie in der Zeile **<+49911xxxxx7->bri>** auf das Symbol , um den Eintrag zu bearbeiten.
- (2) Klicken Sie auf **Hinzufügen**.

Routing-Regeln

Anrufrkontrolle

Priorität	Leitung	Transformation der gerufenen Adresse	Status	Aktion
1	bri-0	<+49911:><0911:><+49:0><+:00>;	✓	^ v  
2	bri-1	<+49911:><0911:><+49:0><+:00>;	✓	^ v  
3	bri-2	<+49911:><0911:><+49:0><+:00>;	✓	^ v  
4	bri-3	<+49911:><0911:><+49:0><+:00>;	✓	^ v  
5	-		✓	^ v  

HINZUFÜGEN

Routing-Regel

Priorität
5

Administrativer Status Aktivieren

Leitung SIP-Link v

Transformation der gerufenen Adresse
|<+49911:><0911:><+49:0><+:00>;

ÜBERNEHMEN




Abb. 128: Call Route editieren

- (3) Wählen Sie unter **Leitung** *SIP-Link*.
- (4) Kopieren Sie im Abschnitt **Anrufrkontrolle** den Wert unter **Transformation der gerufenen Adresse** `<+49911:><0911:><+49:0><+:00>;` und fügen Sie diesen Wert unter **Routing-Regel** in das Feld **Transformation der gerufenen Adresse** ein.

- (5) Klicken Sie auf **Übernehmen** und auf **OK**.
- (6) Wiederholen Sie den Vorgang für Ihre weiteren SIP Accounts.

ISDN-TK-Anlage mit CLIP no screening (optional)



Hinweis

Wenn Sie eine TK-Anlage mit CLIP no screening verwenden, wird ausgehend (in Richtung SIP-Provider) derjenige SIP Account verwendet, der im Menü **Assistenten->Telefonie->SIP-Provider->Erweiterte Einstellungen** unter **Telefonnummer** als **Hauptrufnummer** eingetragen ist.

Rufnummer umwandeln

Im nächsten Schritt wird die Rufnummer eines Anrufers ISDN-konform umgewandelt.

- (1) Gehen Sie in das Menü **VoIP->Media Gateway->CLID-Umwandlung** und öffnen Sie einen Eintrag, der in der **Beschreibung** *bri* enthält, z. B. *CLID_any->bri-3*.

The screenshot shows a configuration page titled 'Basisparameter'. It contains several fields and dropdown menus:

- Beschreibung:** CLID_any->bri-3
- Rufnummer:** Beliebig (dropdown menu)
- Angerufene Leitung:** bri-3 (dropdown menu)
- Angerufene Adresse:** (empty text field)
- Transformation der rufenden Adresse:** <+49911:>;<+49:0>;<+:00>; (highlighted with a red box)

Abb. 129: CLID- Umwandlung - Wert kopieren

- (2) Kopieren Sie den Wert unter **Transformation der rufenden Adresse** in den Zwischenspeicher und klicken Sie auf **Abbrechen**.
- (3) Gehen Sie in das Menü **VoIP->Media Gateway->CLID-Umwandlung->Neu**.

Basisparameter

Beschreibung CLID_any->SIP-Link	
Rufnummer	Beliebig ▾
Angerufene Leitung	SIP-Link ▾
Angerufene Adresse	
Transformation der rufenden Adresse <+49911:>;<+49:0>;<+:00>;	

Abb. 130: CLID- Umwandlung

- (4) Geben Sie eine **Beschreibung** ein, z. B. *CLID_any->SIP-Link*
- (5) Belassen Sie **Rufnummer** *Beliebig*.
- (6) Wählen Sie **Angerufene Leitung** *SIP-Link*.
- (7) Fügen Sie in das Feld **Transformation der rufenden Adresse** den Wert aus der Zwischenablage *<+49911:>;<+49:0>;<+:00>;* ein und bestätigen Sie die Einstellung mit **OK**.
- (8) Klicken Sie auf **Konfiguration speichern**, um die Konfiguration zu speichern.
- (9) Klicken Sie auf **Ausloggen**, um sich vom Gerät abzumelden.

12.2.4 be.IP 4isdn Slave konfigurieren (Teil 2)

Als Nächstes wird ein SIP Client Account auf dem Slave angelegt.

- (1) Loggen Sie sich mit der IP-Adresse *192.168.0.252* auf dem Slave ein.
- (2) Gehen Sie in das Menü **VoIP->Einstellungen->SIP-Konten->Neu**.

Basisparameter	Trunk-Einstellungen
Beschreibung SIP-Link	SIP-Header-Feld: FROM Display Keiner
Administrativer Status Aktiviert	SIP-Header-Feld: FROM User Anruferadresse
Trunk-Modus <input type="radio"/> Aus <input checked="" type="radio"/> Client <input type="radio"/> Server <input type="radio"/> Gateway	SIP-Header-Feld: P-Preferred Benutzername
Registrar 192.168.0.251	SIP-Header-Feld: P-Asserted Keiner
Ausgehender Proxy	Rufnummer
Realm	
Protokoll UDP Port: 5060	
Benutzername be.ip_4isdn	
Authentifizierungs-ID be.ip_4isdn	
Passwort ●●●●●●●●	
Standort Nicht definiert (Registrierung nur in privaten Netzwerken)	
Art der Registrierung <input checked="" type="radio"/> Einzel <input type="radio"/> Bulk (BNC) <input type="radio"/> Keine Registrierung	

Abb. 131: SIP Account (Slave)

- (3) Geben Sie eine **Beschreibung** ein, z. B. *SIP-Link*.
- (4) Wählen Sie **Trunk-Modus** *Client*.
- (5) Geben Sie unter **Registrar** die IP-Adresse des Masters ein, nämlich *192.168.0.251*.



