



# **Benutzerhandbuch Workshops (Auszug)**

## 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	IP - Network Address Translation (NAT) . . . . .	1
1.1	Einleitung . . . . .	1
1.2	Konfiguration. . . . .	2
1.2.1	NAT einschalten . . . . .	2
1.2.2	NAT-Freigaben konfigurieren. . . . .	2
1.3	Ergebnis. . . . .	5
1.4	Kontrolle. . . . .	6
1.5	Konfigurationsschritte im Überblick . . . . .	6
Kapitel 2	IP - Konfiguration eines bintec Routers hinter einem Provider-Router . . . . .	8
2.1	Einleitung . . . . .	8
2.2	Konfiguration der Ports . . . . .	9
2.3	Konfiguration des Internetzugangs . . . . .	11
2.4	Konfiguration der DMZ . . . . .	12
2.4.1	Aktivierung von NAT auf der DMZ-Schnittstelle . . . . .	12
2.4.2	Konfiguration der Portweiterleitung . . . . .	12
2.5	Überprüfen der Konfiguration. . . . .	14
2.5.1	Überprüfen der Portweiterleitung . . . . .	14
2.5.2	Überprüfen der Funktionalität. . . . .	14
2.6	Konfigurationsschritte im Überblick . . . . .	15
Kapitel 3	IP - IPTV am xDSL (ADSL/VDSL) T-Home Entertainment Anschluss . . . . .	18
3.1	Einleitung . . . . .	18

3.2	Konfiguration . . . . .	20
3.2.1	Konfiguration des bintec be.IP . . . . .	20
3.2.2	Konfiguration des IPTV Multicast-Daten Zugangs . . . . .	22
3.2.3	Konfiguration eines DHCP IP- Adress-Pools auf der LAN-Schnittstelle . . . . .	27
3.2.4	Bootfähige Sicherung der Konfiguration . . . . .	29
3.3	Konfigurationsschritte im Überblick . . . . .	29
<b>Kapitel 4</b>	<b>IP - Routing-Protokoll RIPv2 über IPSec-Verbindung. . . . .</b>	<b>32</b>
4.1	Einleitung . . . . .	32
4.2	Konfiguration . . . . .	33
4.2.1	Konfiguration des bintec RS353 am Standort B (Zentrale) . . . . .	33
4.2.2	Konfiguration des bintec RS123 am Standort A (Außenstelle). . . . .	38
4.3	Kontrolle der Funktion . . . . .	42
4.4	Konfigurationsschritte im Überblick . . . . .	43
<b>Kapitel 5</b>	<b>IP - Lastverteilung von zwei parallel genutzten Internetzugängen . . . . .</b>	<b>46</b>
5.1	Einleitung . . . . .	46
5.2	Konfiguration . . . . .	47
5.2.1	Konfiguration der Internetzugänge . . . . .	47
5.2.2	Einrichtung der IP-Lastverteilung . . . . .	49
5.2.3	Spezielle Lastverteilungs-Behandlung von verschlüsselten Verbindungen . . . . .	51
5.2.4	Hinweis zur DNS-Server Konfiguration . . . . .	53
5.3	Konfigurationsschritte im Überblick . . . . .	53
<b>Kapitel 6</b>	<b>IP - Lastverteilung von zwei VPN IPSec-Tunneln über separate Internetzugänge . . . . .</b>	<b>55</b>
6.1	Einleitung . . . . .	55

6.2	Konfiguration . . . . .	56
6.2.1	Konfiguration des Gateways in der Zentrale . . . . .	56
6.2.2	Konfiguration des Gateways in der Filiale . . . . .	71
6.3	Konfigurationsschritte im Überblick . . . . .	88
<b>Kapitel 7</b>	<b>IP - Mit Drop In eine Filiale durch einen VPN-Tunnel mit der Zentrale verbinden . . . . .</b>	<b>97</b>
7.1	Einleitung . . . . .	97
7.2	Konfiguration . . . . .	98
7.3	Konfigurationsschritte im Überblick . . . . .	103
<b>Kapitel 8</b>	<b>IP - Einrichtung einer DMZ mit der Funktionalität der Drop-In-Gruppe . . . . .</b>	<b>106</b>
8.1	Einleitung . . . . .	106
8.2	Konfiguration . . . . .	107
8.2.1	Konfiguration der Ports . . . . .	107
8.2.2	Konfiguration der Drop-In-Gruppe. . . . .	108
8.2.3	Einrichten der Standardroute . . . . .	110
8.2.4	Network Address Translation (NAT) aktivieren . . . . .	111
8.2.5	Konfiguration der Firewall . . . . .	111
8.3	Konfigurationsschritte im Überblick . . . . .	117
<b>Kapitel 9</b>	<b>IP - DSL-Backup über LTE (bintec 4e-LE). . . . .</b>	<b>121</b>
9.1	Einleitung . . . . .	121
9.2	Router konfigurieren . . . . .	121
9.2.1	IP-Konfiguration der Schnittstelle . . . . .	121
9.2.2	DHCP-Server für bintec 4Ge-LE einrichten . . . . .	124
9.2.3	Virtuelle Schnittstelle löschen . . . . .	125
9.2.4	Virtuelle Schnittstelle konfigurieren . . . . .	125

9.2.5	NAT aktivieren . . . . .	127
9.3	Optionale Einstellungen: Telefonie an die DSL-Verbindung binden . . . .	128
9.4	Konfigurationsschritte im Überblick . . . . .	129

# Kapitel 1 IP - Network Address Translation (NAT)

## 1.1 Einleitung

Im Folgenden wird die Konfiguration von Network Address Translation (NAT) erklärt.

Network Address Translation (NAT) ist eine Funktion Ihres Geräts, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen. Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmäßig nur noch in einer Richtung, ausgehend (forward) zugelassen (=Schutzfunktion). Ausnahmeregeln können im Menü **NAT-Konfiguration** konfiguriert werden.

Sie haben eine permanente 2-Mbit-Verbindung ins Internet mit acht IP-Adressen. Ihre Ethernet-Schnittstelle **ETH** ist am Zugangsroutern angeschlossen. Dieser hat die IP-Adresse `62.10.10.1/29`, während die restlichen IPs, von `62.10.10.2` bis `62.10.10.6`, auf der Ethernet-Schnittstelle **ETH** eingetragen sind.

Sie konfigurieren NAT-Freigaben, damit Sie per HTTP auf Ihr Gateway zugreifen können. Ausserdem möchten Sie auf Ihren Terminalserver und auf den Firmen-Webserver über das Internet zugreifen.

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

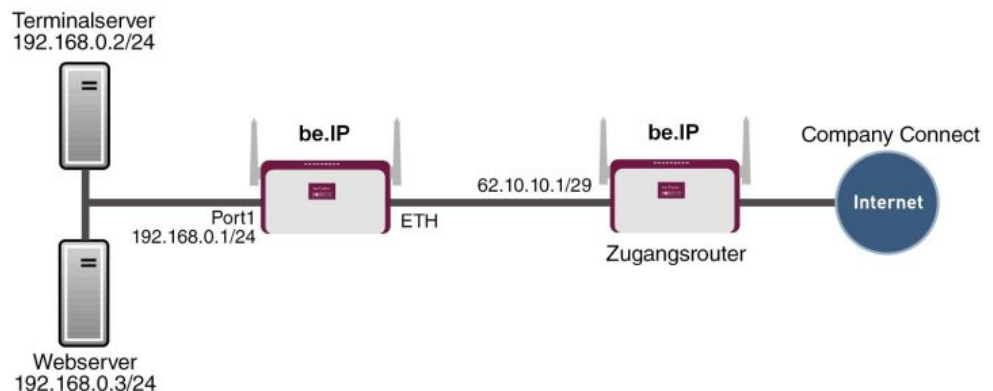


Abb. 1: Beispielszenario NAT

## Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Gateways
- Ein Bootimage der Version 10.1.9
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang. Hier als Beispiel **Company Connect** mit acht IP-Adressen.

## 1.2 Konfiguration

### 1.2.1 NAT einschalten

Im Menü NAT-Schnittstellen wird eine Liste aller NAT-Schnittstellen angezeigt.

Gehen Sie in folgendes Menü, um NAT für ihre Schnittstelle einzuschalten:

- (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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
WAN_ETH0A35-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Abb. 2: **Netzwerk -> NAT -> NAT-Schnittstellen**

Gehen Sie folgendermaßen vor:

- (1) Für die Schnittstelle `LAN_EN1-4` aktivieren Sie die Option **NAT aktiv**. Damit schalten Sie das Feature NAT für die Schnittstelle ein.
- (2) Für die Schnittstelle `LAN_EN1-4` aktivieren Sie die Option **Verwerfen ohne Rückmeldung**. Wenn diese Funktion aktiviert wird, werden keine ICMP-Pakete beantwortet.
- (3) Bestätigen Sie mit **OK**.

### 1.2.2 NAT-Freigaben konfigurieren

#### NAT-Freigabe für das GUI

Ihr Gateway soll mit der festen IP-Adresse `62.10.10.2` über das Internet per HTTP administrierbar sein. Aus Sicherheitsgründen sprechen Sie anstelle von Port `80` z. B. den exter-



nen Port *8080* an.

Gehen Sie in folgendes Menü, um NAT-Einträge zu konfigurieren.

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

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

- Basisparameter:**
  - Beschreibung: GUI
  - Schnittstelle: LAN\_EN1-4
  - Art des Datenverkehrs: eingehend (Ziel-NAT)
- Ursprünglichen Datenverkehr angeben:**
  - Dienst: Benutzerdefiniert
  - Protokoll: TCP
  - Quell-IP-Adresse/Netzmaske: Host, 62.10.10.2
  - Original Ziel-IP-Adresse/Netzmaske: Beliebig
  - Original Ziel-Port/Bereich: -Alle- bis
- Substitutionswerte:**
  - Neue Ziel-IP-Adresse/Netzmaske: Host, 0.0.0.0
  - Neuer Ziel-Port: Original (deaktiviert), 80

Abb. 3: **Netzwerk -> NAT -> NAT-Konfiguration -> Neu**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine **Beschreibung** für die NAT-Konfiguration ein, z. B. *GUI*.
- (2) Wählen Sie die **Schnittstelle** für Ihre NAT-Freigabe aus, z. B. *LAN\_EN1-4*.
- (3) Die **Art des Datenverkehrs** wählen Sie *eingehend (Ziel-NAT)* aus.
- (4) Den **Dienst** lassen Sie auf *Benutzerdefiniert*.
- (5) Als **Protokoll** wählen Sie *TCP*.
- (6) Unter **Quell IP-Adresse/Netzmaske** wählen Sie *Host* aus und geben Sie die externe IP-Adresse des Gateways ein, z. B. *62.10.10.2*.
- (7) Unter **Neuer Ziel-Port** deaktivieren Sie **Original** und geben in das Eingabefeld *80* ein.
- (8) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

### NAT-Freigabe für den Webserver

Der interne Webserver soll unter der IP-Adresse *62.10.10.3* angesprochen werden. Weil der Webserver als Web-Host für einen öffentliche Internetauftritt dient, wird der externe Standard-Port *80* verwendet.

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

The screenshot shows a NAT configuration interface with three main sections:

- Basisparameter:**
  - Beschreibung: Webserver
  - Schnittstelle: LAN\_EN1-4
  - Art des Datenverkehrs: eingehend (Ziel-NAT)
- Ursprünglichen Datenverkehr angeben:**
  - Dienst: http
  - Quell-IP-Adresse/Netzmaske: Host, 62.10.10.3
  - Original Ziel-IP-Adresse/Netzmaske: Beliebig
- Substitutionswerte:**
  - Neue Ziel-IP-Adresse/Netzmaske: Host, 192.168.0.3
  - Neuer Ziel-Port: Original (disabled)

Abb. 4: Netzwerk -> NAT -> NAT-Konfiguration -> Neu

Gehen Sie folgendermaßen vor, um die Freigabe zu konfigurieren:

- (1) Geben Sie eine **Beschreibung** für die NAT-Konfiguration ein, z. B. *Webserver*.
- (2) Die **Schnittstelle** stellen Sie auf *LAN\_EN1-4*.
- (3) Die **Art des Datenverkehrs** wählen Sie *eingehend (Ziel-NAT)* aus.
- (4) Den **Dienst** stellen Sie auf *http*.
- (5) Unter **Quell-IP-Adresse/Netzmaske** wählen Sie *Host* aus und geben Sie die IP-Adresse des internen Webserver ein, hier z. B. *62.10.10.3*.
- (6) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** wählen Sie *Host* aus und tragen die interne IP-Adresse, z. B. *192.168.0.3* ein.
- (7) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

### NAT-Freigabe für den Terminal-Server

Der interne Terminal-Server soll unter der IP-Adresse *62.10.10.4* angesprochen werden. Angreifer könnten bei geöffnetem Port *3389* leicht erkennen, dass Sie einen Terminal-Server einsetzen. Daher sprechen Sie von extern mit Remote Desktop einen anderen Port an, beispielsweise Port *5000*.

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

The screenshot shows a NAT configuration interface with three main sections:

- Basisparameter:**
  - Beschreibung: Terminal-Server
  - Schnittstelle: LAN\_EN1-4
  - Art des Datenverkehrs: eingehend (Ziel-NAT)
- Ursprünglichen Datenverkehr angeben:**
  - Dienst: Benutzerdefiniert
  - Protokoll: TCP
  - Quell-IP-Adresse/Netzmaske: Host, 62.10.10.4
  - Original Ziel-IP-Adresse/Netzmaske: Beliebig
  - Original Ziel-Port/Bereich: -Alle- bis
- Substitutionswerte:**
  - Neue Ziel-IP-Adresse/Netzmaske: Host, 192.168.0.2
  - Neuer Ziel-Port: Original (deaktiviert), 3389

Abb. 5: Netzwerk -> NAT -> NAT-Konfiguration -> Neu

Gehen Sie folgendermaßen vor, um die Freigabe zu konfigurieren:

- (1) Geben Sie eine **Beschreibung** für die NAT-Konfiguration ein, z. B. *Terminal-Server*.
- (2) Die **Schnittstelle** stellen Sie auf *LAN\_EN1-4*.
- (3) Die **Art des Datenverkehrs** wählen Sie *eingehend (Ziel-NAT)* aus.
- (4) Den **Dienst** lassen Sie auf *Benutzerdefiniert*.
- (5) Als **Protokoll** wählen Sie *TCP*.
- (6) Unter **Quell-IP-Adresse/Netzmaske** wählen Sie *Host* aus und geben Sie die IP-Adresse des internen Terminal-Servers ein, hier z. B. *62.10.10.4*.
- (7) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** wählen Sie *Host* aus und tragen die interne IP-Adresse, hier z. B. *192.168.0.2* ein.
- (8) Bei **Neuer Ziel-Port** deaktivieren Sie **Original** und geben in das Eingabefeld *3389* an.
- (9) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

## 1.3 Ergebnis

Sie haben eine NAT-Freigabe konfiguriert, um über das Internet per HTTP auf das Gateway zugreifen können. Zudem gestatten Sie den Zugriff über das Internet auf Ihren internen Webserver und den Terminal-Server.

## 1.4 Kontrolle

Um die Einstellungen zu überprüfen, rufen Sie den Debug-Modus an der Shell mit dem Befehl `debug all` auf. Rufen Sie den Browser an einem externen Rechner im Internet auf und geben Sie die IP-Adresse des Gateways an z. B. `http://62.10.10.2:8080`.

Folgende Meldung müsste erscheinen, wenn Sie von der IP-Adresse `80.65.48.135` kommen:

```
12:14:20 DEBUG/INET: NAT: new incoming session on ifc 5000
prot 6 127.0.0.1:80/ 62.10.10.2:8080 &lt;- 80.65.48.135:1024
```

## 1.5 Konfigurationsschritte im Überblick

### NAT einschalten

Feld	Menü	Wert
NAT aktiv	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für LAN_EN1-4
Verwerfen ohne Rückmeldung	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für LAN_EN1-4

### NAT-Freigaben konfigurieren

Feld	Menü	Wert
Beschreibung	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>GUI</i>
Schnittstelle	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>LAN_EN1-4</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>
Quell-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>62.10.10.2</i>
Neuer Ziel-Port	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>80</i>

**Websserver**

<b>Feld</b>	<b>Menü</b>	<b>Wert</b>
<b>Beschreibung</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>Webserver</i>
<b>Schnittstelle</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>LAN_EN1-4</i>
<b>Art des Datenverkehrs</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>eingehend (Ziel-NAT)</i>
<b>Dienst</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>http</i>
<b>Quell-IP-Adresse/Netzmaske</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>62.10.10.3</i>
<b>Neuer Ziel-Port</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>192.168.0.3</i>

**Terminal Server**

<b>Feld</b>	<b>Menü</b>	<b>Wert</b>
<b>Beschreibung</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>Terminal-Server</i>
<b>Schnittstelle</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>LAN_EN1-4</i>
<b>Art des Datenverkehrs</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>eingehend (Ziel-NAT)</i>
<b>Dienst</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>Benutzerdefiniert</i>
<b>Protokoll</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>TCP</i>
<b>Quell-IP-Adresse/Netzmaske</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>62.10.10.4</i>
<b>Neue Ziel-IP-Adresse/Netzmaske</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>192.168.0.2</i>
<b>Neuer Ziel-Port</b>	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>3389</i>

## Kapitel 2 IP - Konfiguration eines bintec Routers hinter einem Provider-Router

### 2.1 Einleitung

Im Folgenden wird die Konfiguration einer DMZ (Demilitarized Zone) mit einem **bintec be.IP** beschrieben.

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

Alle FTP- und HTTP/HTTPS-Anfragen aus dem Internet sollen an einen FTP- bzw. an einen Webserver in der DMZ weitergeleitet werden. Das Gateway verfügt über eine Internetfestverbindung mit statischer öffentlicher IP-Adresse, die über den Port **ETH** angeschlossen ist.

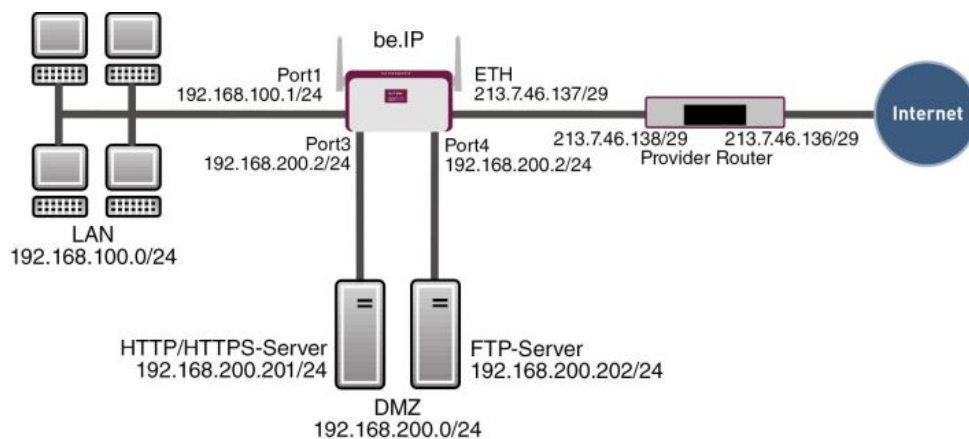


Abb. 6: Beispielszenario DMZ

### Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein **bintec be.IP** Gateway
- Ein Bootimage der Version 10.1.9
- Internetzugang mit statischer öffentlicher IP-Adresse
- Ein FTP- und ein Webserver in der DMZ

- Ihr LAN ist an Port **1** oder **2** (Schnittstelle `en1-0`) des Gateways angeschlossen.
- Ihre DMZ ist an Port **3** oder **4** (Schnittstelle `en1-1`) des Gateways angeschlossen.
- Die Internetfestverbindung ist an Port **ETH** (`en5-0`) angeschlossen.

## 2.2 Konfiguration der Ports

Um die DMZ einzurichten, werden die vier Switchports des **bintec be.IP** auf zwei Schnittstellen aufgeteilt.