Hinweis

Beachten Sie, dass die Parameter **Benutzername**, **Authentifizierungs-ID** und **Passwort** mit den Angaben im Master übereinstimmen müssen.

- (6) Geben Sie einen **Benutzernamen** ein, z. B. *be.IP_4isdn*.
- (7) Geben Sie eine **Authentifizierungs-ID** ein, z. B. *be.IP_4isdn*.
- (8) Geben Sie ein **Passwort** ein, z. B. *beIP4secret*.
- (9) Bestätigen Sie Ihre Eingaben mit **OK**.

Bidirektionales Routing konfigurieren

Für das bidirektionale Routing werden zwei Einträge angelegt, für jede Richtung ein Eintrag.

Eintrag 1

- (1) Gehen Sie in das Menü **VoIP -> Media Gateway -> Anrufkontrolle -> Neu**.

Basisparameter

Beschreibung
SIP-Link -> ISDN-Ports

Administrativer Status Aktivieren

Typ Erlauben ▾

Anrufende Leitung SIP-Link ▾

Anrufende Adresse
*

Angerufene Adresse
*

Routing-Regeln

Anrufkontrolle

Priorität	Leitung	Transformation der gerufenen Adresse	Status	Aktion
1	bri-0		✓	^ ▾
2	bri-1		✓	^ ▾
3	bri-2		✓	^ ▾
4	bri-3		✓	^ ▾

Abb. 132: Call Routing (Eintrag 1)

- (2) Geben Sie eine **Beschreibung** ein, z. B. *SIP-Link->ISDN-Ports*.
- (3) Belassen Sie **Administrativer Status** *Aktivieren* und **Typ** *Erlauben*.
- (4) Wählen Sie unter **Anrufende Leitung** *SIP-Link*.
- (5) Geben Sie bei **Anrufende Adresse** und **Angerufene Adresse** jeweils * ein.
- (6) Klicken Sie auf **Hinzufügen**.
- (7) Wählen Sie unter **Routing-Regel** als **Leitung** *bri-0* und klicken Sie auf **Überneh-**

men.

- (8) Klicken Sie erneut auf **Hinzufügen** und wiederholen Sie den Vorgang für *bri-1* bis *bri-3* bis die oben abgebildete Liste auf Ihrem Gerät angezeigt wird.
- (9) Bestätigen Sie Ihre Einstellungen mit **OK**.

Eintrag 2

- (1) Gehen Sie in das Menü **VoIP->Media Gateway->Anrufkontrolle->Neu**.

Basisparameter

Beschreibung
ISDN-Ports -> SIP-Link

Administrativer Status Aktivieren

Typ Erlauben ▾

Anrufende Leitung Beliebig ▾

Anrufende Adresse
*

Angerufene Adresse
*

Routing-Regeln

Anrufkontrolle

Priorität	Leitung	Transformation der gerufenen Adresse	Status	Aktion
1	SIP-Link		✓	^ ▾ 🗑️ ✎

Abb. 133: Call Routing (Eintrag 2)

- (2) Geben Sie eine **Beschreibung** ein, z. B. *ISDN-Ports -> SIP-Link*.
- (3) Belassen Sie **Administrativer Status** *Aktivieren* und **Typ** *Erlauben*.
- (4) Wählen Sie unter **Anrufende Leitung** *Beliebig*.
- (5) Geben Sie bei **Anrufende Adresse** und **Angerufene Adresse** jeweils * ein.
- (6) Klicken Sie auf **Hinzufügen**.
- (7) Wählen Sie **Leitung** *SIP-Link* und klicken Sie auf **Übernehmen**.
- (8) Bestätigen Sie Ihre Einstellungen mit **OK**.
Die Konfiguration des Slaves ist abgeschlossen.
Die Transformation der Rufnummern erfolgt im Master. Daher muss auf dem Slave keine Konfiguration zu diesem Zweck erfolgen.

- (9) Klicken Sie auf **Konfiguration speichern** und auf **Ausloggen**, um die Konfiguration zu speichern und das Gerät zu verlassen.

12.3 Konfigurationsschritte im Überblick

SYNC-Anschluss Einstellungen

Feld	Menü	Wert
SYNC-Anschluss Modus	Physikalische Schnittstellen->ISDN-Porst->ISDN-Konfiguration	<i>Standard</i> = Aktiviert
SYNC-Anschluss Modus	Physikalische Schnittstellen->ISDN-Porst->ISDN-Konfiguration	<i>Slave</i> = Aktiviert

IP-Adresse ändern (Slave)

Feld	Menü	Wert
IP-Adresse	Assistenten->Erste Schritte -> Grundeinstellungen	<i>192.168.0.252</i>
Standard-Gateway-IP-Adresse	Assistenten->Erste Schritte ->Grundeinstellungen	<i>192.168.0.251</i>
DNS-Server 1	Assistenten->Erste Schritte ->Grundeinstellungen	<i>192.168.0.251</i>
Dieses Gerät als DHCPv4-Server verwenden	Assistenten->Erste Schritte ->Grundeinstellungen	deaktiviert
Systemzeit über Zeitserver aktualisieren	Assistenten->Erste Schritte ->Grundeinstellungen->Erweiterte Einstellungen	<i>Aktiviert</i>
Primärer NTP-Zeitserver	Assistenten->Erste Schritte ->Grundeinstellungen->Erweiterte Einstellungen	<i>192.168.0.251</i>

SIP Account (Master)


Feld	Menü	Wert
Status des Media Gateways	Assistenten->Telefonie->Erste Schritte	<i>Aktiviert</i>
Ortsnetzkenzahl	Assistenten->Telefonie->Erste Schritte	<i>z. B. 911</i>
ISDN x + 1 (bri-x)	Assistenten->Telefonie->Erste Schritte	<i>Punkt-zu-Mehrpunkt</i>



Feld	Menü	Wert
	Schritte	<i>(Mehrgeräteanschlus- ss)</i>
Verbindungstyp	Assistenten->Telefonie->SIP- Provider->Neu	<i>SIP- Einzelrufnummer</i>
Typ	Assistenten->Telefonie->SIP- Provider->Neu	<i>DeutschlandLAN</i>
Beschreibung	Assistenten ->Telefonie ->SIP- Provider ->Neu ->Weiter	<i>z. B. +49911xxxxxx7</i>
Authentifizierungsna- me / Weblogin	Assistenten ->Telefonie ->SIP- Provider ->Neu ->Weiter	<i>z. B. anaony- mous@t-online.de</i>
Passwort / Web Kenn- wort	Assistenten ->Telefonie ->SIP- Provider ->Neu ->Weiter	<i>z. B. tele4_Secret</i>
Benutzername	Assistenten ->Telefonie ->SIP- Provider ->Neu ->Weiter	<i>z. B. +499119876</i>
Einzelrufnummer (MSN)	Assistenten ->Telefonie ->SIP- Provider ->Neu ->Weiter	<i>z. B. 6543</i>
ISDN-Ports	Assistenten ->Telefonie ->SIP- Provider ->Neu ->Weiter	<i>Aktiviert</i>

SIP Server Account (Master)

Feld	Menü	Wert
Beschreibung	VoIP->Einstellungen ->SIP-Konten- >Neu	<i>z. B. SIP-Link</i>
Trunk-Modus	VoIP->Einstellungen ->SIP-Konten- >Neu	<i>Server</i>
Benutzername	VoIP->Einstellungen ->SIP-Konten- >Neu	<i>z. B. be.ip_4isdn</i>
Authentifizierungs-ID	VoIP->Einstellungen ->SIP-Konten- >Neu	<i>z. B. be.ip_4isdn</i>
Passwort	VoIP->Einstellungen ->SIP-Konten- >Neu	<i>z. B. beIP4secret</i>

Eingehende Rufe routen (Master)

Feld	Menü	Wert
Administrativer Status	VoIP->Media Gateway->Anrufkon- trolle-><+49911xxxxxx7->bri>  Hinzufügen	<i>Aktivieren</i>

Feld	Menü	Wert
Leitung	VoIP->Media Gateway->Anrufkontrolle-><+49911xxxxx7>->bri>  Hinzufügen	SIP-Link
Transformation der gerufenen Adresse	VoIP->Media Gateway->Anrufkontrolle-><+49911xxxxx7>->bri>  Hinzufügen	<+49911:>;<0911:>; <+49:0>;<+:00>;

Rufnummer ISDN-konform umwandeln (Master)

Feld	Menü	Wert
Beschreibung	VoIP->Media Gateway->CLID-Umwandlung->Neu	CLID_any->SIP-Link
Rufnummer	VoIP->Media Gateway->CLID-Umwandlung->Neu	Beliebig
Angerufene Leitung	VoIP->Media Gateway->CLID-Umwandlung->Neu	z. B. SIP-Link
Transformation der rufenden Adresse	VoIP->Media Gateway->CLID-Umwandlung->Neu	<+49911:>;<+49:0>; <+:00>;

SIP Client Account (Slave)

Feld	Menü	Wert
Beschreibung	VoIP->Einstellungen->SIP-Konten->Neu	z. B. SIP-Link
Trunk-Modus	VoIP->Einstellungen->SIP-Konten->Neu	Client
Registrar	VoIP->Einstellungen->SIP-Konten->Neu	192.168.0.251
Benutzername	VoIP->Einstellungen->SIP-Konten->Neu	z. B. be.ip_4isdn
Authentifizierungs-ID	VoIP->Einstellungen->SIP-Konten->Neu	z. B. be.ip_4isdn
Passwort	VoIP->Einstellungen->SIP-Konten->Neu	z. B. beIP4secret

Bidirektionales Routing (Eintrag 1, Slave)

Feld	Menü	Wert
Beschreibung	VoIP->Media Gateway->Anrufkontrolle->Neu	SIP-Link->ISDN-Ports
Administrativer Status	VoIP->Media Gateway->Anrufkon-	Aktivieren