- Port **1** und **2** werden der Schnittstelle `en1-0` zugeordnet.
- Port **3** und **4** werden der Schnittstelle `en1-1` zugeordnet.

Gehen Sie in folgendes Menü um die Ports den Schnittstellen zuzuordnen:

- (1) Gehen Sie zu **Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration**.

Switch-Port	Ethernet-Schnittstellenauswahl	Konfigurierte Geschwindigkeit / Konfigurierter Modus	Aktuelle Geschwindigkeit / Aktueller Modus	Flusskontrolle
1	en1-0	Vollständige automatische Aushandlung	100 Mbit/s / Full Duplex	Deaktiviert
2	en1-0	Vollständige automatische Aushandlung	Inaktiv	Deaktiviert
3	en1-1	Vollständige automatische Aushandlung	Inaktiv	Deaktiviert
4	en1-1	Vollständige automatische Aushandlung	Inaktiv	Deaktiviert
5	en1-4	Vollständige automatische Aushandlung	Inaktiv	Deaktiviert

Abb. 7: **Physikalische Schnittstellen -> Ethernet -Ports -> Portkonfiguration**

Gehen Sie folgendermaßen vor, um die Ports zu Schnittstellen zuzuordnen:

- (1) Wählen Sie bei **Ethernet-Schnittstellenauswahl** für die **Switch-Ports 1** und **2** `en1-0` im Dropdown-Menü aus.
- (2) Wählen Sie für die **Switch-Ports 3** und **4** `en1-1` aus.
- (3) Bestätigen Sie mit **OK**.

Im Menü **IP-Konfiguration** können Sie den Ports IP-Adressen zuweisen.

- (1) Gehen Sie zu **LAN -> IP-Konfiguration -> Schnittstellen -> <en1-0>** .



Abb. 8: LAN -> IP-Konfiguration -> Schnittstellen -> <en1-0> -> ✎

Gehen Sie folgendermaßen vor:

- (1) Belassen Sie **Adressmodus** bei *Statisch*. Der Schnittstelle wird eine statische IP-Adresse zugewiesen.
- (2) Tragen Sie bei **IP-Adresse / Netzmaske** die IP-Adresse und die Subnetzmaske ein, hier *192.168.100.1* und *255.255.255.0*.
- (3) Belassen Sie **Schnittstellenmodus** auf *Untagged*. Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet.
- (4) Bestätigen Sie mit **OK**.

Da Ihr Gerät administrativ nun nicht mehr unter der vorherigen IP-Adresse erreichbar ist, sondern unter der neuen IP-Adresse *192.168.100.1*, müssen Sie sich erneut mit dem **GUI** verbinden. Geben Sie dazu die neue IP-Adresse *192.168.100.1* in die Adresszeile Ihres Browsers ein und melden sich erneut an.

Verfahren Sie anschliessend für die Schnittstelle *en1-1* entsprechend:

- (1) Gehen Sie für *en1-1* zu **LAN -> IP-Konfiguration -> Schnittstellen -> <en1-1>**.
- (2) Klicken Sie auf das ✎-Symbol.
- (3) Belassen Sie **Adressmodus** bei *Statisch*.
- (4) Tragen Sie bei **IP-Adresse / Netzmaske** die IP-Adresse und die Subnetzmaske ein, hier *192.168.200.2* und *255.255.255.0*.
- (5) Belassen Sie **Schnittstellenmodus** auf *Untagged*.
- (6) Bestätigen Sie mit **OK**.


Sollte kein Eintrag für eine IP-Adresse vorhanden sein, klicken Sie bei IP-Adresse / Netzmaske auf **Hinzufügen**. Dann erscheint ein Feld für die Eingabe der IP-Adresse und Sie können die IP-Adresse und die Subnetzmaske vergeben.



## 2.3 Konfiguration des Internetzugangs

Das Gateway verfügt über eine Internetfestverbindung über einen Router des Providers. Daher müssen Sie die statische öffentliche IP-Adresse des Gateways definieren und eine Standardroute über den Router des Providers konfigurieren.

Konfigurieren Sie die statische öffentliche IP-Adresse für die Schnittstelle `en5-0` analog zur Konfiguration der Ports im vorherigen Abschnitt:

- (1) Gehen Sie für `en5-0` zu **LAN -> IP-Konfiguration -> Schnittstellen -> <en5-0>**.
- (2) Klicken Sie auf das -Symbol.
- (3) Belassen Sie **Adressmodus** bei *Statisch*.
- (4) Tragen Sie bei **IP-Adresse / Netzmaske** die IP-Adresse und die Subnetzmaske ein, hier `213.7.46.137` und `255.255.255.248`.
- (5) Belassen Sie **Schnittstellenmodus** auf *Untagged*.
- (6) Bestätigen Sie mit **OK**.

Richten Sie eine Standardroute über den Router des Providers ein.

- (1) Gehen Sie zu **Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu**.

Basisparameter	Routenparameter
Routentyp Standardroute über Gateway	Gateway-IP-Adresse 213.7.46.138
Schnittstelle LAN_EN5-0	Metrik 1
Routenklasse <input checked="" type="radio"/> Standard <input type="radio"/> Erweitert	

Abb. 9: **Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Routentyp** *Standardroute über Gateway* aus. Standardroute wird benutzt, wenn keine andere passende Route verfügbar ist.
- (2) Wählen Sie die **Schnittstelle** aus, welche für diese Route verwendet werden soll, z. B. `LAN_EN5-0`.
- (3) Tragen Sie bei **Gateway-IP-Adresse** die IP-Adresse des Internet-Gateways ein, hier `213.7.46.138`.
- (4) Wählen Sie bei **Metrik** die Priorität der Route aus, z. B.
  1. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route.
- (5) Bestätigen Sie Ihre Angaben mit **OK**.

## 2.4 Konfiguration der DMZ

### 2.4.1 Aktivierung von NAT auf der DMZ-Schnittstelle

Auf der Schnittstelle, welche für die Internetverbindung verwendet wird, muss NAT aktiviert werden.

Gehen Sie in folgendes Menü, um NAT für die DMZ-Schnittstelle zu aktivieren:

- (1) Gehen Sie zu **Netzwerk -> NAT -> 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_EN5-0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
WAN_ETH0A35-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Abb. 10: **Netzwerk -> NAT -> NAT-Schnittstellen**

Gehen Sie folgendermaßen vor:

- (1) Für die Schnittstelle `LAN_EN5-0` setzen Sie bei **NAT aktiv** einen Haken. Damit schalten Sie das Feature NAT für die Schnittstelle ein.
- (2) Für die Schnittstelle `LAN_EN5-0` setzen Sie bei **Verwerfen ohne Rückmeldung** einen Haken. Wenn diese Funktion aktiviert wird, gibt es für verworfene Pakete keine Rückmeldung an den Absender.
- (3) Bestätigen Sie mit **OK**.

### 2.4.2 Konfiguration der Portweiterleitung

Da auf der Schnittstelle für die Internetverbindung NAT aktiviert wurde, ist es nun nicht mehr möglich, vom Internet aus auf interne Rechner zuzugreifen. Es soll externen Benutzern allerdings gestattet werden, über FTP auf den FTP-Server und über HTTP bzw. HTTPS auf den Webserver zuzugreifen. Daher müssen Sie für diese Dienste Portweiterleitung einrichten.

Gehen Sie in folgendes Menü, um benötigte Ports an den FTP- bzw. Webserver weiterzuleiten:

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

Basisparameter	Ursprünglichen Datenverkehr angeben
Beschreibung FTP	Dienst ftp
Schnittstelle LAN_EN5-0	Quell-IP-Adresse/Netzmaske Beliebig
Art des Datenverkehrs eingehend (Ziel-NAT)	Original Ziel-IP-Adresse/Netzmaske Host 213.7.46.137
Substitutionswerte	
Neue Ziel-IP-Adresse/Netzmaske Host 192.168.200.202	
Neuer Ziel-Port Original	

Abb. 11: Netzwerk-> NAT -> NAT-Konfiguration -> Neu

Gehen Sie folgendermaßen vor, um eine Portweiterleitung für FTP zu erstellen:

- (1) Geben Sie eine **Beschreibung** für die NAT-Konfiguration ein, z. B. *FTP*.
- (2) Wählen Sie bei **Schnittstelle** *LAN\_EN5-0* aus.
- (3) Als **Art des Datenverkehrs** wählen Sie *eingehend (Ziel-NAT)* aus.
- (4) Wählen Sie bei **Dienst** *ftp* aus.
- (5) Bei **Original Ziel-IP-Adresse/Netzmaske** wählen Sie *Host* aus und tragen Sie die statische öffentliche IP-Adresse des Gateways ein, hier *213.7.46.137*.
- (6) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** wählen Sie *Host* aus und tragen Sie die IP-Adresse des FTP-Servers ein, hier z. B. *192.168.200.202*.
- (7) Bestätigen Sie mit **OK**.

Gehen Sie folgendermaßen vor, um eine Portweiterleitung für HTTP zu erstellen:

- (1) Gehen Sie zu **Routing -> NAT -> NAT-Konfiguration -> Neu**.
- (2) Geben Sie eine **Beschreibung** für die NAT-Konfiguration ein, z. B. *HTTP*.
- (3) Wählen Sie bei **Schnittstelle** *LAN\_EN5-0* aus.
- (4) Als **Art des Datenverkehrs** wählen Sie *eingehend (Ziel-NAT)* aus.
- (5) Wählen Sie bei **Dienst** *http* aus.
- (6) Bei **Original Ziel-IP-Adresse/Netzmaske** wählen Sie *Host* aus und tragen Sie die statische öffentliche IP-Adresse des Gateways ein, hier *213.7.46.137*.
- (7) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** wählen Sie *Host* aus und tragen Sie die IP-Adresse des HTTP-Servers ein, hier z. B. *192.168.200.201*.
- (8) Bestätigen Sie mit **OK**.

Gehen Sie folgendermaßen vor, um eine Portweiterleitung für HTTPS zu erstellen:

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

- (2) Geben Sie eine **Beschreibung** für die NAT-Konfiguration ein, z. B. *HTTPS*.
- (3) Wählen Sie bei **Schnittstelle** *LAN\_EN5-0* aus.
- (4) Als **Art des Datenverkehrs** wählen Sie *eingehend (Ziel-NAT)* aus.
- (5) Wählen Sie bei **Dienst** *http (SSL)* aus.
- (6) Bei **Original Ziel-IP-Adresse/Netzmaske** wählen Sie *Host* aus und tragen Sie die statische öffentliche IP-Adresse des Gateways ein, hier *213.7.46.137*.
- (7) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** wählen Sie *Host* aus und tragen Sie die IP-Adresse des HTTPS-Servers ein, hier z. B. *192.168.200.201*.
- (8) Bestätigen Sie mit **OK**.

## 2.5 Überprüfen der Konfiguration

### 2.5.1 Überprüfen der Portweiterleitung

Die Liste der konfigurierten Portweiterleitung sollte nun wie folgt aussehen:

- (1) Bleiben Sie dazu im Menü **Netzwerk -> NAT -> NAT-Konfiguration**.










NAT-Konfiguration						
Beschr.	Richtng.	Dienst/Protokoll	Quell-IP/Maske:Port	Ziel-IP/Maske:Port	Neu: Quell-IP/Maske:Port (Q)	Neu: Ziel-IP/Maske:Port (Z)
FTP	Eingehend	ftp(TCP)	0.0.0.0/ 0.0.0.0: -	213.7.46.137/ 255.255.255.255:21	(Z)192.168.200.202/ 255.255.255.255	  
HTTP	Eingehend	http(TCP)	0.0.0.0/ 0.0.0.0: -	213.7.46.137/ 255.255.255.255:80	(Z)192.168.200.201/ 255.255.255.255	  
HTTPS	Eingehend	http(SSL)(TCP)	0.0.0.0/ 0.0.0.0: -	213.7.46.137/ 255.255.255.255:443	(Z)192.168.200.201/ 255.255.255.255	  

Abb. 12: **Netzwerk -> NAT -> NAT-Konfiguration**

Durch diese Liste werden nun alle FTP-Anfragen auf die öffentliche IP-Adresse Ihres Gateways an Ihren FTP-Server weitergeleitet. HTTP- und HTTPS-Anfragen werden entsprechend an Ihren Webserver weitergeleitet. Jegliche anderen Anfragen werden vom Gateway abgelehnt.

Klicken Sie auf **Konfiguration speichern** und bestätigen Sie anschließend mit **OK**, um die Konfiguration als Startkonfiguration zu speichern.

### 2.5.2 Überprüfen der Funktionalität

Die Überprüfung der Funktionalität kann nur von der Shell aus erfolgen. Geben Sie dazu den Befehl `debug all` ein und bestätigen Sie mit **Return**.

```



r232bw:&gt; debug all
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80 &lt;- 62.137.56.89:1050
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80 &lt;- 62.137.56.89:1051
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80 &lt;- 62.137.56.89:1052
01:36:33 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.202:21/213.7.46.137:21 &lt;- 84.135.23.189:1053

```


Wie im Debug-Auszug zu sehen ist, wurden HTTP-Anfragen (Port 80) von der IP-Adresse 62.137.56.89 auf die IP-Adresse 192.168.200.201 weitergeleitet. Ebenso wurde eine FTP-Anfrage (Port 21) von der IP-Adresse 84.135.23.189 auf die IP-Adresse 192.168.200.202 weitergeleitet.

## 2.6 Konfigurationsschritte im Überblick

### Konfiguration der Ports

Feld	Menü	Wert
Ethernet-Schnittstellenauswahl	Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration	Switch-Port 1 und 2 auf <i>en1-0</i>
Ethernet-Schnittstellenauswahl	Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration	Switch-Port 3 und 4 auf <i>en1-1</i>
IP-Adresse / Netzmaske	LAN -> IP-Konfiguration -> Schnittstellen -> <en1-0> -> 	<i>192.168.100.1</i> und <i>255.255.255.0</i>
IP-Adresse / Netzmaske	LAN -> IP-Konfiguration -> Schnittstellen -> <en1-1> -> 	<i>192.168.200.2</i> und <i>255.255.255.0</i>

### Konfiguration des Internetzugangs

Feld	Menü	Wert
IP- /Netzmaske	LAN -> IP-Konfiguration -> Schnittstellen -> <en5-0> -> 	<i>213.7.46.137</i> und <i>255.255.255.248</i>
Routentyp	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	<i>Standardroute über Gateway</i>
Schnittstelle	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	<i>LAN_EN5-0</i>
Gateway	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	<i>213.7.46.138</i>

### NAT

Feld	Menü	Wert
NAT aktiv	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für LAN_EN5-0
Verwerfen ohne Rückmeldung	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für LAN_EN5-0

#### Portweiterleitung

Feld	Menü	Wert
Beschreibung	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>FTP</i>
Schnittstelle	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>LAN_EN5-0</i>
Art des Datenverkehrs	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	eingehend (Ziel-NAT)
Dienst	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>ftp</i>
Original Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>213.7.46.137</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>192.168.200.202</i>
Beschreibung	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>HTTP</i>
Schnittstelle	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>LAN_EN5-0</i>
Art des Datenverkehrs	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	eingehend (Ziel-NAT)
Dienst	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>http</i>
Original Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>213.7.46.137</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>192.168.200.201</i>
Beschreibung	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>HTTPS</i>
Schnittstelle	Netzwerk -> NAT -> NAT-	<i>LAN_EN5-0</i>

Feld	Menü	Wert
	<b>Konfiguration -&gt; Neu</b>	
<b>Art des Datenverkehrs</b>	<b>Netzwerk -&gt; NAT -&gt; NAT-Konfiguration -&gt; Neu</b>	eingehend (Ziel-NAT)
<b>Dienst</b>	<b>Netzwerk -&gt; NAT -&gt; NAT-Konfiguration -&gt; Neu</b>	<i>http (SSL)</i>
<b>Original Ziel-IP-Adresse/Netzmaske</b>	<b>Netzwerk -&gt; NAT -&gt; NAT-Konfiguration -&gt; Neu</b>	z. B. <i>213.7.46.137</i>
<b>Neue Ziel-IP-Adresse/Netzmaske</b>	<b>Netzwerk -&gt; NAT -&gt; NAT-Konfiguration -&gt; Neu</b>	z. B. <i>192.168.200.201</i>

## Kapitel 3 IP - IPTV am xDSL (ADSL/VDSL) T-Home Entertainment Anschluss

### 3.1 Einleitung

Die vorliegende Lösung zeigt die Konfiguration eines bintec Routers an einem xDSL T-Home Entertainment-Anschluss der neuen Generation. Bei ADSL sowie VDSL T-Home-Anschlüssen der neuen Generation werden die Internet Daten sowie IPTV Multicast-Daten über getrennte VLAN-Schnittstellen übertragen.

Die folgende Tabelle zeigt die wesentlichen technischen Informationen zur Konfiguration der beiden Zugänge:

#### Internet Daten Zugang

VLAN-ID	7
Netzwerkprotokoll	PPPoE
IP-Zuweisung erfolgt über	IPCP (Internet Protocol Control Protocol)
Routing	Standard Route muss konfiguriert sein
NAT	Aktiv (Network Address Translation)

#### IPTV Multicast Daten Zugang

VLAN-ID	8
IP-Zuweisung erfolgt über	DHCP (Dynamic Host Configuration Protocol)
IGMP-Proxy	Aktiv (Internet Group Management Protocol)
Routing	Erforderliche Routen werden über DHCP gelernt (keine weitere Konfiguration erforderlich)
NAT	Nicht zwingend erforderlich, aus Sicherheitsgründen im Beispiel aktiviert (Network Address Translation)

In diesem Beispiel wird ein VDSL-Anschluss verwendet. Das ADSL/VDSL-Modem ist am physikalischen Ethernet-Port *ETH5* angeschlossen. Wenn Sie ein Gerät mit integriertem DSL-Modem haben, so können Sie selbstverständlich auch das interne Modem verwenden.





### Hinweis

Bitte beachten Sie, dass diese Konfiguration nur funktionsfähig ist, wenn das angeschlossene oder auch das interne Modem sich als reine Modems verhalten (bei den internen Modems der bintec-Geräte ist dies gegeben). Wenn Sie einen ggf. mitgelieferten Router lediglich in den Zustand versetzen, dass er wie ein Modem agiert, kann es unter Umständen zu Problemen kommen.

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

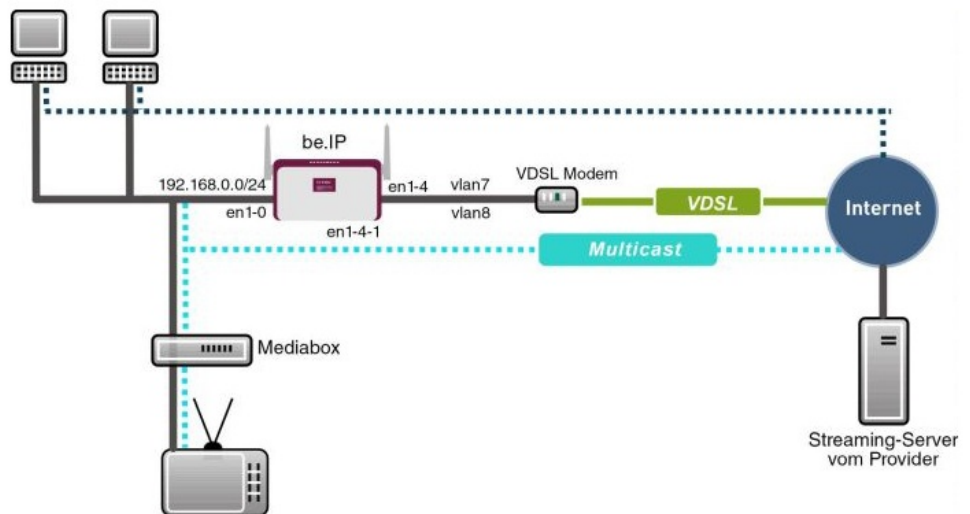


Abb. 13: Beispielszenario

## Voraussetzungen

Provider spezifisch:

- T-Home ADSL/VDSL- Anschluss der neuen Generation mit T-Home Entertainment-Paket
- Media Box (T-Home X301T) oder ähnliches Gerät (meist vom Provider gestellt)

bintec elmeg spezifisch:

- Im vorliegenden Beispiel wurde ein **bintec be.IP** mit Software Version 10.1.9 verwendet.
- Die Konfiguration ist für andere bintec Routertypen identisch.
- Die Konfiguration erfolgt über das **GUI** Web-Konfigurations-Tool.

## 3.2 Konfiguration

### 3.2.1 Konfiguration des bintec be.IP

Zur Konfiguration öffnen Sie einen Internet Browser und starten eine Web (HTTP)-Verbindung zum **bintec be.IP** Router. Soweit nicht anders konfiguriert, verwenden Sie hierzu die Standard IP-Adresse *192.168.0.251*. Nach erfolgreichem Aufbau der HTTP-Verbindung loggen Sie sich über folgende Zugangsdaten ein.

**User** *admin* **Password** *admin* (Standard Passwort sofern nicht anders konfiguriert).

#### Konfiguration des VDSL-Internetzugangs

Zur Konfiguration eines VDSL-Internetzugangs verfügt das **GUI** über einen Assistenten. Gehen Sie dazu in folgendes Menü:

- (1) Gehen Sie zu **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu**.

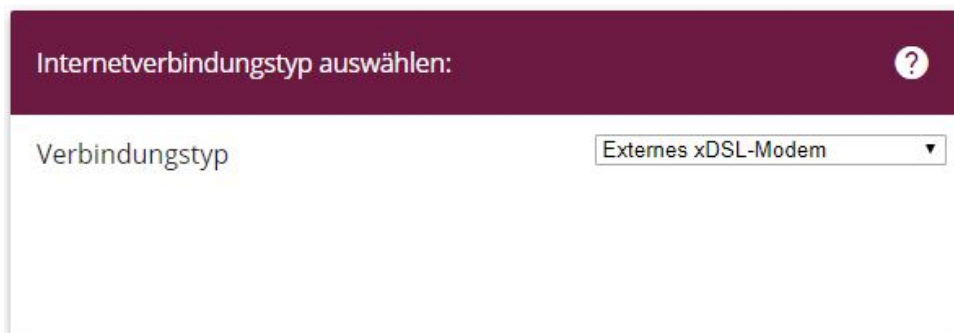


Abb. 14: **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Verbindungstyp** *Externes xDSL-Modem* aus.
- (2) Klicken Sie auf **Weiter**, um eine neue Internetverbindung zu konfigurieren.

Geben Sie die erforderlichen Daten für die Internetverbindung ein.

Beschreibung  
Internet-Daten

<p>Wählen Sie den physischen Ethernet-Port aus, der mit dem externen xDSL-Modem verbunden ist:</p> <p>Physischer Ethernet-Port <input type="text" value="ETH5"/></p>	<p>Wählen Sie aus der Liste Ihren Internetdienstanbieter (ISP) aus:</p> <p>Typ <input type="text" value="Vordefiniert"/></p> <p>Land <input type="text" value="Germany"/></p> <p>Internet Service Provider <input type="text" value="Telekom - VDSL"/></p>
<p>Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:</p> <p>Anschlusskennung <input type="text" value="012345678945"/></p> <p>Zugangsnummer (vormals T-Online Nummer) <input type="text" value="955012345678"/></p> <p>Mitbenutzernummer <input type="text" value="0001"/></p> <p>Persönliches Kennwort <input type="password" value="*****"/></p>	<p>Wählen Sie den Verbindungsmodus aus:</p> <p>Immer aktiv <input checked="" type="checkbox"/> Aktiviert</p>

Abb. 15: Assistenten -> Internet -> Internetverbindungen -> Weiter

Gehen Sie folgendermaßen vor, um eine neue Internetverbindung zu konfigurieren:

- (1) Bei **Beschreibung** geben Sie eine beliebige Bezeichnung für die Internetverbindung ein, z. B. *Internet-Daten* ein.
- (2) Im Menüpunkt **Physischer Ethernet-Port** wählen Sie den physikalischen Ethernet-Port aus an dem das xDSL-Modem angeschlossen ist, hier *ETH5*.
- (3) Bei **Typ** wählen Sie die Option *Vordefiniert* aus.
- (4) Wählen Sie das **Land** aus, indem der Internetzugang eingerichtet werden soll. Hier z. B. *Germany*.
- (5) Bei **Internet Service Provider** wählen Sie für unseren VDSL-Anschluss das Profil *Telekom - VDSL* aus.  
Für einen T-Online-Anschluss werden folgende Angaben benötigt:
- (6) Bei **Anschlusskennung** geben Sie die 12-stellige Anschlusskennung ein, die Sie von der Telekom erhalten haben.
- (7) Geben Sie die **Zugangsnummer** ein (meist 12-stellig), die Sie von der Telekom erhalten haben.
- (8) Geben Sie die **Mitbenutzernummer** ein, die Sie von der Telekom erhalten haben (für den Hauptnutzer immer 0001).
- (9) Geben Sie das **Persönliche Kennwort** ein, das Sie von Ihrem Provider erhalten haben.
- (10) 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.
- (11) Bestätigen Sie Ihre Angaben mit **OK**.

### 3.2.2 Konfiguration des IPTV Multicast-Daten Zugangs

Um die Virtuelle LAN-Schnittstellen für den Multicast-Zugang zu konfigurieren, gehen Sie in folgendes Menü:

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

Basisparameter	Grundlegende IPv4-Parameter
Basierend auf Ethernet-Schnittstelle <span>en1-4</span>	Sicherheitsrichtlinie <input type="radio"/> Nicht Vertrauenswürdig <input checked="" 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 8	DHCP-Metrik 1
MAC-Adresse <span>00:a0:f9</span> <input checked="" type="checkbox"/> Voreingestellte verwenden	IP-Adresse / Netzmaske <input type="text"/> IP-Adresse <input type="text"/> Netzmaske HINZUFÜGEN

#### Erweiterte Einstellungen

Erweiterte IPv4-Einstellungen	
DHCP-MAC-Adresse <input type="text"/>	<input checked="" type="checkbox"/> Voreingestellte verwenden
DHCP-Hostname <input type="text"/>	
DHCP Broadcast Flag	<input type="checkbox"/>
Standardroute erstellen	<input checked="" type="checkbox"/> Aktiviert
Proxy ARP	<input type="checkbox"/>
TCP-MSS-Clamping	<input type="checkbox"/> Deaktiviert

Abb. 17: LAN -> IP-Konfiguration -> Schnittstellen -> Neu

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Basierend auf Ethernet-Schnittstelle** die logische Ethernet-Schnittstelle aus, welches dem oben verwendeten physikalischem Ethernet-Port zugeordnet ist. Für den Ethernet-Port ETH5 ist das die Schnittstelle *en1-4* (siehe dazu

die Erläuterung im Anschluss).

- (2) Den **Schnittstellenmodus** stellen Sie auf *Tagged (VLAN)*. Mit dieser Option weisen Sie die Schnittstelle einem VLAN zu.
- (3) Im Eingabefeld **VLAN-ID** geben Sie die zu verwendende VLAN-ID *8* ein.
- (4) Stellen Sie den **Adressmodus** auf *DHCP*. Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
- (5) Klicken Sie auf **Erweiterte Einstellungen**.
- (6) Deaktivieren Sie die Option **DHCP Broadcast Flag** (Ausstrahlungskennzeichnung).
- (7) Belassen Sie die restlichen Einstellungen und bestätigen Sie Ihre Angaben mit **OK**.

### Erläuterung zur Zuordnung physikalischer Ethernet-Ports und logischen Ethernet-Schnittstellen

Die Zuordnung zwischen den physikalischen Ethernet-Port und der logischen Ethernet-Schnittstelle ist in den Routern mit integriertem Switch flexibel konfigurierbar. Im Auslieferungszustand gilt in der Regel folgende Zuordnung:

Physikalischer Ethernet-Port	Logische Ethernet-Schnittstelle
ETH1 bis ETH4	en1-0
ETH5	en1-4

Genauere Informationen über die bei Ihnen konfigurierte Zuordnung finden Sie im Menü **Physikalische Schnittstellen**. Für den im Workshop verwendeten **bintec be.IP** Router sieht dies im Auslieferungszustand wie folgt aus:

- (1) Gehen Sie zu **Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration**.

Switch-Port	Ethernet-Schnittstellenauswahl	Konfigurierte Geschwindigkeit / Konfigurierter Modus	Aktuelle Geschwindigkeit / Aktueller Modus	Flusskontrolle
1	en1-0	Vollständige automatische Aushandlung	100 Mbit/s / Full Duplex	Deaktiviert
2	en1-0	Vollständige automatische Aushandlung	inaktiv	Deaktiviert
3	en1-0	Vollständige automatische Aushandlung	inaktiv	Deaktiviert
4	en1-0	Vollständige automatische Aushandlung	inaktiv	Deaktiviert
5	en1-4	Vollständige automatische Aushandlung	inaktiv	Deaktiviert

Abb. 18: Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration

### Konfiguration des IGMP-Proxy (Internet Group Management Protocol)

Im Folgenden konfigurieren Sie den zum Empfang der IPTV Multicast-Daten notwendigen IGMP-Proxy.

- (1) Gehen Sie zu **Multicast -> IGMP -> IGMP -> Neu**.

### IGMP-Einstellungen

Schnittstelle	LAN_EN1-0
Abfrage Intervall	125 Sekunden
Maximale Antwortzeit	10,0 Sekunden
Robustheit	2
Antwortintervall (Letztes Mitglied)	1,0 Sekunden
Maximale Anzahl der IGMP-Statusmeldungen	0 Meldungen pro Sekunde
Modus	<input type="radio"/> Host <input checked="" type="radio"/> Routing

## Erweiterte Einstellungen

Abb. 20: Multicast -&gt; IGMP -&gt; IGMP -&gt; Neu

Gehen Sie folgendermaßen vor, um den IGMP-Proxy zu konfigurieren.

- (1) Bei **Schnittstelle** wählen Sie die logische Ethernet-Schnittstelle aus, an der die Media-Box oder die Client-PCs angeschlossen sind. In unserem Beispiel sind das die Ethernet-Ports ETH1 bis ETH4. Aufgrund oben genannter Zuordnung ist die logische Ethernet-Schnittstelle `LAN_EN1-0` zu wählen.
- (2) Wählen Sie bei **Modus** `Routing` aus.
- (3) Klicken Sie auf **Erweiterte Einstellungen**.
- (4) Aktivieren Sie die Option **IGMP Proxy**.
- (5) Als **Proxy-Schnittstelle** wählen Sie die generierte VLAN-Schnittstelle `LAN_EN1-4-1` aus.
- (6) Belassen Sie die restlichen Einstellungen und bestätigen Sie Ihre Angaben mit **OK**.

Die fertige Konfiguration sieht wie folgt aus (der Eintrag für die IGMP-Proxy-Schnittstelle (`en1-4-1`) wird automatisch erzeugt):

Schnittstelle	Aktuelle IGMP-Version	IGMP
en1-0	0	<input checked="" type="checkbox"/> Aktiviert
en1-4-1	0	<input checked="" type="checkbox"/> Aktiviert

Abb. 21: Multicast -&gt; IGMP -&gt; IGMP

### Aktivierung der Multicast Routing-Funktion

Standardmäßig ist das Weiterleiten von IP Multicast-Paketen auf dem bintec Router deaktiviert. Im folgenden Konfigurationsschritt aktivieren Sie die Multicast Routing-Funktion auf

dem Router. Gehen Sie dazu in folgendes Menü:

- (1) Gehen Sie zu **Multicast -> IGMP -> Optionen**.

Grundeinstellungen	
IGMP-Status	<input type="radio"/> Aktiv <input type="radio"/> Inaktiv <input checked="" type="radio"/> Auto
Modus	<input checked="" type="radio"/> Kompatibilitätsmodus <input type="radio"/> Nur Version 3
Maximale Gruppen	<input type="text" value="64"/>
Maximale Quellen	<input type="text" value="64"/>
Maximale Anzahl der IGMP-Statusmeldungen	<input type="text" value="0"/> Meldungen pro Sekunde

Abb. 22: **Multicast -> IGMP -> Optionen**

Gehen Sie folgendermaßen vor:

- (1) Setzen Sie den **IGMP-Status** auf *Aktiv* oder *Auto*.
- (2) Bestätigen Sie die Angabe mit **OK**.



#### Hinweis

Das einmalige Bestätigen der Konfigurationsseite mit **OK** ist zwingend erforderlich. Dies gilt auch dann, wenn der **IGMP-Status** bereits auf *Auto* oder *Aktiv* eingestellt ist.

### Aktivierung von NAT auf der IGMP Proxy-Schnittstelle

Aus Sicherheitsgründen und um das Funktionieren von Video-on Demand-Diensten sicher zu stellen, ist die NAT-Funktion zu aktivieren.

- (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_EN1-1	<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"/>	3
LAN_EN1-4-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
WAN_ETH0A35-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
WAN_INTERNET-DATEN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Abb. 23: **Netzwerk -> NAT -> NAT-Schnittstellen**

Gehen Sie folgendermaßen vor:

- (1) Aktivieren Sie unter **NAT aktiv** die Schnittstelle `LAN_EN1-4-1`.
- (2) Bestätigen Sie mit **OK**.

### 3.2.3 Konfiguration eines DHCP IP- Adress-Pools auf der LAN-Schnittstelle

Die T-Home Media-Box erfordert die dynamische Zuweisung der IP-Adress-Einstellungen über DHCP. Zu diesem Zweck ist die Konfiguration eines DHCP IP-Adress- Pools auf der LAN-Schnittstelle erforderlich. In unserem Fall ist das die Schnittstelle `en1-0`.

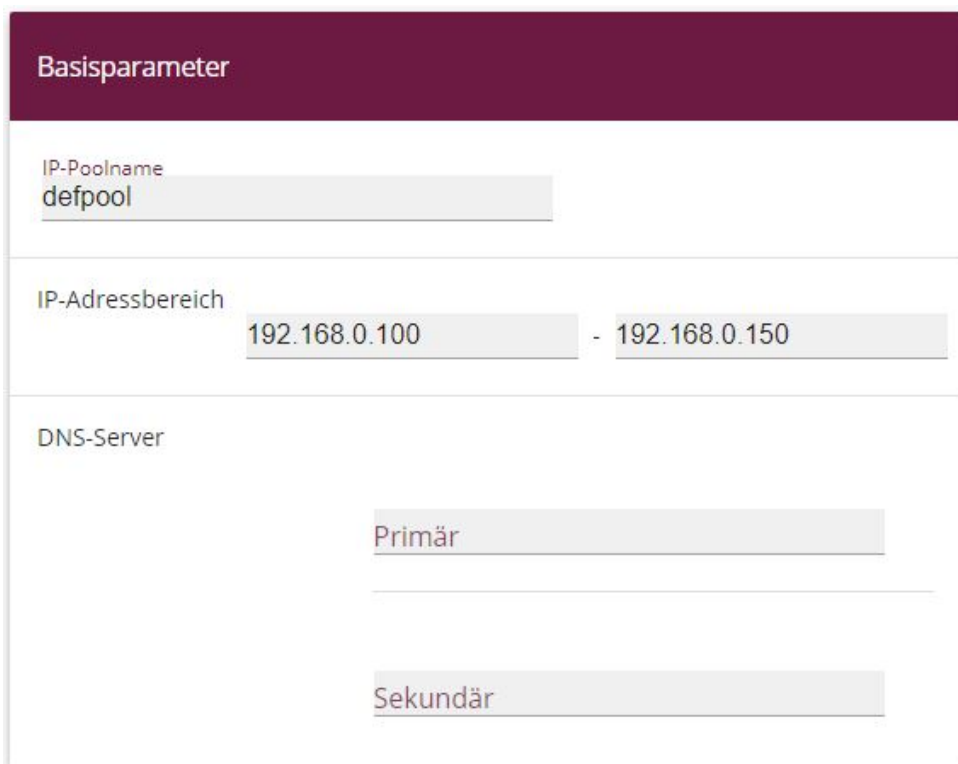


#### Hinweis

Diesen Konfigurationsschritt nur ausführen, wenn in Ihrem lokalen Netzwerk kein weiterer DHCP-Server existiert. In diesem Fall tragen Sie die LAN IP-Adresse des Routers als **Router** auf dem DHCP-Server ein. In unserem Beispiel ist die LAN IP-Adresse des **bintec be.IP** `192.168.0.251`.

Ist kein DHCP-Server in Ihrem lokalen Netzwerk vorhanden, gehen Sie wie folgt vor:

- (1) Gehen Sie zu **Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu**.



The screenshot shows a web-based configuration interface for a DHCP server. The title bar is dark red and contains the text "Basisparameter". Below this, there are three main sections:

- IP-Poolname:** A text input field containing the value "defpool".
- IP-Adressbereich:** Two text input fields separated by a hyphen. The first field contains "192.168.0.100" and the second field contains "192.168.0.150".
- DNS-Server:** Two text input fields. The top field is labeled "Primär" and the bottom field is labeled "Sekundär". Both fields are currently empty.

Abb. 24: Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu

Gehen Sie folgendermaßen vor, um ein IP-Adress-Pool einzurichten:

- (1) Bei **IP-Poolname** geben Sie eine beliebige Beschreibung ein, um den Pool eindeutig zu benennen, z. B. *defpool* aus.
- (2) Geben Sie einen **IP-Adressbereich** an. In unserem Beispiel ist ein IP-Adressbereich von *192.168.0.100* bis *192.168.0.150* konfiguriert.
- (3) Bestätigen Sie Ihre Angaben mit **OK**.



#### Hinweis

Der IP-Adressbereich muss innerhalb des auf der LAN-Schnittstelle konfigurierten IP-Netzbereiches liegen.

Gehen Sie zu **Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu**.

**Basisparameter**

Schnittstelle	en1-0 ▼
IP-Poolname	defpool ▼
Pool-Verwendung	Lokal ▼
<b>Beschreibung</b>	

Abb. 25: **Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu**

Gehen Sie folgendermaßen vor, um ein DHCP-Pool einzurichten:

- (1) Bei **Schnittstelle** wählen Sie die logische Schnittstelle *en1-0* aus.
- (2) Wählen Sie den im Menü **IP-Pool-Konfiguration** konfigurierten **IP-Poolnamen** aus. In unserem Beispiel *defpool*.
- (3) Unter **Pool-Verwendung** wählen Sie *Lokal* aus.
- (4) Bestätigen Sie Ihre Angaben mit **OK**.