Feld	Menü	Wert
	trolle->Neu	
Typ	VoIP->Media Gateway->Anrufkontrolle->Neu	<i>Erlauben</i>
Anrufende Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu	<i>SIP-Link</i>
Anrufende Adresse	VoIP->Media Gateway->Anrufkontrolle->Neu	*
Angerufene Adresse	VoIP->Media Gateway->Anrufkontrolle->Neu	*
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	1
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	<i>bri-0</i>
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	2
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	<i>bri-1</i>
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	3
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	<i>bri-2</i>
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	4
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	<i>bri-3</i>

Bidirektionales Routing (Eintrag 2, Slave)

Feld	Menü	Wert
Beschreibung	VoIP->Media Gateway->Anrufkontrolle->Neu	<i>ISDN-Ports->SIP-Link</i>
Administrativer Status	VoIP->Media Gateway->Anrufkontrolle->Neu	<i>Aktivieren</i>
Typ	VoIP->Media Gateway->Anrufkontrolle->Neu	<i>Erlauben</i>
Anrufende Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu	<i>Beliebig</i>
Anrufende Adresse	VoIP->Media Gateway->Anrufkon-	*

Feld	Menü	Wert
	trolle->Neu	
Angerufene Adresse	VoIP->Media Gateway->Anrufkontrolle->Neu	*
Priorität	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	1
Leitung	VoIP->Media Gateway->Anrufkontrolle->Neu->Hinzufügen	<i>SIP-Link</i>

Kapitel 13 be.IP 4isdn als CAPI-Server einrichten

Im Folgenden wird die Konfiguration einer **be.IP 4isdn** als CAPI-Server im Fax Gateway-Modus beschrieben.

Voraussetzungen

- Eine **be.IP 4isdn** im Fax Gateway-Modus (in der GUI als "PBX-Modus (Telefonanlage)" bezeichnet)
- CAPI-Treiber (Laden Sie die Installationsdatei **Remote CAPI für MS-Windows** von unserer Homepage aus dem Download-Bereich).

13.1 Konfiguration

Öffnen Sie eine Web-Browser und geben Sie die IP-Adresse der **be.IP 4isdn** ein. Geben Sie Ihre Anmeldedaten ein und klicken Sie auf **Login**. Die Statusseite der Benutzeroberfläche öffnet sich in der **Ansicht Benutzer**.

Um die **be.IP 4isdn** als Fax-Gateway zu konfigurieren, klicken Sie auf die Karteikarte **Telefonie**.

Legen Sie zuerst die Ländereinstellungen und das Standardziel für kommende Anrufe fest.

Gehen Sie dazu in das Menü **Assistenten->Telefonie->Optionen**.

Ländereinstellungen	
Ländereinstellung	Deutschland
Internationaler Präfix / Länderkennzahl	00 / 49
Nationaler Präfix / Ortsnetzkennzahl	0 / 911

Abb. 134: **Assistenten->Telefonie->Optionen**

Gehen Sie folgendermaßen vor:

- (1) Bei **Ländereinstellungen** wählen Sie das Land aus, in dem das System genutzt wird.
- (2) Geben Sie das **Internationale Präfix / Länderkennzahl** ein. Standardmäßig ist der Eintrag mit *00/49* für Deutschland vorgelegt.
- (3) Tragen Sie den nationalen Präfix / Ortsnetzkennzahl ein. Der **Nationale Präfix** ist mit *0* vorgelegt. Bei **Ortsnetzkennzahl** tragen Sie z. B. *911* für Nürnberg ein.
- (4) Bestätigen Sie mit **OK**.

Im Menü **Assistenten->Telefonie->Anschlüsse->Neu** konfigurieren Sie einen SIP-Provider-Anschluss. Wichtig bei der Wahl des Anschlusses ist, dass der SIP-Provider Fax unterstützt (z. B. Deutsche Telekom).

Typ der Sprachverbindung auswählen:

Verbindungstyp SIP - Einzelrufnummer ▼

Typ DeutschlandLAN Benutzerdefiniert

Abb. 135: **Assistenten->Telefonie->Anschlüsse->Neu**

- (1) Wählen Sie den **Verbindungstyp** *SIP-Einzelrufnummer* aus.
- (2) Bei **Typ** wählen Sie z. B. für einen Telekom-Anschluss *DeutschlandLAN* aus.
- (3) Mithilfe von **Weiter** gelangen Sie in den nächsten Konfigurationsschritt.

SIP-Provider-Einstellungen

Typ

Name Fax-Nummer

Anschlussart Einzelrufnummer

Authentifizierungs-ID anonymous@t-online.de

Passwort *****

Benutzername +49911234567

Rufnummern

Einzelrufnummer (MSN)	Beschreibung
234567	Fax-Extern

HINZUFÜGEN

Abb. 136: **Assistenten->Telefonie->Anschlüsse->Neu->Weiter**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie zur besseren Wiedererkennung einen **Namen** der Verbindung ein, z. B. *Fax-Nummer*.
- (2) Geben Sie die **Authentifizierungs-ID** Ihres Providers ein, hier z. B. die ID der Deutschen Telekom *anonymous@t-online.de*.
- (3) Geben Sie den **Benutzernamen** ein, den Sie von Ihrem Provider erhalten haben, hier z. B. *+49911234567*.
- (4) Bei **Einzelrufnummer (MSN)** geben Sie mit **Hinzufügen** die Nummer ein, über welche das angeschlossene Fax erreichbar ist. Hier z. B. *234567*.
- (5) Geben Sie eine **Beschreibung** ein, z. B. *Fax-Extern*.
- (6) Bestätigen Sie Ihre Eingaben mit **OK**.