### 3.2.4 Bootfähige Sicherung der Konfiguration

Die Konfiguration ist hiermit abgeschlossen. Die Internet Datenverbindung sowie der Empfang der IPTV Daten sollte bei richtigem Anschluss der Endgeräte einwandfrei funktionieren. Zur bootfähigen Sicherung der Konfiguration verlassen Sie das **GUI** mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

## 3.3 Konfigurationsschritte im Überblick

### Verbindungstyp auswählen

Feld	Menü	Wert
<b>Verbindungstyp</b>	<b>Assistenten -&gt; Internet -&gt; Internetverbindungen</b>	<i>Externes xDSL-Modem</i>

### Internetverbindung einrichten

Feld	Menü	Wert
Beschreibung	Assistenten -> Internet -> Internetverbindungen -> Weiter	z. B. <i>Internet-Daten</i>
Physischer Ethernet-Port	Assistenten -> Internet -> Internetverbindungen -> Weiter	<i>ETH5</i>
Typ	Assistenten -> Internet -> Internetverbindungen -> Weiter	<i>Vordefiniert</i>
Land	Assistenten -> Internet -> Internetverbindungen -> Weiter	z. B. <i>Germany</i>
Internet Service Provider	Assistenten -> Internet -> Internetverbindungen -> Weiter	z. B. <i>Telekom - VDSL</i>
Anschlusskennung	Assistenten -> Internet -> Internetverbindungen -> Weiter	z. B. <i>012345678945</i>
Zugangsnummer	Assistenten -> Internet -> Internetverbindungen -> Weiter	z. B. <i>955012345678</i>
Mitbenutzernummer	Assistenten -> Internet -> Internetverbindungen -> Weiter	<i>0001</i>
Persönliches Kennwort	Assistenten -> Internet -> Internetverbindungen -> Weiter	z. B. <i>geheim</i>
Immer aktiv	Assistenten -> Internet -> Internetverbindungen -> Weiter	<i>Aktiviert</i>

#### Konfiguration der VLAN-Schnittstelle

Feld	Menü	Wert
Basierend auf Ethernet-Schnittstelle	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>en1-4</i>
Schnittstellenmodus	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>Tagged (VLAN)</i>
VLAN-ID	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>8</i>
Adressmodus	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>DHCP</i>
DHCP Broadcast Flag	LAN -> IP-Konfiguration -> Schnittstellen -> Neu -> Erweiterte Einstellungen	Deaktiviert

#### IGMP-Proxy konfigurieren

Feld	Menü	Wert
Schnittstelle	Multicast -> IGMP-> IGMP -> Neu	<i>LAN_EN1-0</i>

Feld	Menü	Wert
Modus	Multicast -> IGMP-> IGMP -> Neu	<i>Routing</i>
IGMP Proxy	Multicast -> IGMP-> IGMP -> Neu -> Erweiterte Einstellungen	<i>Aktiviert</i>
Proxy-Schnittstelle	Multicast -> IGMP-> IGMP -> Neu -> Erweiterte Einstellungen	<i>LAN_EN1-4-1</i>

#### Multicast Routing Funktion aktivieren

Feld	Menü	Wert
IGMP-Status	Multicast-> IGMP -> Optionen	<i>Aktiv</i> oder <i>Auto</i>

#### NAT aktivieren

Feld	Menü	Wert
Schnittstelle LAN_EN1-4-1	Netzwerk -> NAT -> NAT-Schnittstellen	NAT aktiv <i>Aktiviert</i>

#### DHCP IP-Adress-Pool konfigurieren

Feld	Menü	Wert
IP-Poolname	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	z. B. <i>defpool</i>
IP-Adressbereich	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	z. B. <i>192.168.0.100 - 192.168.0.150</i>

#### DHCP konfigurieren

Feld	Menü	Wert
Schnittstelle	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>en1-0</i>
IP-Poolname	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	z. B. <i>defpool</i>
Pool-Verwendung	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>Lokal</i>

## Kapitel 4 IP - Routing-Protokoll RIPv2 über IP-Sec-Verbindung

### 4.1 Einleitung

Die vorliegende Lösung zeigt die Vernetzung zweier Standorte über eine IPsec-Verbindung, bei dem das Routingprotokoll RIPv2 zur Übermittlung der in den beiden Standorten konfigurierten IP-Netzbereiche genutzt wird. Der Einsatz eines Routing-Protokolls ist besonders bei komplexeren Netzstrukturen von Vorteil (mehrere IP-Netzbereiche), da Änderungen in der Netzstruktur automatisch über das Routing-Protokoll an alle beteiligten Router im Netz propagiert werden. Das folgende Beispiel soll die Wirkungsweise kurz erläutern.

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

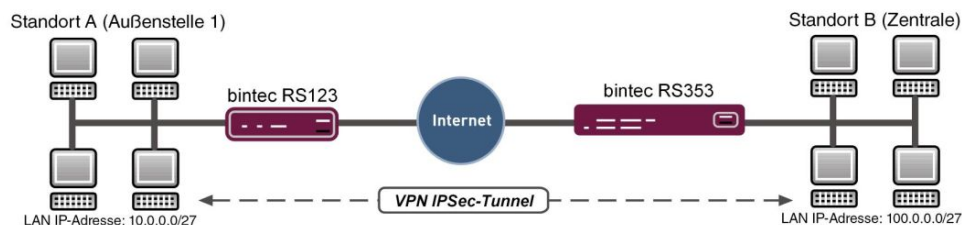


Abb. 26: Beispielszenario

In unserem Beispiel soll nun ein weiteres Netzwerk am Standort A hinzugefügt werden. Bei statisch konfiguriertem Routing hätte dies zur Folge, dass die Konfiguration der VPN-Gateways an beiden Standorten angepasst werden müßte. Bei der Nutzung eines Routing-Protokolls entfällt dies. Konfiguriert muss in diesem Fall nur das Standort A VPN-Gateway. Konkret muss der Administrator nur das Netzwerk auf der LAN-Schnittstelle des Standort A VPN-Gateways konfigurieren. Alles weitere wird vom Routing-Protokoll übernommen.

Die VPN-Gateways unterstützen die Verwendung von Routing-Protokollen auch in Verbindung mit IPsec-Verbindungen. Der folgende Workshop soll dies anhand eines konkreten Beispiels verdeutlichen.

### Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein VPN-Gateway der **bintec RS353**-Serie in der Zentrale

- Ein VPN-Gateway der **bintec RS123**-Serie in der Außenstelle
- Ein Bootimage der Version 10.1.9 auf beiden Gateways
- Beide Gateways benötigen eine unabhängige Verbindung zum Internet

## Hinweise zum Test-Setup

### RS123 Standort A (Außenstelle):

System-Name	RS123-Außenstelle-1 (wird als lokale IPSec-Peer-ID verwendet)
LAN IP-Adresse	10.0.0.30
LAN IP-Subnetzmaske	255.255.255.224
Öffentliche Internet IP-Adresse	62.146.1.1 (hier kann auch ein Hostname verwendet werden)
Standard Gateway IP-Adresse	62.146.1.2
Lokale IP-Adresse der IPSec-Schnittstelle	1.0.0.1 (Wichtig: Diese IP-Adresse muß eindeutig sein, d.h. darf nicht im LAN-IP-Adressbereich der Standorte liegen.)

### RS353 Standort B (Zentrale):

System-Name	RS353-Zentrale (wird als lokale IPSec-Peer-ID verwendet)
LAN IP-Adresse	100.0.0.30
LAN IP-Subnetzmaske	255.255.255.224
Öffentliche Internet IP-Adresse	62.147.1.1 (hier kann auch ein Hostname verwendet werden)
Standard Gateway IP-Adresse	62.147.1.2
Lokale IP-Adresse der IPSec-Schnittstelle	1.0.0.2 (Wichtig: Diese IP-Adresse muß eindeutig sein, d.h. darf nicht im LAN-IP-Adressbereich der Standorte liegen.)

## 4.2 Konfiguration

### 4.2.1 Konfiguration des bintec RS353 am Standort B (Zentrale)

#### Konfiguration der IPSec-Verbindung

Richten Sie zuerst eine neue Verbindung ein. Im Beispiel werden die IPSec Phase 1 / IP-

Sec Phase 2 Standard-Profil verwendet.

Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **VPN -> IPsec -> IPsec-Peers -> Neu**.

Peer-Parameter	IPv4-Schnittstellenrouten						
Administrativer Status <input checked="" type="radio"/> Aktiv <input type="radio"/> Inaktiv	Sicherheitsrichtlinie <input type="radio"/> Nicht Vertrauenswürdig <input checked="" type="radio"/> Vertrauenswürdig						
Beschreibung Außenstelle-1	IPv4-Adressvergabe <input type="text" value="Statisch"/>						
Peer-Adresse IP-Version <input type="text" value="IPv4 bevorzugt"/> 62.146.1.1	Standardroute <input type="checkbox"/>						
Peer-ID Fully Qualified Domain Name (FQDN) RS123-Außenstelle-1	Lokale IP-Adresse 1.0.0.2						
IKE (Internet Key Exchange) <input type="text" value="IKEv1"/>	Routeneinträge						
Preshared Key *****	<table border="1"> <thead> <tr> <th>Entfernte IP-Adresse</th> <th>Netzmaske</th> <th>Metrik</th> </tr> </thead> <tbody> <tr> <td>1.0.0.1</td> <td>255.255.255.255</td> <td>1</td> </tr> </tbody> </table>	Entfernte IP-Adresse	Netzmaske	Metrik	1.0.0.1	255.255.255.255	1
Entfernte IP-Adresse	Netzmaske	Metrik					
1.0.0.1	255.255.255.255	1					
IP-Version des Tunnelnetzwerks <input type="text" value="IPv4"/>	HINZUFÜGEN						

#### Erweiterte Einstellungen

Erweiterte IPsec-Optionen	Erweiterte IP-Optionen
Phase-1-Profil <input type="text" value="Keines (Standardprofil verwenden)"/>	Öffentliche Schnittstelle <input type="text" value="Vom Routing ausgewählt"/>
Phase-2-Profil <input type="text" value="Keines (Standardprofil verwenden)"/>	Öffentliche IPv4-Quelladresse <input type="checkbox"/>
XAUTH-Profil <input type="text" value="Eines auswählen"/>	Öffentliche IPv6-Quelladresse <input type="checkbox"/>
Anzahl erlaubter Verbindungen <input checked="" type="radio"/> Ein Benutzer <input type="radio"/> Mehrere Benutzer	Überprüfung der IPv4-Rückroute <input type="checkbox"/>
Startmodus <input type="radio"/> Auf Anforderung <input checked="" type="radio"/> Immer aktiv	IPv4 Proxy ARP <input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv

Abb. 28: **VPN -> IPsec -> IPsec-Peers -> Neu**

Gehen Sie folgendermaßen vor um eine neue Verbindung hinzuzufügen:

- (1) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Außenstelle-1*.
- (2) Bei **Peer-Adresse** geben Sie die öffentliche Internet IP-Adresse ein, z. B. *62.146.1.1*.
- (3) Bei **Peer-ID** geben Sie die ID des Peers ein, z. B. *RS123-Außenstelle-1*.
- (4) Im **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung, z. B. *test* ein.
- (5) Die **Lokale IP-Adresse** legt die IP-Adresse der IPsec-Schnittstelle fest, hier z. B. *1.0.0.2*.



**Hinweis**

Tragen Sie hier NICHT die LAN-IP-Adresse des **bintec RS353** ein, sondern verwenden Sie eine IP-Adresse die NICHT im LAN-IP-Adressbereich eines Standortes liegt.

- (6) Als **Routeneintrag** ist die Lokale IP-Adresse der IPsec-Schnittstelle der Außenstelle zu konfigurieren, hier z. B. `1.0.0.1`. Die Subnetmaske kann in diesem Fall `255.255.255.255` sein (Hostroute).

**Hinweis**

Tragen Sie hier NICHT die eigentlichen Netzwerkrouten zum Erreichen des entfernten Standortes ein. Das Anlegen der Netzwerkrouten die zum Erreichen der jeweiligen Standorte notwendig sind wird in unserem Fall vom Routingprotokoll RIP übernommen.

- (7) Der **Startmodus** muss auf *Immer aktiv* konfiguriert sein. In diesem Modus wird die IPsec-Verbindung immer automatisch aufgebaut, das heißt, die Verbindung ist immer aktiv. Dies ist notwendig, damit RIP die Routen zum jeweiligen Nachbar-Gateway übertragen kann.
- (8) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

**Anpassen des Phase-1-Profiles**

Zur Konfiguration des Phase-1-Profiles öffnen Sie das als Standard gekennzeichnetes Profil aus.

- (1) Gehen Sie zu **VPN -> IPsec -> Phase-1-Profile** -> .

### Phase-1-Parameter (IKE)

Beschreibung  
Multi-Proposal

Proposals

Verschlüsselung	Authentifizierung	Aktiviert
AES ▼	SHA1 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input checked="" type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>

DH-Gruppe 5(1536 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  
RS353-Zentrale

Abb. 29: VPN -> IPsec -> Phase-1-Profil -> ✎

Gehen Sie folgendermaßen vor:

- (1) Bei **Lokaler ID-Wert** geben Sie die ID Ihres Geräts ein, hier z. B. *RS353-Zentrale*.
- (2) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

### Konfiguration des Routing Protokolls RIP für die IPsec-Schnittstelle

Im Menü RIP-Schnittstellen wird das Routing-Protokoll konfiguriert.

- (1) Gehen Sie zu **Routing-Protokolle -> RIP -> RIP-Schnittstellen -><Außenstelle-1>** .



The screenshot shows the configuration page for RIP on the interface 'Außenstelle-1'. It features three dropdown menus:

- Version in Senderrichtung:** Set to 'RIP V2 Multicast'.
- Version in Empfangsrichtung:** Set to 'RIP V2'.
- Routenankündigung:** Set to 'Nur aktiv'.

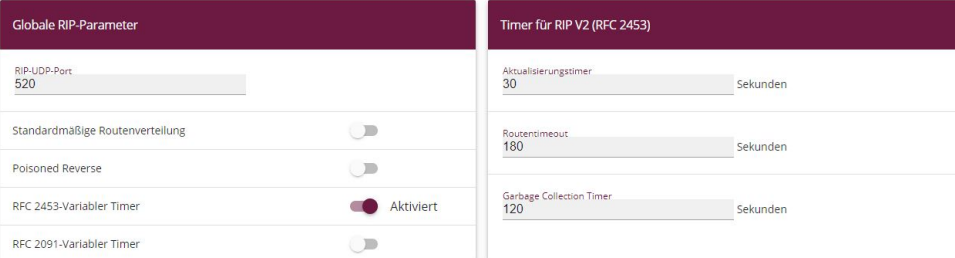
Abb. 30: **Routing-Protokolle -> RIP -> RIP-Schnittstellen -><Außenstelle-1>** 

Gehen Sie folgendermaßen vor:

- (1) Für die **Version in Senderrichtung** wählen Sie *RIP V2 Multicast* aus. Die RIP-Protokoll-Pakete verwenden als Zieladresse die Multicast-Adresse *224.0.0.9*. Sie können hier auch andere RIP-Varianten verwenden. Wichtig ist nur, dass die verwendete RIP-Version (RIPv1/RIPv2) auf beiden VPN-Gateways identisch ist.
- (2) Für die **Version in Empfangsrichtung** wählen Sie *RIP V2* aus.
- (3) Bei **Routenankündigung** wählen Sie *Nur aktiv* aus.
- (4) Bestätigen Sie Ihre Eingaben mit **OK**.

Im letzten Schritt der Konfiguration wird die Verteilung der Standardroute deaktiviert.

- (1) Gehen Sie zu **Routing-Protokolle -> RIP -> RIP-Optionen**.



The screenshot shows the 'RIP-Optionen' configuration page, divided into two sections:

- Globale RIP-Parameter:**
  - RIP-UDP-Port: 520
  - Standardmäßige Routenverteilung:
  - Poisoned Reverse:
  - RFC 2453-Variabler Timer:  Aktiviert
  - RFC 2091-Variabler Timer:
- Timer für RIP V2 (RFC 2453):**
  - Aktualisierungstimer: 30 Sekunden
  - Routenzeitout: 180 Sekunden
  - Garbage Collection Timer: 120 Sekunden

Abb. 31: **Routing-Protokolle -> RIP -> RIP-Optionen**

Gehen Sie folgendermaßen vor:

- (1) Deaktivieren Sie den Parameter **Standardmäßige Routenverteilung**. Hiermit wird verhindert, dass die konfigurierte Standard-Route über RIP propagiert wird.
- (2) Bestätigen Sie mit **OK**.

Hiermit ist die Konfiguration des **bintec RS353**-Gateways abgeschlossen.

## 4.2.2 Konfiguration des bintec RS123 am Standort A (Außenstelle)

### Konfiguration der IPsec-Verbindung

Richten Sie zuerst eine neue Verbindung ein. Im Beispiel werden die IPsec Phase 1 / IPsec Phase 2 Standard-Profile verwendet.

Gehen Sie dazu in folgendes Menü:

- (1) Gehen Sie zu **VPN -> IPsec -> IPsec-Peers -> Neu**.

The screenshot displays the configuration interface for an IPsec peer and its associated routes. It is divided into several sections:

- Peer-Parameter:**
  - Administrativer Status:  Aktiv  Inaktiv
  - Beschreibung: Zentrale
  - Peer-Adresse: IP-Version | IPv4 bevorzugt, 62.147.1.1
  - Peer-ID: Fully Qualified Domain Name (FQDN), RS353-Zentrale
  - IKE (Internet Key Exchange): IKEv1
  - Preshared Key: \*\*\*\*\*
  - IP-Version des Tunnelnetzwerks: IPv4
- IPv4-Schnittstellenrouten:**
  - Sicherheitsrichtlinie:  Nicht Vertrauenswürdig  Vertrauenswürdig
  - IPv4-Adressvergabe: Statisch
  - Standardroute:
  - Lokale IP-Adresse: 1.0.0.1
  - Routeneinträge:
    - Entfernte IP-Adresse: 1.0.0.2
    - Netzmaske: 255.255.255.255
    - Metrik: 1
  - HINZUFÜGEN
- Erweiterte Einstellungen:**
  - Erweiterte IPsec-Optionen:**
    - Phase-1-Profil: Keines (Standardprofil verwenden)
    - Phase-2-Profil: Keines (Standardprofil verwenden)
    - XAUTH-Profil: Eines auswählen
    - Anzahl erlaubter Verbindungen:  Ein Benutzer  Mehrere Benutzer
    - Startmodus:  Auf Anforderung  Immer aktiv
    - Backup Peer: Keiner
  - Erweiterte IP-Optionen:**
    - Öffentliche Schnittstelle: Vom Routing ausgewählt
    - Öffentliche IPv4-Quelladresse:
    - Öffentliche IPv6-Quelladresse:
    - Überprüfung der IPv4-Rückroute:
    - IPv4 Proxy ARP:  Inaktiv  Aktiv oder Ruhend  Nur aktiv

Abb. 33: VPN -> IPsec -> IPsec-Peers -> Neu

Gehen Sie folgendermaßen vor um eine neue Verbindung hinzuzufügen:

- (1) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Zentrale*.
- (2) Bei **Peer-Adresse** geben Sie die öffentliche Internet IP-Adresse ein, z. B. *62.147.1.1*.
- (3) Bei **Peer-ID** geben Sie die ID des Peers ein, z. B. *RS353-Zentrale*.
- (4) Im **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung, z. B. *test* ein.
- (5) Die **Lokale IP-Adresse** legt die IP-Adresse der IPSec-Schnittstelle fest, hier z. B. *1.0.0.1*.



#### Hinweis

Tragen Sie hier NICHT die LAN-IP-Adresse des **bintec RS123** ein, sondern verwenden Sie eine IP-Adresse die NICHT im LAN-IP-Adressbereich eines Standortes liegt.

- (6) Als **Routeneintrag** ist die Lokale IP-Adresse der IPSec-Schnittstelle der Zentrale zu konfigurieren, hier z. B. *1.0.0.2*. Die Subnetmask kann in diesem Fall *255.255.255.255* sein (Hostroute).



#### Hinweis

Tragen Sie hier NICHT die eigentlichen Netzwerkrouen zum Erreichen des entfernten Standortes ein. Das Anlegen der Netzwerkrouen die zum Erreichen der jeweiligen Standorte notwendig sind wird in unserem Fall vom Routingprotokoll RIP übernommen.

- (7) Der **Startmodus** muss auf *Immer aktiv* konfiguriert sein. In diesem Modus wird die IPSec-Verbindung immer automatisch aufgebaut, das heißt, die Verbindung ist immer aktiv. Dies ist notwendig, damit RIP die Routen zum jeweiligen Nachbar-Gateway übertragen kann.
- (8) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

### Anpassen des Phase-1-Profiles

Zur Konfiguration des Phase-1-Profiles öffnen Sie das als Standard gekennzeichnetes Profil aus.

- (1) Gehen Sie zu **VPN -> IPSec -> Phase-1-Profile** -> .

### Phase-1-Parameter (IKE)

Beschreibung  
Multi-Proposal

Proposals

Verschlüsselung	Authentifizierung	Aktiviert
AES	SHA1	<input type="checkbox"/>
AES	MD5	<input checked="" type="checkbox"/>
3DES	MD5	<input checked="" 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  
RS123-Aussenstelle-1

Abb. 34: VPN -> IPsec -> Phase-1-Profil -> 

Gehen Sie folgendermaßen vor:

- (1) Bei **Lokaler ID-Wert** geben Sie die ID Ihres Geräts ein, hier z. B. *RS123-Außenstelle-1*.
- (2) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.