Im nächsten Schritt konfigurieren Sie ein neues CAPI-Endgerät.

Gehen Sie in das Menü **Assistenten->Telefonie->Telefone /Endgeräte->Neues Endgerät**.

Abb. 137: **Assistenten->Telefonie->Telefone /Endgeräte->Neues Endgerät**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Schnittstellentyp** die Option *CAPI* aus.
- (2) Geben Sie eine **Beschreibung** für das Endgerät ein, z. B. *Fax CAPI*.
- (3) Bestätigen Sie mit **OK**.

Im letzten Schritt fügen Sie für das Gerät eine Nummer hinzu. Klicken Sie auf der Karteikarte **CAPI, Fax CAPI** auf **Nummer hinzufügen**.

The image shows three panels of a configuration interface for telephone settings.

Grundeinstellungen

- Interne Rufnummer**: Bitte geben Sie die interne Rufnummer ein, die später dem Endgerät zugewiesen wird. Int. Rufnummer: 42
- Beschreibung**: Bitte geben Sie die Beschreibung ein, die im Display des Systemtelefons angezeigt werden soll. Beschreibung: Fax 42
- Parallelruf**: Deaktiviert (toggle switch)

Ausgehende Einstellungen

- Gehende Rufnummer**: Bitte wählen Sie die ausgehende Rufnummer für externe Gespräche. Radio buttons: Standard (unselected), 234567 (selected).
- Wahlberechtigung / Automatische Amtsholung**: Bitte wählen Sie die Wahlberechtigung für externe Gespräche. Dropdown menu: Uneingeschr. AutoAmt

Eingehende Einstellungen

Rufnummern	Zuordnung Tag	Zuordnung Nacht
234567	<input checked="" type="checkbox"/> Zugewiesen	<input checked="" type="checkbox"/> Zugewiesen

Abb. 138: Assistenten->Telefonie->Telefone /Endgeräte->Nummer hinzufügen

Gehen Sie folgendermaßen vor:

- (1) Geben Sie die **Interne Rufnummer** ein, z. B. 42.
- (2) Bei **Beschreibung** geben Sie z. B. *Fax 42* ein.
- (3) Bei **Gehende Rufnummer** wählen Sie die Fax-Rufnummer aus, hier z. B. 234567.
- (4) Die Option **Wahlberechtigung / Automatische Amtsholung** belassen Sie bei *Uneingeschr. AutoAmt*.
- (5) Unter **Eingehende Einstellungen** aktivieren Sie die Option *Zuordnung Tag* und *Zuordnung Nacht*.
- (6) Bestätigen Sie Ihre Eingaben mit **OK**.

Damit ist die Konfiguration an der **be.IP 4isdn** abgeschlossen.

Öffnen Sie den **Remote Multi CAPI Client** . Klicken Sie auf **Mehrere Geräte**.

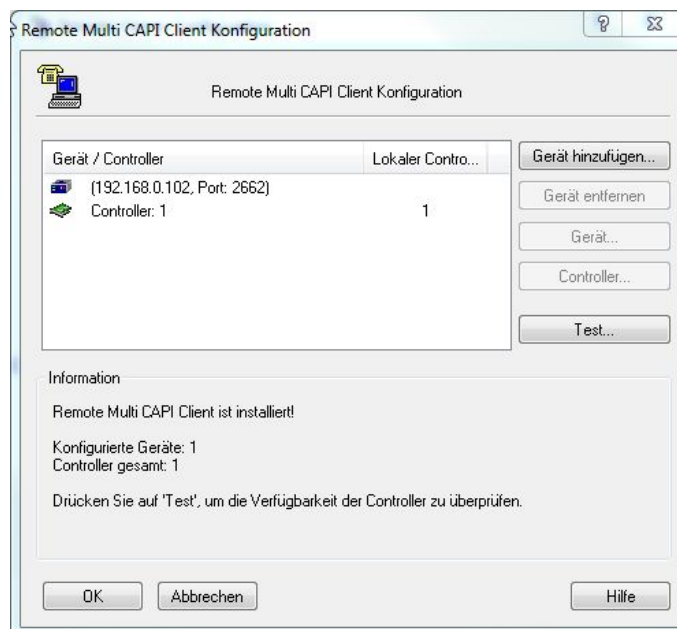


Abb. 139: Remote Multi CAPI Client

Das Remote Multi CAPI Client ist eingerichtet.

Durch Klicken auf die Schaltfläche **Test...** bekommen Sie die Meldung das alle konfigurierten Controller verfügbar sind.



13.2 Konfigurationsschritte im Überblick

Ländereinstellungen

Feld	Menü	Wert
Ländereinstellung	Assistenten ->Telefonie ->Optionen	z. B. <i>Deutschland</i>
Internationaler Präfix / Länderkennzahl	Assistenten ->Telefonie ->Optionen	z. B. <i>00 / 49</i>
Nationaler Präfix / Ortskennzahl	Assistenten ->Telefonie ->Optionen	z. B. <i>0 / 911</i>

SIP-Provider einstellungen

Feld	Menü	Wert
Name	Assistenten ->Telefonie ->Anschlüsse ->Neu	z. B. <i>Fax-Nummer</i>
Authentifizierungs-ID	Assistenten ->Telefonie ->Anschlüsse ->Neu	z. B. <i>anonymous@t-online.de</i>
Benutzername	Assistenten ->Telefonie ->Anschlüsse ->Neu	z. B. <i>+49911234567</i>
Einzelrufnummer (MSN)	Assistenten ->Telefonie ->Anschlüsse ->Neu	z. B. <i>234567</i> und <i>Fax-Extern</i>

CAPI-Endgerät hinzufügen

Feld	Menü	Wert
Schnittstellentyp	Assistenten ->Telefonie ->Telefone / Endgeräte ->Neues Endgerät	<i>CAPI</i>
Beschreibung	Assistenten ->Telefonie ->Telefone / Endgeräte ->Neues Endgerät	z. B. <i>Fax CAPI</i>

Nummer hinzufügen

Feld	Menü	Wert
Interne Rufnummer	Assistenten ->Telefonie ->Telefone / Endgeräte ->Nummer hinzufügen	z. B. <i>42</i>
Beschreibung	Assistenten ->Telefonie ->Telefone / Endgeräte ->Nummer hinzufügen	z. B. <i>Fax 42</i>
Gehende Rufnummer	Assistenten ->Telefonie ->Telefone / Endgeräte ->Nummer hinzufügen	z. B. <i>234567</i>
Wahlberechtigung / Automatische Amtsho-	Assistenten ->Telefonie ->Telefone / Endgeräte ->Nummer hinzufügen	<i>Uneingeschr. Auto-Amt</i>

Feld	Menü	Wert
lung		
Zuordnung Tag	Assistenten ->Telefonie ->Telefone / Endgeräte ->Nummer hinzufügen	<i>Zugewiesen</i>
Zuordnung Nacht	Assistenten ->Telefonie ->Telefone / Endgeräte ->Nummer hinzufügen	<i>Zugewiesen</i>

Kapitel 14 Konfigurationshilfen

14.1 Startansicht ändern

Die **be.IP** startet nach der Anmeldung bis zum vollständigen Durchlaufen des Assistenten **Schnellstart** immer in der Ansicht **Schnellstart**.

Nach vollständigem Durchlaufen dieses Assistenten startet die **be.IP** immer in der Ansicht **Benutzer**.

Voraussetzungen

Eine **be.IP plus**

Konfigurationsziel

Ihre **be.IP plus** soll nach der Anmeldung als *admin* eine andere als die oben erläuterte Ansicht anzeigen.

Sie können unter folgenden Ansichten wählen:

- **Schnellstart**
- **Benutzer**
- **Vollzugriff**.

14.1.1 Konfiguration

Sie können die Startansicht der **be.IP plus** ändern.

- (1) Starten Sie eine SSH-Verbindung zu Ihrem Gerät, z. B. mit Putty.
Sie befinden sich auf der SNMP Shell des Geräts. Der Login-Prompt wird angezeigt.
- (2) Melden Sie sich als **admin** an Ihrem Gerät an.
- (3) Geben Sie `biboextadminitialguiview?` ein, um die möglichen Ansichten anzeigen zu lassen.
`(readwrite) full_access (1), user (2), initial_operation (3)`
wird angezeigt.
- (4) Wenn Sie die Startansicht in **Vollzugriff** ändern wollen, geben Sie `biboextadminitialguiview=full_access` ein.
- (5) Wenn Sie die Startansicht in **Benutzer** ändern wollen, geben Sie `biboextadmini-`

tialguiview=user ein.

- (6) Wenn Sie die Startansicht in **Schnellstart** ändern wollen, geben Sie `biboextadminitialguiview=initial_operation` ein.
- (7) Wenn Sie wollen, dass die jeweilige Einstellung nach einem Reboot bestehen bleibt, speichern Sie die aktuelle Konfiguration.

14.2 Einrichtung an einem Vodafone VDSL-Anschluss

Im Folgenden wird die Einrichtung der Internet- und der Voice-Verbindung beschrieben. Diese Einstellungen sind wichtig für die Konfiguration an einem Vodafone VDSL-Anschluss.

14.2.1 Einrichtung der Internet-Verbindung

Um eine Internet-Verbindung herzustellen, müssen Sie eine Verbindung zu Ihrem Internet-Service-Provider einrichten.

Gehen Sie dazu in das Menü **WAN->Internet + Einwählen->PPPoE->Neu**.