## Konfiguration des Routing Protokolls RIP für die IPsec-Schnittstelle

Im Menü RIP-Schnittstellen wird das Routing-Protokoll konfiguriert.

- (1) Gehen Sie zu **Routing-Protokolle** -> **RIP** -> **RIP-Schnittstellen** -><Zentrale> .

RIP-Parameter für: Zentrale

Version in Senderichtung	RIP V2 Multicast ▾
Version in Empfangsrichtung	RIP V2 ▾
Routenankündigung	Aktiv oder Ruhend ▾

Abb. 35: **Routing-Protokolle** -> **RIP** -> **RIP-Schnittstellen** -><Zentrale> 

Gehen Sie folgendermaßen vor:

- (1) Für die **Version in Senderichtung** wählen Sie *RIP V2 Multicast* aus. Die RIP-Protokoll-Pakete verwenden als Zieladresse die Multicast-Adresse *224.0.0.9*. Sie können hier auch andere RIP-Varianten verwenden. Wichtig ist nur, dass die verwendete RIP-Version (RIPv1/RIPv2) auf beiden VPN-Gateways identisch ist.
- (2) Für die **Version in Empfangsrichtung** wählen Sie *RIP V2* aus.
- (3) Bei **Routenankündigung** wählen Sie *Aktiv oder Ruhend* aus.
- (4) Bestätigen Sie Ihre Eingaben mit **OK**.

Im letzten Schritt der Konfiguration wird die Verteilung der Standardroute deaktiviert.

- (1) Gehen Sie zu **Routing-Protokolle** -> **RIP** -> **RIP-Optionen**.

Globale RIP-Parameter	Timer für RIP V2 (RFC 2453)
RIP-UDP-Port 520	Aktualisierungstimer 30 Sekunden
Standardmäßige Routenverteilung <input type="checkbox"/>	Routenzeitout 180 Sekunden
Poisoned Reverse <input type="checkbox"/>	Garbage Collection Timer 120 Sekunden
RFC 2453-Variabler Timer <input checked="" type="checkbox"/> Aktiviert	
RFC 2091-Variabler Timer <input type="checkbox"/>	

Abb. 36: **Routing-Protokolle** -> **RIP** -> **RIP-Optionen**

Gehen Sie folgendermaßen vor:

- (1) Deaktivieren Sie den Parameter **Standardmäßige Routenverteilung**. Hiermit wird verhindert, dass die konfigurierte Standard-Route über RIP propagiert wird.
- (2) Bestätigen Sie mit **OK**.

Hiermit ist die Konfiguration des **bintec RS123**-Gateways abgeschlossen.

### 4.3 Kontrolle der Funktion

Wenn Ihre Internetverbindung funktioniert sowie die Einstellungen gemäß Anleitung richtig vorgenommen wurden sollte die Standortverbindung hiermit funktionieren.

Zur Kontrolle gehen Sie in das Menü **Netzwerk -> Routen -> IPV4-Routing-Tabelle**.

Hier sehen Sie auf beiden VPN-Gateways die Netzwerkrouuten zum Erreichen des jeweiligen Standortes. Die über **RIP** propagierten Routen sind mit Protokoll *RIP* in der Tabelle gekennzeichnet.

Ergebnis: Standort B (Zentrale)

Routen								
Ziel-IP-Adresse	Netzmaske	Gateway	Schnittstelle	Metrik	Routentyp	Erweiterte Route	Protokoll	
1.0.0.1	255.255.255.255	1.0.0.2	IPSEC_AUSSENSTELLE-1	1	Host-Route über Schnittstelle	<input type="checkbox"/>	Lokal	
62.146.1.0	255.255.255.252	1.0.0.1	IPSEC_AUSSENSTELLE-1	1	Host-Route über Schnittstelle	<input type="checkbox"/>	RIP	
62.147.1.0	255.255.255.252	62.147.1.1	LAN_EN1-4	0	Netzwerkroute via Schnittstelle	<input type="checkbox"/>	Lokal	
10.0.0.0	255.255.255.224	1.0.0.1	IPSEC_AUSSENSTELLE-1	1	Host-Route über Schnittstelle	<input type="checkbox"/>	RIP	
100.0.0.0	255.255.255.224	100.0.0.30	LAN_EN1-0	0	Host-Route über Schnittstelle	<input type="checkbox"/>	Lokal	
0.0.0.0	0.0.0.0	62.147.1.2	LAN_EN1-4	1	Netzwerkroute via Schnittstelle	<input type="checkbox"/>	Lokal	

Abb. 37: **Netzwerk -> Routen -> IPV4-Routing-Tabelle**

Ergebnis: Standort A (Außenstelle)



Routen									
Ziel-IP-Adresse	Netzmaske	Gateway	Schnittstelle	Metrik	Routentyp	Erweiterte Route	Protokoll		
1.0.0.2	255.255.255.255	1.0.0.1	IPSEC_ZENTRALE	1	Host-Route über Schnittstelle	<input type="checkbox"/>	Lokal		
62.146.1.0	255.255.255.252	62.146.1.1	LAN_EN1-4	0	Host-Route über Schnittstelle	<input type="checkbox"/>	Lokal		
62.147.1.0	255.255.255.252	1.0.0.2	IPSEC_ZENTRALE	1	Netzwerkroute via Schnittstelle	<input type="checkbox"/>	RIP		
10.0.0.0	255.255.255.224	10.0.0.30	LAN_EN1-0	0	Host-Route über Schnittstelle	<input type="checkbox"/>	Lokal		
100.0.0.0	255.255.255.224	1.0.0.2	IPSEC_ZENTRALE	1	Host-Route über Schnittstelle	<input type="checkbox"/>	RIP		
0.0.0.0	0.0.0.0	62.146.1.2	LAN_EN1-4	1	Netzwerkroute via Schnittstelle	<input type="checkbox"/>	Lokal		

Abb. 38: Netzwerk -> Routen -> IPV4-Routing-Tabelle

Jede Änderung der LAN IP-Konfiguration wirkt sich nun automatisch auf die Routing-Einträge der beiden VPN-Gateways aus.

## 4.4 Konfigurationsschritte im Überblick




### IPsec-Verbindung konfigurieren (Zentrale)

Feld	Menü	Wert
Beschreibung	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. <i>Aussenstelle-1</i>
Peer-Adresse	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. <i>62.146.1.1</i>
Peer-ID	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. <i>RS123-Aussenstelle-1</i>
Preshared Key	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. <i>test</i>
Lokale IP-Adresse	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. <i>1.0.0.2</i>
Routeneinträge	VPN -> IPsec -> IPsec-Peers -> Neu	<i>1.0.0.1</i> und <i>255.255.255.255</i>
Startmodus	VPN -> IPsec -> IPsec-Peers -> Neu	<i>Immer aktiv</i>

### Phase-1-Profil anpassen

Feld	Menü	Wert
Lokaler ID-Wert	VPN -> IPsec -> Phase-1-Profile ->	z. B. <i>RS353-Zentrale</i>

### Routing-Protokoll konfigurieren

Feld	Menü	Wert
Version in Sende- richtung	Routing-Protokolle -> RIP -> RIP- Schnittstellen -><Außenstelle-1> 	RIP V2 Multicast
Version in Emp- fangsrichtung	Routing-Protokolle -> RIP -> RIP- Schnittstellen -><Außenstelle-1> 	RIP V2
Routenankündi- gung	Routing-Protokolle -> RIP -> RIP- Schnittstellen -><Außenstelle-1> 	Nur aktiv


#### RIP-Optionen einstellen

Feld	Menü	Wert
Standardmäßige Routenverteilung	Routing-Protokolle -> RIP -> RIP- Optionen	Deaktiviert

#### IPsec-Verbindung konfigurieren (Außenstelle)

Feld	Menü	Wert
Beschreibung	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. Zentrale
Peer-Adresse	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. 62.147.1.1
Peer-ID	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. RS353-Zentrale
Preshared Key	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. test
Lokale IP-Adresse	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. 1.0.0.1
Routeneinträge	VPN -> IPsec -> IPsec-Peers -> Neu	1.0.0.2 und 255.255.255.255
Startmodus	VPN -> IPsec -> IPsec-Peers -> Neu	Immer aktiv

#### Phase-1-Profil anpassen

Feld	Menü	Wert
Lokaler ID-Wert	VPN -> IPsec -> Phase-1-Profile -> 	z. B. RS123-Aussenstelle -1

#### Routing-Protokoll konfigurieren

Feld	Menü	Wert
Version in Sende- richtung	Routing-Protokolle -> RIP -> RIP- Schnittstellen -><Zentrale> 	RIP V2 Multicast
Version in Emp- fangsrichtung	Routing-Protokolle -> RIP -> RIP- Schnittstellen -><Zentrale> 	RIP V2
Routenankündi- gung	Routing-Protokolle -> RIP -> RIP- Schnittstellen -><Zentrale> 	Aktiv oder Ruhend

**RIP-Optionen einstellen**

<b>Feld</b>	<b>Menü</b>	<b>Wert</b>
<b>Standardmäßige Routenverteilung</b>	<b>Routing-Protokolle -&gt; RIP -&gt; RIP- Optionen</b>	<i>Deaktiviert</i>

## Kapitel 5 IP - Lastverteilung von zwei parallel genutzten Internetzugängen

### 5.1 Einleitung

Der folgende Workshop zeigt die Konfiguration eines Internet Zugangs-Gateways mit zwei parallel genutzten Internetzugängen. Die erste ADSL-Leitung wird mit dem integrierten ADSL-Modem des hier genutzten **bintec be.IP plus** hergestellt. Für den Aufbau der zweiten ADSL-Leitung wird ein externes ADSL-Modem an dem ETH5 Port des **bintec be.IP plus** angebunden. Der Datenverkehr wird auf Basis von IP-Sitzungen jeweils zur Hälfte auf die beiden ADSL-Leitungen verteilt. Desweiteren wird am Beispiel von verschlüsselten HTTP-Verbindungen (HTTPS) beschrieben wie Verbindungsabbrüche, welche durch die Verteilung auf verschiedene Internetzugänge auftreten können, wirkungsvoll vermieden werden.

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

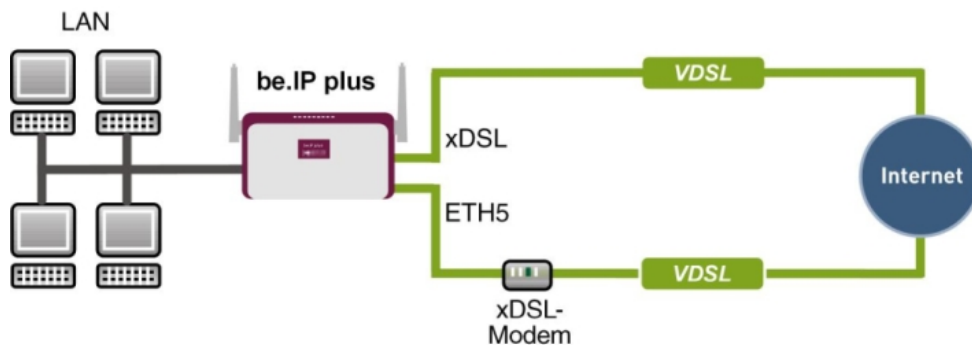


Abb. 39: Beispielszenario

### Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein bintec ADSL-Gateway z. B. **bintec be.IP plus** mit Systemsoftware 10.1.5 Patch 6
- Zwei unabhängige ADSL-Internetverbindungen
- Ein externes ADSL-Modem welches an dem ETH5 Port des **bintec be.IP plus** angebunden ist

## 5.2 Konfiguration

### 5.2.1 Konfiguration der Internetzugänge

Zur Konfiguration öffnen Sie einen Internet Browser und starten eine Web (HTTP)-Verbindung zum **bintec be.IP plus**. Zur Konfiguration der beiden Internetzugänge verfügt das **GUI** über einen Assistenten.

Gehen Sie dazu in folgendes Menü:

- (1) Gehen Sie zu **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu**.
- (2) Wählen Sie bei **Verbindungstyp** *Internes ADSL-Modem* aus.
- (3) Klicken Sie auf **Weiter** um eine neue Internetverbindung zu konfigurieren.
- (4) Geben Sie die erforderlichen Daten für die Verbindung ein.

The screenshot shows a configuration assistant with four main sections:

- Grundeinstellungen**: A section with a header bar. Below it, the label "Beschreibung" is followed by a text input field containing "ADSL-1".
- Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:**: A section with a header bar and a help icon. Below it, the label "Typ" is followed by a radio button labeled "Benutzerdefiniert" which is selected. Below the radio button is a dropdown menu showing "VDSL/ADSL auto - PPPoE (PPP über Ethernet)".
- Wird die Konfiguration eines VLAN vom ISP angefordert (z. B. mit VDSL-Modem):**: A section with a header bar and a help icon. Below it, the label "VLAN" is followed by a toggle switch that is currently turned off.
- Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:**: A section with a header bar and a help icon. Below it, there are two input fields: "Benutzername" with the value "feste\_ip@provider.de" and "Persönliches Kennwort" with a masked password "\*\*\*\*\*".

Abb. 40: **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu** -> **Weiter**

Gehen Sie folgendermaßen vor, um einen Internetzugang zu konfigurieren:

- (1) Bei **Beschreibung** tragen Sie z. B. *ADSL-1* ein.
- (2) Bei **Typ** wählen Sie *Benutzerdefiniert über PPPoE (PPP über Ethernet)*

aus.

- (3) Als **Benutzername** geben Sie den Namen ein, welchen Sie von Ihrem Provider erhalten haben z. B. *feste-ip@provider.de*.
- (4) Geben Sie das **Persönliche Kennwort** ein, welches Sie von Ihrem Provider erhalten haben, z. B. *test12345*.
- (5) Bestätigen Sie Ihre Angaben mit **OK**.

Für die Einrichtung der zweiten ADSL-Verbindung wird der Assistent ein weiteres mal ausgeführt.

- (1) Gehen Sie zu **Assistenten -> Internet -> Internetverbindungen -> Neu**.
- (2) Wählen Sie bei **Verbindungstyp** *Externes xDSL-Modem* aus.
- (3) Klicken Sie auf **Weiter** um eine neue Internetverbindung zu konfigurieren.
- (4) Geben Sie die erforderlichen Daten für die Verbindung ein.

Beschreibung  
ADSL-2

<p>Wählen Sie den physischen Ethernet-Port aus, der mit dem externen xDSL-Modem verbunden ist:</p> <p>Physischer Ethernet-Port <span>ETH5 ▾</span></p>	<p>Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:</p> <p>Typ <span>Benutzerdefiniert ▾</span></p>
<p>Wird die Konfiguration eines VLAN vom ISP angefordert (z. B. mit VDSL-Modem)?</p> <p>VLAN <input type="checkbox"/></p>	<p>Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:</p> <p>Benutzername #0001@t-online.de</p> <p>Persönliches Kennwort *****</p>

Abb. 41: **Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter**



### Hinweis

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

Gehen Sie folgendermaßen vor, um die zweite Internetverbindung zu konfigurieren:

- (1) Bei **Beschreibung** geben Sie eine beliebige Bezeichnung für die Internetverbindung ein, z. B. *ADSL-2* ein.
- (2) Im Menüpunkt **Physischer Ethernet-Port** wählen Sie den physischen Ethernet-Port aus an dem das xDSL-Modem angeschlossen ist, hier *ETH5*.

- (3) Bei **Benutzername** geben Sie die Zugangsdaten ein, die Sie von Ihrem Provider erhalten haben, z. B. `#0001@t-online.de`.
- (4) Geben Sie das **Persönliche Kennwort** ein, das Sie von Ihrem Provider erhalten haben, z. B. `test12345`.
- (5) 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.
- (6) Bestätigen Sie Ihre Angaben mit **OK**.

Nach erfolgter Konfiguration zeigt der Assistent zur Konfiguration von Internetverbindungen zwei Einträge.

- (1) Gehen Sie zu **Assistenten -> Internet -> Internetverbindungen**.

Liste konfigurierter Internetverbindungen:			
Beschreibung	Typ		
ADSL-1	PPP over Ethernet		
ADSL-2	Externes xDSL-Modem		

Abb. 42: **Assistenten -> Internet -> Internetverbindungen**

## 5.2.2 Einrichtung der IP-Lastverteilung

Zur Einrichtung der IP-Lastverteilung muss zunächst eine Lastverteilungsgruppe angelegt werden.

- (1) Gehen Sie zu **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu**.

Basisparameter			
Gruppenbeschreibung	Internetzugang		
Verteilungsrichtlinie	Sitzungs-Round-Robin		
Verteilungsmodus	<input checked="" type="radio"/> Immer <input type="radio"/> Nur aktive Schnittstellen verwenden		
Schnittstellenauswahl für Verteilung			
Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung
HINZUFÜGEN			

Abb. 43: **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu**

Gehen Sie folgendermaßen vor, um eine Lastverteilungsgruppe anzulegen:

- (1) Bei **Gruppenbeschreibung** geben Sie eine Bezeichnung für die Lastverteilungsgruppe ein, z. B. *Internetzugang*.
- (2) Wählen Sie bei **Verteilungsrichtlinie** das Verfahren ein, nach dem die Daten verteilt werden, hier *Sitzungs-Round-Robin* (für eine Lastverteilung Basierend auf IP-Sitzungen).

Anschließend können die beiden ADSL-Internetzugänge zu dieser Lastverteilungsgruppe hinzugefügt werden.

Klicken Sie dazu auf **Hinzufügen**.

The image shows a screenshot of a network configuration interface. It consists of two main sections, each with a dark red header and a white content area.

The first section, titled "Basisparameter", contains two rows of configuration fields:

Gruppenbeschreibung	Internetzugang
Verteilungsrichtlinie	Sitzungs-Round-Robin

The second section, titled "Schnittstellenauswahl für Verteilung", contains two rows of configuration fields:

Schnittstelle	WAN_ADSL-1
Verteilungsverhältnis	50 %

Abb. 44: Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu -> Hinzufügen

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Schnittstelle** den ersten ADSL-Zugang *WAN\_ADSL-1* aus.
- (2) Bei **Verteilungsverhältnis** geben Sie *50 %* ein.
- (3) Klicken Sie auf **Übernehmen**.



- (4) Fügen Sie mit **Hinzufügen** die zweite ADSL-Leitung hinzu.
- (5) Wählen Sie bei **Schnittstelle** den zweiten ADSL-Zugang `WAN_ADSL-2` aus.
- (6) Bei **Verteilungsverhältnis** geben Sie `50 %` ein.
- (7) Klicken Sie auf **Übernehmen**.

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

- (1) Gehen Sie zu **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen**.

**Basisparameter**

Gruppenbeschreibung  
Internetzugang

Verteilungsrichtlinie Sitzungs-Round-Robin ▾

Verteilungsmodus  Immer  Nur aktive Schnittstellen verwenden

**Schnittstellenauswahl für Verteilung**

Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung	
WAN_ADSL-1	50 %	0.0.0.0		🗑️ ✎
WAN_ADSL-2	50 %			🗑️ ✎

**HINZUFÜGEN**

Abb. 45: **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen**

### 5.2.3 Spezielle Lastverteilungs-Behandlung von verschlüsselten Verbindungen

Mit der bis jetzt abgeschlossenen Konfiguration werden IP-Sitzungen jeweils zur Hälfte auf die beiden ADSL-Leitungen verteilt. Durch dieses Verhalten 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 ADSL-Verbindungen. Bei parallelen Verbindungen zum gleichen Server würden beide ADSL-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.

- (1) Gehen Sie zu **Netzwerk -> Lastverteilung -> Special Session Handling -> Neu**.

### Basisparameter

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

Abb. 46: 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**.

Mit dieser Konfiguration werden HTTPS-Verbindungen die von einem lokalen Host an einen gleichen HTTPS Web-Server gesendet werden über einen Zeitraum von 900 Sekunden an eine der beiden ADSL-Leitungen gebunden. Hierdurch bleibt die Absenderadresse der HTTPS-Daten gleich, wodurch Verbindungsabbrüche verhindert werden.