Basisparameter		IPv4-Einstellungen	
Beschreibung	Germany-Vodafone	Sicherheitsrichtlinie	<input checked="" type="radio"/> Nicht Vertrauenswürdig <input type="radio"/> Vertrauenswürdig
PPPoE-Modus	<input checked="" type="radio"/> Standard <input type="radio"/> Mehrfachverbindung	IP-Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen
PPPoE-Ethernet-Schnittstelle	efm35-60	Standardroute	<input checked="" type="checkbox"/> Aktiviert
Benutzername	vodafone-vdsl.komlett/xxxxxxx	NAT-Eintrag erstellen	<input checked="" type="checkbox"/> Aktiviert
Passwort		
VLAN	<input checked="" type="checkbox"/> Aktiviert		
VLAN-ID	7		
Immer aktiv	<input checked="" type="checkbox"/> Aktiviert		
IPv6-Einstellungen			
IPv6	<input type="checkbox"/>		

Abb. 140: **WAN->Internet + Einwählen->PPPoE->Neu**

Erweiterte Einstellungen

Erweiterte Einstellung		Erweiterte IPv4-Einstellungen	
Blockieren nach Verbindungsfehler für	<input type="text" value="60"/> Sekunden	MTU	<input checked="" type="checkbox"/> Automatisch
Maximale Anzahl der erneuten Einwählversuche	<input type="text" value="5"/>		
Authentifizierung	<input type="text" value="PAP/CHAP"/>		
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert		
TCP-ACK-Pakete priorisieren	<input type="checkbox"/>		
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert		

Abb. 141: WAN->Internet + Einwählen->PPPoE->Neu->Erweiterte Einstellungen

Gehen Sie folgendermaßen vor:

- (1) Bei **Beschreibung** geben Sie einen Namen ein, um den PPPoE-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
- (2) Wählen Sie die **PPPoE-Ethernet-Schnittstelle** für die Verbindung aus.
- (3) Bei **Benutzername** muss *vodafone-vdsl.komplett/* vorangestellt werden. Dahinter tragen Sie die Anmeldekennung ein.
- (4) Aktivieren Sie die Funktion **VLAN**.
- (5) Die **VLAN-ID** ist Standardmäßig auf 7 gestellt. Sie können die VLAN-ID ändern (z. B. 132) oder Sie geben die VLAN-ID ein, die Sie von Ihrem Provider erhalten haben.
- (6) Klicken Sie auf **Erweiterte Einstellungen**.
- (7) Wählen Sie die **Authentifizierung** *PAP/CHAP* aus.
- (8) Bestätigen Sie Ihre Angaben mit **OK**.

14.2.2 Einrichtung der Voice-Verbindung

Im Menü **VoIP->Einstellungen->SIP-Provider->Neu** konfigurieren Sie die Voice-Verbindung.

The image shows a configuration interface for SIP settings, divided into five panels:

- Grundeinstellungen:**
 - Beschreibung: Privat
 - Provider-Status: Aktiv Inaktiv
 - Anschlussart: Einzelrufnummer Durchwahl
 - Authentifizierungs-ID: 09119876543
 - Passwort: *****
 - Benutzername: 09119876543
 - Domäne: (empty)
- Einstellungen für Gehende Rufnummer:**
 - Gehende Rufnummer: Standard
- Registrar:**
 - Registrar: 0911.sip.arcor.de
 - Port Registrar: 5060
 - Transportprotokoll: UDP TCP TLS
- STUN:**
 - STUN-Server: stun.arcor.com
 - Port-STUN-Server: 3478
- Timer:**
 - Registrierungstimer: 600 Sekunden

Abb. 143: VoIP->Einstellungen->SIP-Provider->Neu

Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine **Beschreibung** für die Verbindung ein, z. B. *Privat*.
- (2) Bei **Authentifizierungs-ID** und bei **Benutzername** geben Sie die Rufnummer inklusive der Vorwahl ein, z. B. *09119876543*.
- (3) Geben Sie das **Passwort** ein, das Sie von Ihrem Provider erhalten haben.
- (4) Bei **Registrar** geben Sie die Vorwahl des Anschlusses und die Endung ein, z. B. *0911.sip.arcor.de*.
- (5) Sie können einen **STUN-Server** eingeben, hier z. B. *stun.arcor.com*.
- (6) Bestätigen Sie Ihre Angaben mit **OK**.

Damit sind die Einstellungen, die für einen Vodafone VDSL-Anschluss nötig sind, abgeschlossen. Alle weiteren Einstellungen bleiben gleich wie bei einem anderen Anbieter.

14.3 Konfiguration eines DynDNS-Accounts

Im Folgenden wird die Konfiguration eines DynDNS-Accounts auf einer **be.IP plus** oder auf einem bintec VPN-Router beschrieben.

Voraussetzungen

- (1) Eine **be.IP plus** oder ein bintec VPN-Router mit der Systemsoftware 10.1.Rev. 5.
- (2) Eine aktive Internetverbindung mit dynamischer IP-Adresse
- (3) Ein DynDNS-Account bei einem DynDNS-Provider

Zur Konfiguration wird das Graphical User Interface (GUI) verwendet.

Anmerkung

Es gibt eine Vielzahl von deutschen und internationalen DynDNS-Providern, bei denen ein DynDNS-Konto angelegt werden kann. Es gibt sowohl kostenlose als auch kostenpflichtige Angebote. Beispiele sind etwa DynDNS.com, selfHOST.de oder SPDNS.de. In unserem Beispiel wird ein Account von TwoDNS.de verwendet.

14.3.1 Konfiguration

Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse ihres Routers in das Adressfeld ein. Melden Sie sich mit Ihren Anmeldedaten auf dem Router an.