## 5.2.4 Hinweis zur DNS-Server Konfiguration

Beim Aufbau der ADSL-Verbindungen bezieht die **be.IP plus** neben der öffentlichen IP-Adresse auch die IP-Adressen der DNS-Server zur Namensauflösung von dem konfigurierten Internet-Provider. Vor allem bei der Verwendung von unterschiedlichen Internet-Providern müssen die DNS-Server Verbindungsspezifisch verwendet werden. Die folgende Konfiguration wurde beim Anlegen der ADSL-Verbindungen bereits automatisch erstellt.

(1) Gehen Sie zu **Lokale Dienste -> DNS -> DNS-Server**.

Beschreibung	DNS-Server	Priorität	Schnittstellenbeschreibung	Modus	Status
wiz.ADSL-1	P: S:	5	WAN_ADSL-1	Dynamisch	Deaktiviert
wiz.ADSL-2	P: S:	5	WAN_ADSL-2	Dynamisch	Ruhend

Abb. 47: Lokale Dienste -> DNS -> DNS-Server

## 5.3 Konfigurationsschritte im Überblick

### Erste Internetverbindung einrichten

Feld	Menü	Wert
Verbindungstyp	Assistenten -> Internet -> Internetverbindungen -> Neu	Internes ADSL-Modem
Beschreibung	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ADSL-1</i>
Benutzername	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>feste_ip@provider.de</i>
Persönliches Kennwort	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>test12345</i>

### Zweite Internetverbindung einrichten

Feld	Menü	Wert
Verbindungstyp	Assistenten -> Internet -> Internetverbindungen -> Neu	Externes xDSL-Modem
Beschreibung	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ADSL-2</i>

Feld	Menü	Wert
Physischer Ethernet-Port	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ETH5</i>
Benutzername	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>#0001@t-online.de</i>
Persönliches Kennwort	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>test12345</i>

#### Lastverteilungsgruppe anlegen

Feld	Menü	Wert
Gruppenbeschreibung	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	z. B. <i>Internetzugang</i>
Verteilungsrichtlinie	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	<i>Sitzungs-Round-Robin</i>
Schnittstelle	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>WAN_ADSL-1</i>
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>50 %</i>
Schnittstelle	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>WAN_ADSL-2</i>
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>50 %</i>

#### Special Session Handling

Feld	Menü	Wert
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	<i>900 Sekunden</i>

## Kapitel 6 IP - Lastverteilung von zwei VPN IPSec-Tunneln über separate Internetzugänge

### 6.1 Einleitung

Der vorliegende Workshop zeigt die Konfiguration einer VPN IPSec-Vernetzung in Verbindung mit IP-Lastverteilung. Am Standort der Zentrale werden zur Ausfallsicherheit und um eine höhere Bandbreite zu erreichen zwei unabhängige Internetanbindungen gleichzeitig verwendet. Das Gateway am Standort der Filiale ist mit einer ADSL-Leitung an das Internet angebunden und initiiert immer zwei VPN IPSec-Tunnel zum Gateway der Zentrale um dort beide ADSL-Leitungen gleichzeitig zu verwenden. Das Gateway der Zentrale muss durch zwei feste WAN IP-Adressen oder durch die Verwendung von DynDNS (bei dynamischen WAN IP-Adressen) aus dem Internet erreichbar sein. Durch die Konfiguration der IP-Lastverteilung werden Routingkonflikte bei den Internetverbindungen und bei den beiden VPN IPSec-Verbindungen vermieden. Die Tunnelverbindungen werden von beiden VPN-Gateways gegenseitig periodisch überwacht. Beim Ausfall eines Tunnels wird automatisch der komplette Datenverkehr auf den noch funktionierenden VPN-Tunnel gelenkt wird.

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

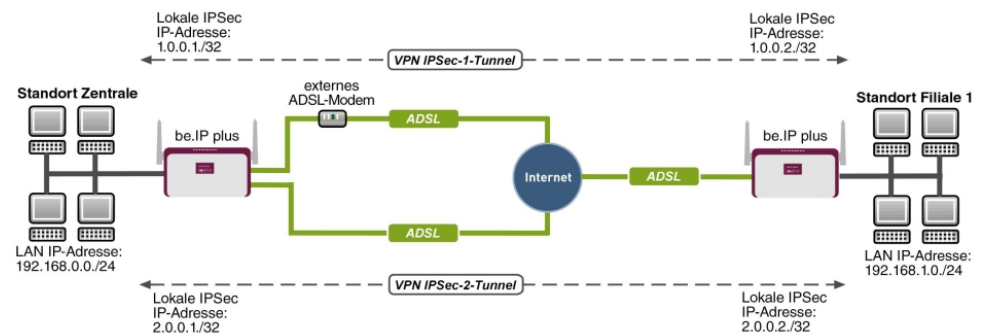


Abb. 48: Beispielszenario

### Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

Standort der Zentrale

- ein bintec VPN-Gateway z. B. **bintec be.IP plus** mit Systemsoftware 10.1.5 Patch 6

- zwei unabhängige ADSL-Internetverbindungen (bei dynamischen WAN IP-Adressen kann mit DynDNS gearbeitet werden)
- ein externes ADSL-Modem welches an dem ETH5 Port des **bintec be.IP plus**-Gateways angebunden ist

Standort der Filiale

- ein bintec VPN-Gateway z. B. **bintec be.IP plus** mit Systemsoftware 10.1.5 Patch 6
- ein ADSL-Internetzugang

## 6.2 Konfiguration

### 6.2.1 Konfiguration des Gateways in der Zentrale

#### Einrichtung der Internetverbindungen

Am Standort der Zentrale werden zur Ausfallsicherheit und um eine höhere Bandbreite zu erreichen zwei ADSL-Internetzugänge parallel verwendet. Diese Internetzugänge werden mit Hilfe des **Assistenten** konfiguriert.

- (1) Gehen Sie zu **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu**.
- (2) Wählen Sie bei **Verbindungstyp** *Internes ADSL-Modem* aus.
- (3) Klicken Sie auf **Weiter** um eine neue Internetverbindung zu konfigurieren.
- (4) Geben Sie die erforderlichen Daten für die Verbindung ein.

Abb. 49: **Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter**

Gehen Sie folgendermaßen vor, um einen Internetzugang zu konfigurieren:

- (1) Bei **Beschreibung** tragen Sie z. B. *ADSL-1* ein.
- (2) Bei **Typ** wählen Sie *Benutzerdefiniert über PPPoE (PPP über Ethernet)* aus.
- (3) Bei **Benutzername** geben Sie den Namen ein, welches Sie von Ihrem Provider erhalten haben z. B. *ADSL-Benutzername*.
- (4) Geben Sie das **Passwort** ein, welches Sie von Ihrem Provider erhalten haben, z. B. *test12345*.
- (5) 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.
- (6) Bestätigen Sie Ihre Angaben mit **OK**.

Für die Einrichtung der zweiten ADSL-Verbindung wird der Assistent ein weiteres mal ausgeführt.

- (1) Gehen Sie zu **Assistenten -> Internet -> Internetverbindungen -> Neu**.
- (2) Wählen Sie bei **Verbindungstyp** *Externes xDSL-Modem* aus.
- (3) Klicken Sie auf **Weiter** um eine neue Internetverbindung zu konfigurieren.

- (4) Geben Sie die erforderlichen Daten für die Verbindung ein.

The screenshot shows a configuration assistant with four panels:

- Panel 1:** "Beschreibung" with the text "ADSL-2".
- Panel 2:** "Wählen Sie den physischen Ethernet-Port aus, der mit dem externen xDSL-Modem verbunden ist:" with a dropdown menu showing "ETH5".
- Panel 3:** "Wird die Konfiguration eines VLAN vom ISP angefordert (z. B. mit VDSL-Modem):" with a toggle switch turned off.
- Panel 4:** "Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:" with fields for "Benutzername" (containing "ADSL-Benutzername2") and "Persönliches Kennwort" (masked with dots).

Abb. 50: **Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter**



### Hinweis

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

Gehen Sie folgendermaßen vor, um die zweite Internetverbindung zu konfigurieren:

- (1) Bei **Beschreibung** geben Sie eine beliebige Bezeichnung für die Internetverbindung ein, z. B. *ADSL-2* ein.
- (2) Im Menüpunkt **Physischer Ethernet-Port** wählen Sie den physikalischen Ethernet-Port aus an dem das xDSL-Modem angeschlossen ist, hier *ETH5*.
- (3) Bei **Benutzername** geben Sie die Zugangsdaten ein, die Sie von Ihrem Provider erhalten haben, z. B. *ADSL-Benutzername2* .
- (4) Geben Sie das **Paswort** ein, das Sie von Ihrem Provider erhalten haben, z. B. *test12345*.
- (5) Bestätigen Sie Ihre Angaben mit **OK**.

Nach erfolgter Konfiguration zeigt der Assistent zur Konfiguration von Internetverbindungen zwei Einträge.

- (1) Gehen Sie zu **Assistenten -> Internet -> Internetverbindungen**.



Liste konfigurierter Internetverbindungen:				
Beschreibung	Typ			
ADSL-1	PPP over Ethernet	⊘	🗑️	✎
ADSL-2	Externes xDSL-Modem	🕒	🗑️	✎

Abb. 51: Assistenten -> Internet -> Internetverbindungen

## Einrichtung der IP-Lastverteilung

Zur Einrichtung der IP-Lastverteilung muss zunächst eine Lastverteilungsgruppe angelegt werden.

- (1) Gehen Sie zu **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu**.

**Basisparameter**

Gruppenbeschreibung  
Internetzugang

Verteilungsrichtlinie Sitzungs-Round-Robin

Verteilungsmodus  Immer  Nur aktive Schnittstellen verwenden

**Schnittstellenauswahl für Verteilung**

Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung
HINZUFÜGEN			

Abb. 52: Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu

Gehen Sie folgendermaßen vor, um eine Lastverteilungsgruppe anzulegen:

- (1) Bei **Gruppenbeschreibung** geben Sie eine Bezeichnung für die Lastverteilungsgruppe ein, z. B. *Internetzugang*.
- (2) Wählen Sie bei **Verteilungsrichtlinie** das Verfahren ein, nach dem die Daten verteilt werden, hier *Sitzungs-Round-Robin* (für eine Lastverteilung Basierend auf IP-Sitzungen).

Anschließend können die beiden ADSL-Internetzugänge zu dieser Lastverteilungsgruppe hinzugefügt werden.

Klicken Sie dazu auf **Hinzufügen**.

The image shows two screenshots of a network configuration interface. The top screenshot is titled 'Basisparameter' and contains two rows of settings: 'Gruppenbeschreibung' set to 'Internetzugang' and 'Verteilungsrichtlinie' set to 'Sitzungs-Round-Robin'. The bottom screenshot is titled 'Schnittstellenauswahl für Verteilung' and contains two rows: 'Schnittstelle' set to a dropdown menu showing 'WAN\_ADSL-1' and 'Verteilungsverhältnis' set to a text input field containing '50' followed by a '%' symbol.

Abb. 53: **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Schnittstelle** den ersten ADSL-Zugang *WAN\_ADSL-1* aus.
- (2) Bei **Verteilungsverhältnis** geben Sie *50* % ein.
- (3) Klicken Sie auf **Übernehmen**.
- (4) Fügen Sie mit **Hinzufügen** die zweite ADSL-Leitung hinzu.
- (5) Wählen Sie bei **Schnittstelle** den zweiten ADSL-Zugang *WAN\_ADSL-2* aus.
- (6) Bei **Verteilungsverhältnis** geben Sie *50* % ein.
- (7) Klicken Sie auf **Übernehmen**.

Ergebnis:

**Basisparameter**

Gruppenbeschreibung  
Internetzugang

Verteilungsrichtlinie Sitzungs-Round-Robin ▾

Verteilungsmodus  Immer  Nur aktive Schnittstellen verwenden

**Schnittstellenauswahl für Verteilung**

Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung	
WAN_ADSL-1	50 %	0.0.0.0		🗑️ ✎
WAN_ADSL-2	50 %			🗑️ ✎
HINZUFÜGEN				

Abb. 54: Netzwerk -> Lastverteilung -> Lastverteilungsgruppen

Nach diesem Konfigurationsschritt sind bereits beide Internetverbindungen mit Hilfe der IP-Lastverteilung verwendbar. In diesem Szenario sind durch das Aktivieren der IP-Lastverteilung keine Erweiterten Routingeinträge notwendig um den Aufbau der VPN IP-Sec-Tunnel zu ermöglichen.

## Einrichtung der VPN IPSec-Verbindungen

Die VPN IPSec-Verbindungen werden in diesem Szenario immer vom Gateway der Filiale zum Gateway der Zentrale aufgebaut. Für beide Tunnelverbindungen kann das gleiche IP-Sec Phase1- und Phase2-Profil verwendet werden. Legen Sie dazu zwei neue VPN-Tunnel an.

- (1) Gehen Sie zu **VPN -> IPSec -> IPSec-Peers -> Neu**.

**Peer-Parameter**

Administrativer Status  Aktiv  Inaktiv

Beschreibung  
Filiale1\_Peer-1

Peer-Adresse IP-Version | IPv4 bevorzugt ▾

Peer-ID E-Mail-Adresse ▾  
Filiale1\_Peer-1@bintec-elmeg.com

IKE (Internet Key Exchange) IKEv1 ▾

Preshared Key  
\*\*\*\*\*

IP-Version des Tunnelnetzwerks IPv4 ▾

**IPv4-Schnittstellenrouten**

Sicherheitsrichtlinie  Nicht Vertrauenswürdig  Vertrauenswürdig

IPv4-Adressvergabe Statisch ▾

Standardroute  Deaktiviert

Lokale IP-Adresse  
1.0.0.1

Routeneinträge

Entfernte IP-Adresse	Netzmaske	Metrik	
1.0.0.2	255.255.255.255	1 ▾	
192.168.1.0	255.255.255.0	1 ▾	🗑️

HINZUFÜGEN

Erweiterte Einstellungen

Erweiterte IPSec-Optionen		Erweiterte IPSec-Optionen	
Phase-1-Profil	<input type="text" value="Keines (Standardprofil verwenden)"/>	Öffentliche Schnittstelle	<input type="text" value="Vom Routing ausgewählt"/>
Phase-2-Profil	<input type="text" value="Keines (Standardprofil verwenden)"/>	Öffentliche IPv4-Quelladresse	<input type="checkbox"/>
XAUTH-Profil	<input type="text" value="Eines auswählen"/>	Öffentliche IPv6-Quelladresse	<input type="checkbox"/>
Anzahl erlaubter Verbindungen	<input checked="" type="radio"/> Ein Benutzer <input type="radio"/> Mehrere Benutzer	Überprüfung der IPv4-Rückroute	<input type="checkbox"/>
Startmodus	<input checked="" type="radio"/> Auf Anforderung <input type="radio"/> Immer aktiv	IPv4 Proxy ARP	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv

Abb. 56: VPN -> IPSec -> IPSec-Peers -> Neu

Gehen Sie folgendermaßen vor um eine neue Verbindung hinzuzufügen:

- (1) Stellen Sie den **Administrativer Status** auf *Aktiv*. Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung.
- (2) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Filiale1\_Peer-1*.
- (3) Bei **Peer-Adresse** wird keine Adresse eingetragen, da der VPN-Tunnel immer vom Gateway der Filiale zum Gateway der Zentrale aufgebaut wird.
- (4) Bei **Peer-ID** wird für den ersten VPN-Tunnel zur Anbindung der Filiale der ID-Typ *E-Mail-Adresse* und der ID-Wert *Filiale1\_Peer1@bintec-elmeg.com* verwendet. Die **Peer-ID** muss eindeutig sein und mit dem lokalen ID-Wert der Gegenstelle übereinstimmen.
- (5) Bei **IKE (Internet Key Exchange)** wählen Sie die Version des Internet Key Exchange Protokolls. In diesem Szenario muss *IKEv1* verwendet werden.
- (6) Im **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung, z. B. *test12345* ein.
- (7) Für **IPv4-Adressvergabe** wählen Sie den Konfigurationsmodus *Statisch* aus.
- (8) In diesem Szenario wird die Option **Standardroute** nicht gesetzt.
- (9) Die **Lokale IP-Adresse** ist die IP-Adresse welche an die Tunnel-Schnittstelle gebunden wird. Hier wird eine Adresse aus einem bisher nicht verwendeten Netzwerk verwendet, z. B. *1.0.0.1*. Durch diese eindeutige IP-Adresse können Ping-Anfragen, zur Überwachung des VPN-Tunnels, gezielt über die VPN-Tunnel-Schnittstelle gesendet werden.
- (10) Als **Routeneintrag** wird die IP-Adresse / Netzmaske des Zielnetzwerk definiert. Falls weitere Zielnetzwerke über den Tunnel geroutet werden sollen, können diese mit **Hinzufügen** hinzugefügt werden.  
In unserem Beispiel sind zwei Routingeinträge notwendig.  
Tragen Sie eine Adresse aus dem Bereich der **Lokalen IP-Adresse** der Tunnel-Schnittstelle ein, welche zur Überwachung des Tunnels verwendet wird z. B. *1.0.0.2*. Diese Adresse muss mit der **Lokalen IP-Adresse** der VPN Tunnel-

Schnittstelle am Filial-Gateway übereinstimmen für das **Netzwerk** der Filiale, in diesem Beispiel `192.168.1.0/24` ist ein weiterer Routing-Eintrag notwendig.

- (11) Als **Phase-1-Profil** wird das *Standardprofil* verwendet, welches automatisch generiert wurde.
- (12) Als **Phase-2-Profil** wird das *Standardprofil* verwendet, welches automatisch generiert wurde.
- (13) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

Nach der Konfiguration der ersten VPN IPSec-Verbindung zur Anbindung der Filiale kann nun der zweite VPN IPSec-Tunnel angelegt werden.

- (1) Gehen Sie zu **VPN -> IPSec -> IPSec-Peers -> Neu**.

The screenshot shows two panels in a configuration tool. The left panel, titled 'Peer-Parameter', has the following fields: 'Administrativer Status' (radio buttons for 'Aktiv' and 'Inaktiv', with 'Aktiv' selected), 'Beschreibung' (text field with 'Filiale1\_Peer-2'), 'Peer-Adresse' (text field with 'IP-Version' dropdown set to 'IPv4 bevorzugt'), 'Peer-ID' (dropdown for 'E-Mail-Adresse' with value 'Filiale1\_Peer-2@bintec-elmeg.com'), 'IKE (Internet Key Exchange)' (dropdown for 'IKEv1'), 'Pre-shared Key' (password field with asterisks), and 'IP-Version des Tunnelnetzwerks' (dropdown for 'IPv4'). The right panel, titled 'IPv4-Schnittstellenrouten', has: 'Sicherheitsrichtlinie' (radio buttons for 'Nicht Vertrauenswürdig' and 'Vertrauenswürdig', with 'Vertrauenswürdig' selected), 'IPv4-Adressvergabe' (dropdown for 'Statisch'), 'Standardroute' (checkbox for 'Deaktiviert'), 'Lokale IP-Adresse' (text field with '2.0.0.1'), and a table for 'Routeneinträge' with columns 'Entfernte IP-Adresse', 'Netzmaske', and 'Metrik'. The table contains two entries: one with '2.0.0.2', '255.255.255.255', and '1'; and another with '192.168.1.0', '255.255.255.0', and '1'. A 'HINZUFÜGEN' button is at the bottom.

Abb. 57: VPN -> IPSec -> IPSec-Peers -> Neu

Gehen Sie folgendermaßen vor um eine neue Verbindung hinzuzufügen:

- (1) Stellen Sie den **Administrativer Status** auf *Aktiv*. Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung.
- (2) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Filiale1\_Peer-2*.
- (3) Bei **Peer-Adresse** wird keine Adresse eingetragen, da der VPN-Tunnel immer vom Gateway der Filiale zum Gateway der Zentrale aufgebaut wird.
- (4) Bei **Peer-ID** wird für den ersten VPN-Tunnel zur Anbindung der Filiale der ID-Typ *E-Mail-Adresse* und der ID-Wert *Filiale1\_Peer2@bintec-elmeg.com* verwendet. Die **Peer-ID** muss eindeutig sein und mit dem lokalen ID-Wert der Gegenstelle übereinstimmen.
- (5) Bei **IKE (Internet Key Exchange)** wählen Sie die Version des Internet Key Exchange Protokolls. In diesem Szenario muss *IKEv1* verwendet werden.

- (6) Im **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung, z. B. *test12345* ein.
- (7) Für **IPv4-Adressvergabe** wählen Sie den Konfigurationsmodus *Statisch* aus.
- (8) In diesem Szenario wird die Option **Standardroute** nicht gesetzt.
- (9) Die **Lokale IP-Adresse** ist die IP-Adresse welche an die Tunnel-Schnittstelle gebunden wird. Hier wird eine Adresse aus einem bisher nicht verwendeten Netzwerk verwendet z. B. *2.0.0.1*. Durch diese eindeutige IP-Adresse können Ping-Anfragen, zur Überwachung des VPN-Tunnels, gezielt über die VPN-Tunnel-Schnittstelle gesendet werden.
- (10) Als **Routeneintrag** wird die IP-Adresse / Netzmaske das Zielnetzwerk definiert. Falls weitere Zielnetzwerke über den Tunnel geroutet werden sollen, können diese mit **Hinzufügen** hinzugefügt werden.  
In unserem Beispiel sind zwei Routingeinträge notwendig.  
Tragen Sie eine Adresse aus dem Bereich der **Lokalen IP-Adresse** der Tunnel-Schnittstelle ein, welche zur Überwachung des Tunnels verwendet wird z. B. *2.0.0.2*. Diese Adresse muss mit der **Lokalen IP-Adresse** der VPN Tunnel-Schnittstelle am Filial-Gateway übereinstimmen für das **Netzwerk** der Filiale, in diesem Beispiel *192.168.1.0/24* ist ein weiterer Routing-Eintrag notwendig.
- (11) Als **Phase-1-Profil** wird das *Standardprofil* verwendet, welches automatisch generiert wurde.
- (12) Als **Phase-2-Profil** wird das *Standardprofil* verwendet, welches automatisch generiert wurde.
- (13) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

Beim Anlegen der ersten VPN IPSec-Verbindung wurde automatisch ein IPSec **Phase-1-Profile** angelegt auf welches die beiden VPN IPSec-Tunnel verweisen. Um dieses **Phase-1-Profile** für die IPSec-Authentifizierung verwenden zu können muss die lokale IPsec-ID angepasst werden.

- (1) Gehen Sie zu **VPN -> IPSec -> Phase-1-Profile -> <Multi-Proposal>** .

### Phase-1-Parameter (IKE)

Beschreibung  
Multi-Proposal

Proposals

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

DH-Gruppe 5(1536 Bit) ▼

Lebensdauer 14400 Sekunden 0 kBytes

Authentifizierungsmethode Preshared Keys ▼

Modus  Main Modus (ID Protect)  Aggressiv  Strikt

Lokaler ID-Typ E-Mail-Adresse ▼

Lokaler ID-Wert  
central@bintec-elmeg.com

Abb. 58: VPN -> IPSec -> Phase-1-Profil -> <Multi-Proposal> ✎

Gehen Sie folgendermaßen vor:

- (1) Bei **Lokaler ID-Typ** wählen Sie den Typ der lokalen ID aus, hier *E-Mail-Adresse*.
- (2) Bei **Lokaler ID-Wert** geben Sie einen Wert an, mit dem das Gateway der Zentrale identifiziert werden kann, hier z. B. *central@bintec-elmeg.com*.
- (3) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

## Überwachung der VPN IPSec-Verbindungen

Zur Überwachung der VPN IPSec-Tunnelverbindungen werden über beide Tunnel periodisch Ping-Anfragen zum Gateway der Filiale gesendet. Falls diese Ping Anfrage drei mal nicht beantwortet wird, lässt das Gateway der Zentrale über den jeweiligen Tunnel keine neuen Verbindungen zu. Sobald das Gateway der Filiale die Ping Anfrage wieder drei mal beantwortet, werden neue IP-Verbindungen zugelassen. Während der Ausfallzeit eines VPN-Tunnels werden alle Daten über den noch verbleibenden VPN-Tunnel geleitet.

Für die Ping-Überwachung der VPN IPSec-Tunnel wurden beim Anlegen der IPsec-Peers bereits eindeutige IP-Adressen (in diesem Beispiel 1.0.0.2 und 2.0.0.2) vergeben. Mit diesen Adressen wird die Erreichbarkeit des Gateways der Filiale periodisch überwacht.

Im Menü **Hosts** können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

- (1) Gehen Sie zu **Lokale Dienste -> Überwachung -> Hosts -> Neu**.



### Trigger

Überwachte IP-Adresse

Quell-IP-Adresse

Intervall  Sekunden

Erfolgreiche Versuche

Fehlgeschlagene Versuche

Auszuführende Aktion

Aktion	Schnittstelle
<input type="text" value="Überwachen"/>	

**HINZUFÜGEN**

Abb. 59: Lokale Dienste -> Überwachung -> Hosts -> Neu

Gehen Sie folgendermaßen vor:

- (1) Mit der **Gruppen-ID** kann die Überwachung von Hosts zu Gruppen verkettet werden. In diesem Szenario muss jede Host-Überwachung eine eindeutige Gruppen-ID verwenden.
- (2) Bei **Überwachte IP-Adresse** geben Sie die IP-Adresse des Hosts ein, welcher überwacht werden soll. Für die Überwachung des ersten VPN IPSec-Tunnels wird in unserem Beispiel mit der Adresse `1.0.0.2` das Gateway der Filiale überwacht.
- (3) Durch Setzen der **Quell-IP-Adresse** zur Host-Überwachung wird sichergestellt dass das Ping-Packet mit der **Lokalen IP-Adresse** der VPN Tunnel-Schnittstelle gesendet wurde so dass das Gateway der Filiale wieder über diesen Weg antworten kann.

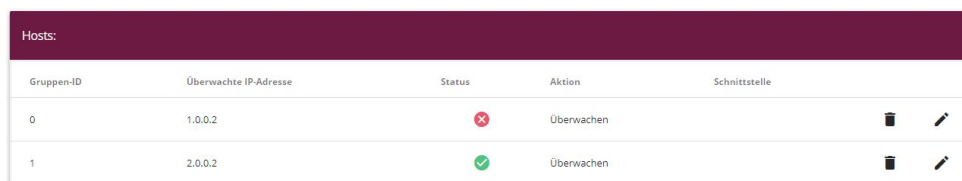
Wählen Sie *Spezifisch* und geben Sie die lokale IP-Adresse der ersten VPN IP-Sec-Schnittstelle an, z. B. *1.0.0.1*.

- (4) Bei **Intervall** geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll, hier z. B. *3* Sekunden.
- (5) Bei **Erfolgreiche Versuche** geben Sie die Anzahl der Pings ein, die unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird. Hier z. B. nach *3* fehlgeschlagenen Versuchen.
- (6) Bei **Fehlgeschlagene Versuche** geben Sie die Anzahl der Pings ein, die beantwortet werden müssen, damit ein Host wieder als erreichbar angesehen wird. In unserem Beispiel wird ein Host nach *3* erfolgreichen Ping Anfragen/Antworten wieder als erreichbar angesehen. Mit dieser Funktion sollen zu häufige Schwankungen der Verbindungen vermieden werden.
- (7) Unter **Auszuführende Aktionen** wählen Sie die Option *Überwachen* aus, da der Status von Schnittstellen nicht verändert werden soll.
- (8) Bestätigen Sie mit **OK**.

Zur Überwachung des zweiten VPN IPSec-Tunnels muss nach dem Speichern ein zweiter Eintrag zur Host-Überwachung angelegt werden. Legen Sie den zweiten Host-Überwachungs-Eintrag, mit Ausnahme der IP-Adressen, identisch zum ersten Eintrag an. In dem zweiten Eintrag zur Host-Überwachung werden die **Lokalen IP-Adressen** der zweiten VPN IPSec-Schnittstelle verwendet. In unserem Beispiel wird als **Überwachte IP-Adresse** die Adresse *2.0.0.2* und für die **Quell-IP-Adresse** die *2.0.0.1* verwendet.

Nach erfolgter Konfiguration werden in der Liste der Überwachten Hosts zwei Einträge gezeigt, welche die Erreichbarkeit der IP-Adressen des Filial-Gateways überwachen.

Ergebnis:









Gruppen-ID	Überwachte IP-Adresse	Status	Aktion	Schnittstelle
0	1.0.0.2		Überwachen	 
1	2.0.0.2		Überwachen	 

Abb. 60: Lokale Dienste -> Überwachung -> Hosts

## Konfiguration der IP-Lastverteilung für die VPN IPSec-Verbindungen

Für die Verteilung der IP-Sitzungen auf beide VPN IPSec-Verbindungen wird eine weitere Lastverteilungs-Gruppe angelegt.

- (1) Gehen Sie zu **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu**.

The screenshot shows a configuration window with two main sections. The top section, titled 'Basisparameter', contains a text field for 'Gruppenbeschreibung' with the value 'VPN\_Filiale1', a dropdown menu for 'Verteilungsrichtlinie' set to 'Sitzungs-Round-Robin', and radio buttons for 'Verteilungsmodus' with 'Immer' selected. The bottom section, titled 'Schnittstellenauswahl für Verteilung', is a table with columns for 'Schnittstelle', 'Verteilungsverhältnis', 'Routenselektor', and 'IP-Adresse zur Nachverfolgung'. A 'HINZUFÜGEN' button is located below the table.

Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung
HINZUFÜGEN			

Abb. 61: Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu

Gehen Sie folgendermaßen vor, um eine Lastverteilungsgruppe anzulegen:

- (1) Bei **Gruppenbeschreibung** geben Sie eine Bezeichnung für die Lastverteilungsgruppe ein, z. B. *VPN\_Filiale1*.
- (2) Wählen Sie bei **Verteilungsrichtlinie** das Verfahren ein, nach dem die Daten verteilt werden, hier *Sitzungs-Round-Robin* (für eine Lastverteilung Basierend auf IP-Sitzungen).

Anschließend können die beiden IPSec-Schnittstellen zu dieser Lastverteilungsgruppe hinzugefügt werden.

Klicken Sie dazu auf **Hinzufügen**.

Basisparameter	
Gruppenbeschreibung	VPN_Filiale1
Verteilungsrichtlinie	Sitzungs-Round-Robin

Schnittstellenauswahl für Verteilung	
Schnittstelle	IPSEC_FILIALE1_PEER-1 ▼
Verteilungsverhältnis	50 %

Erweiterte Einstellungen

Erweiterte Einstellung	
Routenselektor	Keiner ▼
IP-Adresse zur Nachverfolgung	1.0.0.2 ▼

Abb. 62: **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Schnittstelle** die erste VPN IPSec-Schnittstelle zur Anbindung der Filiale aus, hier `IPSEC_FILIALE1_PEER-1`.

- (2) Bei **Verteilungsverhältnis** geben Sie *50 %* ein. Mit dieser Option wird festgelegt in welchem Verhältnis neue IP-Sitzungen auf die Schnittstellen der IP-Lastverteilungsgruppe verteilt werden.
- (3) Der **Routenselektor** wird in diesem Beispiel bei *Keiner* belassen, da keine Schnittstellen mehrfach in unterschiedlichen Lastverteilungsgruppen zugewiesen wurden.
- (4) Mit der Option **IP-Adresse zur Nachverfolgung** wird die IP-Adresse aus der bereits konfigurierten Host-Überwachung gewählt, z. B. *1.0.0.2*. Sobald die Host-Überwachung den Abbruch der Verbindung feststellt, werden keine weiteren IP-Sitzungen über diesen VPN IPsec-Tunnel aufgebaut.
- (5) Klicken Sie auf **Übernehmen**.
- (6) Fügen Sie mit **Hinzufügen** die zweite VPN IPsec-Schnittstelle hinzu.
- (7) Wählen Sie bei **Schnittstelle** *IPSEC\_FILIALE1\_PEER-2* aus.
- (8) Bei **Verteilungsverhältnis** geben Sie *50 %* ein.
- (9) Wählen Sie die **IP-Adresse zur Nachverfolgung** aus, z. B. *2.0.0.2*.
- (10) Klicken Sie auf **Übernehmen**.

Ergebnis:

Basisparameter

Gruppenbeschreibung  
VPN\_Filiale1

Verteilungsrichtlinie Sitzungs-Round-Robin ▾

Verteilungsmodus  Immer  Nur aktive Schnittstellen verwenden

---

Schnittstellenauswahl für Verteilung

Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung	
IPSEC_FILIALE1_PEER-1	50 %		1.0.0.2	🗑️ ✎
IPSEC_FILIALE1_PEER-2	50 %		2.0.0.2	🗑️ ✎

HINZUFÜGEN

Abb. 63: Netzwerk -> Lastverteilung -> Lastverteilungsgruppen

## 6.2.2 Konfiguration des Gateways in der Filiale

### Einrichtung der Internetverbindung

Der Internetzugang des Filial-Gateways kann mit Hilfe des **Assistenten** eingerichtet werden.

- (1) Gehen Sie zu **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu**.
- (2) Wählen Sie bei **Verbindungstyp** *Internes ADSL-Modem* aus.
- (3) Klicken Sie auf **Weiter** um eine neue Internetverbindung zu konfigurieren.
- (4) Geben Sie die erforderlichen Daten für die Verbindung ein.

The screenshot displays a multi-step configuration assistant for creating a new internet connection. The steps are as follows:

- Grundeeinstellungen:** The 'Beschreibung' field is set to 'PPPoE1'.
- Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:** The 'Typ' dropdown is set to 'Benutzerdefiniert' (User-defined), with a sub-option 'VDSL/ADSL auto - PPPoE (PPP über Ethernet)' selected.
- Wird die Konfiguration eines VLAN vom ISP angefordert (z. B. mit VDSL-Modems)?** The 'VLAN' toggle switch is turned off.
- Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:** The 'Benutzername' field contains 'ADSL-Benutzername' and the 'Persönliches Kennwort' field contains 'test12345'.
- Wählen Sie den Verbindungsmodus aus:** The 'Immer aktiv' toggle switch is turned on, labeled 'Aktiviert'.
- Geben Sie die vom Internetdiensteanbieter (ISP) definierten ATM-Einstellungen ein:** The 'Virtual Path Identifier (VPI)' field is set to '1' and the 'Virtual Channel Identifier (VCI)' field is set to '32'.

Abb. 64: **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu** -> **Weiter**

Gehen Sie folgendermaßen vor, um einen Internetzugang zu konfigurieren:

- (1) Bei **Beschreibung** tragen Sie z. B. *PPPoE1* ein.
- (2) Bei **Typ** wählen Sie *Benutzerdefiniert über PPPoE (PPP über Ethernet)* aus.
- (3) Bei **Benutzername** geben Sie den Namen ein, welches Sie von Ihrem Provider erhalten haben z. B. *ADSL-Benutzername*.
- (4) Geben Sie das **Passwort** ein, welches Sie von Ihrem Provider erhalten haben, z. B. *test12345*.
- (5) Aktivieren Sie die Option **Immer aktiv**.

- (6) Bestätigen Sie Ihre Angaben mit **OK**.

### **Einrichtung der VPN IPSec-Verbindungen**

Die beiden IPSec-Peers am Gateway der Filiale müssen unterschiedliche Lokale IPSec-ID's verwenden. Legen Sie vor dem Konfigurieren der eigentlichen IPSec-Peers die zwei Phase-1-Profile an.

- (1) Gehen Sie zu **VPN -> IPSec -> Phase-1-Profile -> Neu**.

### Phase-1-Parameter (IKE)

Beschreibung  
Filiale1\_Peer1

Proposals

Verschlüsselung	Authentifizierung	Aktiviert
AES	SHA1	<input type="checkbox"/>
AES	MD5	<input checked="" type="checkbox"/>
3DES	MD5	<input checked="" 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 E-Mail-Adresse

Lokaler ID-Wert  
Filiale1\_Peer1@bintec-elmeg.com

Abb. 65: VPN -> IPSec -> Phase-1-Profil -> Neu

Gehen Sie folgendermaßen vor.

- (1) Bei **Beschreibung** geben Sie dem Phase-1-Profil einen eindeutigen Namen z. B. *Filiale1\_Peer1*.



- (2) Bei **Proposals** wird eine Kombination aus Verschlüsselungs- und Authentifizierungsalgorithmus gewählt z. B. *AES / SHA1*. Diese Einstellung muss mit der des Zentralen Gateways übereinstimmen.
- (3) Wählen Sie die **DH-Gruppe** (Diffie-Hellmann-Gruppe) die bei der Schlüsselberechnung für den Aufbau der IPSec Phase-1 verwendet werden soll. Diese Einstellung muss mit der des Zentralen Gateways übereinstimmen, z. B. *DH-Gruppe 2 (1024 Bit)*.
- (4) Bei **Lebensdauer** wird die Gültigkeit der berechneten Schlüssel festgelegt. Hier kann der Standardwert von *14400* Sekunden übernommen werden. Diese Einstellung sollte mit der des Zentralen Gateways übereinstimmen.
- (5) In unserem Beispiel werden die VPN IPSec-Tunnel über die **Authentifizierungsmethode** *Preshared Keys* authentifiziert. Hierzu wird bei der IPSec-Peer-Konfiguration ein gemeinsames Passwort vergeben.
- (6) Da in diesem Konfigurationsbeispiel Internetzugänge mit dynamischen Adressen und zur IPSec-Authentifizierung Preshared Keys verwendet werden, muss der **Modus** auf *Aggressiv* gesetzt werden. Diese Einstellung muss mit dem Gateway der Zentrale übereinstimmen.
- (7) Der **Lokaler ID-Type** gibt die Art des Lokalen ID-Werts an. In unserem Beispiel wird eine Lokale ID des Typs *E-Mail-Adresse* verwendet.
- (8) Der **Lokaler ID-Wert** muss eindeutig sein und mit der Option Peer-ID am Gateway der Zentrale übereinstimmen. Für das Phase-1-Profil der ersten IPSec Verbindung wird in diesem Beispiel *Filiale1\_Peer1@bintec-elmeg.com* verwendet.
- (9) Bestätigen Sie Ihre Angaben mit **OK**.

Das zweite IPsec **Phase-1-Profil** kann mit Ausnahme der Beschreibung und des Lokalen-ID-Werts identisch angelegt werden.

Konfigurieren Sie das zweite IPsec **Phase-1-Profil** analog zur Konfiguration des ersten Profils.

- (1) Gehen Sie zu **VPN -> IPSec -> Phase-1-Profile -> Neu**.

### Phase-1-Parameter (IKE)

Beschreibung  
Filiale1\_Peer2

Proposals

Verschlüsselung	Authentifizierung	Aktiviert
AES	SHA1	<input type="checkbox"/>
AES	MD5	<input checked="" type="checkbox"/>
3DES	MD5	<input checked="" 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 E-Mail-Adresse

Lokaler ID-Wert  
Filiale1\_Peer2@bintec-elmeg.com

Abb. 66: VPN -> IPSec -> Phase-1-Profil -> Neu

Gehen Sie folgendermaßen vor.

- (1) Bei **Beschreibung** geben Sie dem Phase-1-Profil einen eindeutigen Namen z. B.