Gehen Sie in das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu.**

Basisparameter

Hostname
IhreFirma@dd-dns.de

Schnittstelle Telekom ▾

Benutzername
IhrUser

Passwort
••••••

Provider dyndns ▾

Aktualisierung aktivieren Aktiviert

Abb. 144: Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu

Gehen Sie folgendermaßen vor:

- (1) Geben Sie den **Hostname** ein, wie er beim DynDNS-Provider registriert ist, z. B. *IhreFirma@dd-dns.de*.
- (2) Wählen Sie die **WAN-Schnittstelle** aus, deren IP-Adresse an den DynDNS-Provider übermittelt werden soll, z. B. *Telekom*.
- (3) Bei **Benutzername** geben Sie den Namen des Kontos ein, wie es beim DynDNS-Provider registriert ist, hier z. B. *IhrUser*.
- (4) Geben Sie das **Passwort** ein, wie es beim DynDNS-Provider registriert ist, z. B. *superSecret*.
- (5) Wählen Sie den DynDNS-**Provider** aus, bei dem oben genannte Daten registriert sind, hier z. B. *TwoDNS*.
- (6) Aktivieren Sie die Option **Aktualisierung aktivieren**.
- (7) Bestätigen Sie Ihre Angaben mit **OK**.

Hilfe zu den verfügbaren Konfigurationsoptionen erhalten Sie über das Online-Hilfe-System.

14.4 Verwendung von Amtsleistungsmerkmalen und Funktionen am IP-basierten Anschluss

IP-basierte Telefonanschlüsse stellen ähnlich wie ISDN-Anschlüsse verschiedene Amtsleistungsmerkmale zur Verfügung, hier am Beispiel eines „Deutschland LAN IP Voice&Data“ der Deutschen Telekom.

Eine Auflistung aller möglichen Funktionen finden Sie unter <https://hilfe.telekom.de/hsp/cms/content/HSP/de/3378/FAQ/theme-133631783/Auftrag/theme-82239611/IP-basierter-Anschluss/faq-445419652>

In den folgenden Erklärungen wird die sofortige Anrufweberschaltung (AWS-sofort) als Beispiel benutzt:

Sofortige Anrufweberschaltung (AWS-sofort)

AWS-sofort einrichten und aktivieren	 *21* Zielrufnummer # <Ansage abwarten> 
Zuvor eingerichtete AWS-sofort aktivieren	 *21 # <Ansage abwarten> 
AWS-sofort deaktivieren	 #21 # <Ansage abwarten> 
AWS-sofort deaktivieren und löschen	 ##21 # <Ansage abwarten> 
Überprüfen, ob eine AWS-sofort aktiviert ist	 *#21 # <Ansage abwarten> 

Die Zielrufnummer muss immer mit Vorwahl eingegeben werden. Bestimmte **Sonderrufnummern** sind **nicht zugelassen**, ebenso Zielrufnummern, die auf Ihrer Negativliste eingetragen wurden.

14.4.1 be.IP und be.IP plus als Mediagateway

Diese Geräte leiten die von ISDN empfangenen Zeichenfolgen entsprechend über SIP an das „Amt“ weiter, so dass hier bei der Eingabe am Endgerät ausschließlich die Besonderheiten einer ggf. nachgeschalteten ISDN-Telefonanlage zu beachten und beim jeweiligen Hersteller der Telefonanlage zu erfragen sind.

14.4.2 be.IP plus als PBX

Hier sind je nach Einstellung in der Berechtigungsklasse zwei Fälle zu unterscheiden

- Amtsholung mit der Amtskennziffer
- Automatische Amtsholung

14.4.2.1 Amtsholung mit der Amtskennziffer

Ist eine Amtsholung eingestellt, so muss diese Amtskennziffer (im Normalfall die „0“) der eigentlichen Sequenz vorangestellt werden, so dass sich für unser Beispiel der Einrichtung und Aktivierung einer „AWS-sofort“ zur Rufnummer 0228-123456789 die Zeichenfolge **0*21*0228123456789#** ergibt. Die Amtskennziffer muss natürlich je nach Einstellung gewählt werden.

14.4.2.2 Automatische Amtsholung

Mit automatischer Amtsholung muss beachtet werden, dass ein vorangestelltes Zeichen „*“ die Wahl zu einer internen Nebenstelle einleitet.

Beispiel: Will bei eingestellter automatischer Amtsholung die Nebenstelle 10 ein internes Gespräch mit der Nebenstelle 30 führen, so lautet die Wahlsequenz dafür: ***30**

Dieses vorher beschriebene Merkmal der **be.IP plus** als PBX führt aber dazu, dass die Eingabe der Zeichenfolge „*21“ als versuchte Anwahl zur internen Nebenstelle 21 gedeutet wird. In der Wahlsequenz muss also für die Telefonanlage deutlich werden, dass diese Zeichenfolge mit vorangestelltem Zeichen „*“ ins Amt übermittelt werden muss.

Dies geschieht durch eine bewusste „Internwahl“ mit nachgestellter Amtsholung mittels der Amtskennziffer (im Normalfall die „0“), also durch ein Vorstellen von „*0“!

Für das Beispiel der Einrichtung und Aktivierung einer „AWS-sofort“ zur Rufnummer 0228-123456789 ergibt sich also die Zeichenfolge: ***0*21*0228123456789#**

Die Amtskennziffer muss natürlich je nach Einstellung gewählt werden.