*Filiale1\_Peer2.*

- (2) Bei **Proposals** wird eine Kombination aus Verschlüsselungs- und Authentifizierungsalgorithmus gewählt z. B. *AES / SHA1*. Diese Einstellung muss mit der des Zentralen Gateways übereinstimmen.
- (3) Wählen Sie die **DH-Gruppe** (Diffie-Hellmann-Gruppe) die bei der Schlüsselberechnung für den Aufbau der IPSec Phase-1 verwendet werden soll. Diese Einstellung muss mit der des Zentralen Gateways übereinstimmen, z. B. *DH-Gruppe 2 (1024 Bit)*.
- (4) Bei **Lebensdauer** wird die Gültigkeit der berechneten Schlüssel festgelegt. Hier kann der Standardwert von *14400* Sekunden übernommen werden. Diese Einstellung sollte mit der des Zentralen Gateways übereinstimmen.
- (5) In unserem Beispiel werden die VPN IPSec-Tunnel über die **Authentifizierungsmethode** *Preshared Keys* authentifiziert. Hierzu wird bei der IPSec-Peer-Konfiguration ein gemeinsames Passwort vergeben.
- (6) Da in diesem Konfigurationsbeispiel Internetzugänge mit dynamischen Adressen und zur IPSec-Authentifizierung Preshared Keys verwendet werden, muss der **Modus** auf *Aggressiv* gesetzt werden. Diese Einstellung muss mit dem Gateway der Zentrale übereinstimmen.
- (7) Der **Lokaler ID-Type** gibt die Art des Lokalen ID-Werts an. In unserem Beispiel wird eine Lokale ID des Typs *E-Mail-Adresse* verwendet.
- (8) Der **Lokaler ID-Wert** muss eindeutig sein und mit der Option Peer-ID am Gateway der Zentrale übereinstimmen. Für das Phase-1-Profil der ersten IPSec Verbindung wird in diesem Beispiel *Filiale1\_Peer2@bintec-elmeg.com* verwendet.
- (9) Bestätigen Sie Ihre Angaben mit **OK**.

In der Übersicht der IPSec **Phase-1-Profile** werden anschließend zwei Einträge für die zu konfigurierenden IPSec-Verbindungen angezeigt

- (1) Gehen Sie zu **VPN -> IPSec -> Phase-1-Profile**.

IKEv1 (Internet Key Exchange, Version 1)								
Standard	Beschreibung	Proposals	Authentifizierung	Modus	DH-Gruppe	Lebensdauer		
<input type="radio"/>	Filiale1_Peer1	[AES/SHA1][AES/MD5][3DES/MD5]	Preshared Keys	Aggressiv	2(1024 Bit)	0KB / 4h		
<input checked="" type="radio"/>	Multi-Proposal	[AES/SHA2 256][AES/SHA1][3DES/SHA1]	Preshared Keys	Aggressiv	5(1536 Bit)	0KB / 4h		
<input type="radio"/>	Filiale1_Peer2	[AES/SHA1][AES/MD5][3DES/MD5]	Preshared Keys	Aggressiv	2(1024 Bit)	0KB / 4h		

NEUES IKEV1-PROFIL ERSTELLEN

Abb. 67: VPN -> IPSec -> Phase-1-Profile

Nun werden zwei IPSec-Verbindungen zur Anbindung der Zentrale hinzugefügt.

- (1) Gehen Sie zu **VPN -> IPSec -> IPSec-Peers -> Neu**.

### Peer-Parameter

Administrativer Status  Aktiv  Inaktiv

Beschreibung  
Zentrale\_Peer-1

Peer-Adresse IP-Version | IPv4 bevorzugt  
62.146.53.200

Peer-ID E-Mail-Adresse  
central@bintec-elmeg.com

IKE (Internet Key Exchange) IKEv1

Preshared Key  
\*\*\*\*\*

IP-Version des Tunnelnetzwerks IPv4

### IPv4-Schnittstellenrouten

Sicherheitsrichtlinie  Nicht Vertrauenswürdig  Vertrauenswürdig

IPv4-Adressvergabe Statisch

Standardroute  Deaktiviert

Lokale IP-Adresse  
1.0.0.2

Entfernte IP-Adresse	Netzmaske	Metrik	
1.0.0.1	255.255.255.255	1	
192.168.0.0	255.255.255.0	1	

HINZUFÜGEN

### Erweiterte IPSec-Optionen

Phase-1-Profil Filiale1\_Peer1

Phase-2-Profil \* Multi-Proposal

XAUTH-Profil Eines auswählen

Anzahl erlaubter Verbindungen  Ein Benutzer  Mehrere Benutzer

Startmodus  Auf Anforderung  Immer aktiv

Abb. 69: **VPN -> IPSec -> IPSec-Peers -> Neu**

Gehen Sie folgendermaßen vor um eine neue Verbindung hinzuzufügen:

- (1) Stellen Sie den **Administrativer Status** auf *Aktiv*. Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung.
- (2) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Zentrale\_Peer-1*.
- (3) Bei **Peer-Adresse** geben Sie die statische IP Adresse oder den Host-Namen ein, mit

dem der erste Internetzugang des Gateways der Zentrale erreichbar ist. In unserem Beispiel ist das die statische IP-Adresse `62.146.53.200`.

- (4) Die **Peer-ID** muss mit dem Lokalen ID-Wert des Gateways der Zentrale übereinstimmen. In diesem Beispiel wird der Typ *E-Mail-Adresse* und der ID-Wert *central@bintec-elmeg.com* verwendet.
- (5) Bei **IKE (Internet Key Exchange)** wählen Sie die Version des Internet Key Exchange Protokolls. In diesem Szenario muss *IKEv1* verwendet werden.
- (6) Im **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung, z. B. *test12345* ein.
- (7) Für **IPv4-Adressvergabe** wählen Sie den Konfigurationsmodus *Statisch* aus.
- (8) Wählen Sie aus, ob die Route zu diesem IPsec-Peer als Standard-Route festgelegt wird. In diesem Szenario wird die Option **Standardroute** nicht gesetzt.
- (9) Die **Lokale IP-Adresse** ist die IP-Adresse welche an die Tunnel-Schnittstelle gebunden wird, hier z. B. *1.0.0.2*. Hier wird eine Adresse aus einem bisher nicht verwendeten Netzwerk verwendet. Mit dieser Adresse wird der VPN IPsec-Tunnel überwacht.
- (10) Als **Routeneintrag** wird die IP-Adresse / Netzmaske das Zielnetzwerk definiert. Falls weitere Zielnetzwerke über den Tunnel geroutet werden sollen, können diese mit **Hinzufügen** hinzugefügt werden.  
In unserem Beispiel sind zwei Routingeinträge notwendig.  
Tragen Sie die IP-Adresse ein, welche am Gateway der Zentrale als lokale IP-Adresse der Tunnel-Schnittstelle verwendet wird z. B. *1.0.0.1*. Für das Netzwerk der Zentrale, in diesem Beispiel *192.168.0.0/24*, muss auch ein Routing-Eintrag angelegt werden.
- (11) Als **Phase-1-Profil** muss das bereits angelegte IPsec Phase-1-Profil ausgewählt werden, welches für den ersten VPN IPsec-Tunnel angelegt wurde, z. B. *Filiale1\_Peer1*.
- (12) Als **Phase-2-Profil** wird das Standard Phase-2-Profil verwendet welches automatisch generiert wurde, hier das *\*Multi-Proposal*.
- (13) Das **XAUTH-Profil** wird in diesem Szenario nicht verwendet.
- (14) **Anzahl erlaubter Verbindungen** kann auf dem Standardwert *Ein Benutzer* belassen werden.
- (15) Da die VPN IPsec-Verbindungen immer vom Gateway der Filiale zum Gateway der Zentrale aufgebaut werden, muss hier der **Startmodus** auf *Immer aktiv* gesetzt werden.
- (16) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

Nach der Konfiguration der ersten VPN IPsec-Verbindung zur Anbindung der Zentrale kann nun der zweite VPN IPsec-Tunnel angelegt werden.

- (1) Gehen Sie zu **VPN -> IPsec -> IPsec-Peers -> Neu**.

### Peer-Parameter

Administrativer Status  Aktiv  Inaktiv

Beschreibung  
Zentrale\_Peer-2

Peer-Adresse IP-Version | IPv4 bevorzugt  
62.146.53.201

Peer-ID E-Mail-Adresse  
central@bintec-elmeg.com

IKE (Internet Key Exchange) IKEv1

Refreshed Key  
\*\*\*\*\*

IP-Version des Tunnelnetzwerks IPv4

### IPv4-Schnittstellenrouten

Sicherheitsrichtlinie  Nicht Vertrauenswürdig  Vertrauenswürdig

IPv4-Adressvergabe Statisch

Standardroute  Deaktiviert

Lokale IP-Adresse  
2.0.0.2

Routeneinträge

Entfernte IP-Adresse	Netzmaske	Metrik
2.0.0.1	255.255.255.255	1
192.168.0.0	255.255.255.0	1

HINZUFÜGEN

### Erweiterte IPSec-Optionen

Phase-1-Profil Filiale1\_Peer2

Phase-2-Profil \* Multi-Proposal

XAUTH-Profil Eines auswählen

Anzahl erlaubter Verbindungen  Ein Benutzer  Mehrere Benutzer

Startmodus  Auf Anforderung  Immer aktiv

Backup Peer Keiner

Abb. 71: VPN -> IPSec -> IPSec-Peers -> Neu

Gehen Sie folgendermaßen vor um eine neue Verbindung hinzuzufügen:

- (1) Stellen Sie den **Administrativer Status** auf *Aktiv*. Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung.
- (2) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Zentrale\_Peer-2*.

- (3) Bei **Peer-Adresse** geben Sie die statische IP Adresse oder den Host-Namen ein, mit dem der erste Internetzugang des Gateways der Zentrale erreichbar ist. In unserem Beispiel ist das die statische IP-Adresse *62.146.53.201*.
- (4) Die **Peer-ID** muss eindeutig sein und mit dem lokalen ID-Wert der Gegenstelle übereinstimmen. In unserem Beispiel wird der Typ *E-Mail-Adresse* und der ID-Wert *central@bintec-elmeg.com* verwendet.
- (5) Bei **IKE (Internet Key Exchange)** wählen Sie die Version des Internet Key Exchange Protokolls. In diesem Szenario muss *IKEv1* verwendet werden.
- (6) Im **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung, z. B. *test12345* ein.
- (7) Für **IPv4-Adressvergabe** wählen Sie den Konfigurationsmodus *Statisch* aus.
- (8) In diesem Szenario wird die Option **Standardroute** nicht gesetzt.
- (9) Die **Lokale IP-Adresse** ist die IP-Adresse welche an die Tunnel-Schnittstelle gebunden wird, hier z. B. *2.0.0.2*. Hier wird eine Adresse aus einem bisher nicht verwendeten Netzwerk verwendet. Mit dieser Adresse wird der VPN IPsec-Tunnel überwacht.
- (10) Als **Routeneintrag** wird die Ziel-IP-Adresse / Netzmaske bzw. das Zielnetzwerk definiert. Falls weitere Zielnetzwerke über den Tunnel geroutet werden sollen, können diese mit **Hinzufügen** hinzugefügt werden.  
In unserem Beispiel sind zwei Routingeinträge notwendig.  
Tragen Sie die IP-Adresse ein, welche am Gateway der Zentrale als lokale IP-Adresse der Tunnel-Schnittstelle verwendet wird z. B. *2.0.0.1*. Für das **Netzwerk** der Zentrale, in diesem Beispiel *192.168.1.0/24* ist ein weiterer Routing-Eintrag notwendig.
- (11) Als **Phase-1-Profil** muss das bereits angelegte IPsec Phase-1-Profil ausgewählt werden, welches für den ersten VPN IPsec-Tunnel angelegt wurde, z. B. *Filiale1\_Peer2*.
- (12) Als **Phase-2-Profil** wird das Standard Phase-2-Profil verwendet welches automatisch generiert wurde, hier das *\*Multi-Proposal*.
- (13) Das **XAUTH-Profil** wird in diesem Szenario nicht verwendet.
- (14) **Anzahl erlaubter Verbindungen** kann auf dem Standardwert *Ein Benutzer* belassen werden.
- (15) Da die VPN IPsec-Verbindungen immer vom Gateway der Filiale zum Gateway der Zentrale aufgebaut werden, muss hier der **Startmodus** auf *Immer aktiv* gesetzt werden.
- (16) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

Ergebnis:

IKEv1 (Internet Key Exchange, Version 1)							
Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status	Aktion
IPSec-Statistische-Peers							
1	Zentrale_Peer-1	62.146.53.200	central@bintec- elmeg.com	Filiale1_Peer1	Multi-Proposal		
2	Zentrale_Peer-2	62.146.53.201	central@bintec- elmeg.com	Filiale1_Peer2	Multi-Proposal		

Abb. 72: VPN -> IPSec -> IPSec-Peers

## Überwachung der VPN IPSec-Verbindungen

Zur Überwachung der VPN IPSec-Tunnelverbindungen werden über beide Tunnel periodisch Ping-Anfragen zum Gateway der Zentrale gesendet. Falls diese Ping-Anfrage drei mal nicht beantwortet wird, lässt das Gateway der Filiale über den jeweiligen Tunnel keine neuen Verbindungen zu. Sobald das Gateway der Zentrale die Ping Anfrage wieder drei mal beantwortet, werden neue IP-Verbindungen zugelassen. Während der Ausfallzeit eines VPN-Tunnels werden alle Daten über den noch verbleibenden VPN-Tunnel geleitet.

Für die Ping-Überwachung der VPN IPSec-Tunnel wurden beim Anlegen der IPsec-Peers bereits eindeutige IP-Adressen (in diesem Beispiel 1.0.0.1 und 2.0.0.1) vergeben. Mit diesen Adressen wird die Erreichbarkeit des Gateways der Filiale periodisch überwacht.

Im Menü **Hosts** können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

(1) Gehen Sie zu **Lokale Dienste -> Überwachung -> Hosts -> Neu**.



### Trigger

Überwachte IP-Adresse

Quell-IP-Adresse

Intervall  Sekunden

Erfolgreiche Versuche

Fehlgeschlagene Versuche

Auszuführende Aktion

Aktion	Schnittstelle
<input type="text" value="Überwachen"/>	

**HINZUFÜGEN**

Abb. 73: Lokale Dienste -> Überwachung -> Hosts -> Neu

Gehen Sie folgendermaßen vor:

- (1) Mit der **Gruppen-ID** kann die Überwachung von Hosts zu Gruppen verkettet werden. In diesem Szenario muss jede Host-Überwachung eine eindeutige Gruppen-ID verwenden.
- (2) Bei **Überwachte IP-Adresse** geben Sie die IP-Adresse des Hosts ein, welcher überwacht werden soll. Für die Überwachung des ersten VPN IPSec-Tunnels wird in unserem Beispiel mit der Adresse `1.0.0.1` das Gateway der Filiale überwacht.
- (3) Durch Setzen der **Quell-IP-Adresse** zur Host-Überwachung wird sichergestellt dass das Ping-Packet mit der **Lokalen IP-Adresse** der VPN Tunnel-Schnittstelle gesendet

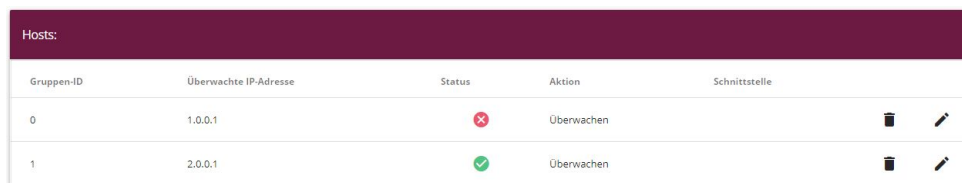
wurde so dass das Gateway der Filiale wieder über diesen Weg antworten kann.  
Wählen Sie *Spezifisch* und geben Sie die lokale IP-Adresse der ersten VPN IP-Sec-Schnittstelle an, z. B. *1.0.0.2*.

- (4) Bei **Intervall** geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll, hier z. B. *3* Sekunden.
- (5) Bei **Erfolgreiche Versuche** geben Sie die Anzahl der Pings ein, die unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird. Hier z. B. nach *3* fehlgeschlagenen Versuchen.
- (6) Bei **Fehlgeschlagene Versuche** geben Sie die Anzahl der Pings ein, die beantwortet werden müssen, damit ein Host wieder als erreichbar angesehen wird. In unserem Beispiel wird ein Host nach *3* erfolgreichen Ping Anfragen/Antworten wieder als erreichbar angesehen. Mit dieser Funktion sollen zu häufige Schwankungen der Verbindungen vermieden werden.
- (7) Unter **Auszuführende Aktionen** wählen Sie die Option *Überwachen* aus, da der Status von Schnittstellen nicht verändert werden soll.
- (8) Bestätigen Sie mit **OK**.

Zur Überwachung des zweiten VPN IPSec-Tunnels muss nach dem Speichern ein zweiter Eintrag zur Host-Überwachung angelegt werden. Legen Sie den zweiten Host-Überwachungs-Eintrag, mit Ausnahme der IP-Adressen, identisch zum ersten Eintrag an. In dem zweiten Eintrag zur Host-Überwachung werden die **Lokalen IP-Adressen** der zweiten VPN IPSec-Schnittstelle verwendet. In unserem Beispiel wird als **Überwachte IP-Adresse** die Adresse *2.0.0.1* und für die **Quell-IP-Adresse** die *2.0.0.2* verwendet.

Nach erfolgter Konfiguration werden in der Liste der Überwachten Hosts zwei Einträge gezeigt, welche die Erreichbarkeit der IP-Adressen des Filial-Gateways überwachen.

Ergebnis:



Hosts:					
Gruppen-ID	Überwachte IP-Adresse	Status	Aktion	Schnittstelle	
0	1.0.0.1	✖	Überwachen		
1	2.0.0.1	✔	Überwachen		

Abb. 74: Lokale Dienste -> Überwachung -> Hosts

## Konfiguration der IP-Lastverteilung für die VPN IPSec-Verbindungen

Für die Verteilung der IP-Sitzungen auf beide VPN IPSec-Verbindungen wird eine Lastverteilungs-Gruppe angelegt.

- (1) Gehen Sie zu **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu**.

Basisparameter			
Gruppenbeschreibung	IPSec_Zentrale		
Verteilungsrichtlinie	Sitzungs-Round-Robin		
Verteilungsmodus	<input checked="" type="radio"/> Immer <input type="radio"/> Nur aktive Schnittstellen verwenden		

Schnittstellenauswahl für Verteilung			
Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung
HINZUFÜGEN			

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

Gehen Sie folgendermaßen vor, um eine Lastverteilungsgruppe anzulegen:

- (1) Bei **Gruppenbeschreibung** geben Sie eine Bezeichnung für die Lastverteilungsgruppe ein, z. B. *IPSec\_Zentrale*.
- (2) Wählen Sie bei **Verteilungsrichtlinie** das Verfahren ein, nach dem die Daten verteilt werden, hier *Sitzungs-Round-Robin* (für eine Lastverteilung Basierend auf IP-Sitzungen).

Anschließend können die beiden ADSL-Internetzugänge zu dieser Lastverteilungsgruppe hinzugefügt werden.

Klicken Sie dazu auf **Hinzufügen**.

Basisparameter	
Gruppenbeschreibung	IPSec_Zentrale
Verteilungsrichtlinie	Sitzungs-Round-Robin

Schnittstellenauswahl für Verteilung	
Schnittstelle	IPSEC_ZENTRALE_PEER-1 ▼
Verteilungsverhältnis	50 %

**Erweiterte Einstellungen**

Erweiterte Einstellung	
Routenselektor	Keiner ▼
IP-Adresse zur Nachverfolgung	1.0.0.1 ▼

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

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Schnittstelle** die erste VPN IPSec-Schnittstelle zur Anbindung der Zentrale aus, hier *IPSEC\_Zentrale\_PEER-1*.
- (2) Bei **Verteilungsverhältnis** geben Sie *50 %* ein. Mit dieser Option wird festgelegt in welchem Verhältnis neue IP-Sitzungen auf die Schnittstellen der IP-Lastverteilungsgruppe verteilt werden.

- (3) Der **Routenselektor** wird in diesem Beispiel bei *Keiner* belassen, da keine Schnittstellen mehrfach in unterschiedlichen Lastverteilungsgruppen zugewiesen wurden.
- (4) Mit der Option **IP-Adresse zur Nachverfolgung** wird eine IP-Adresse aus der bereits konfigurierten Host-Überwachung gewählt, z. B. *1.0.0.1*. Sobald die Host-Überwachung den Abbruch der Verbindung feststellt, werden keine weiteren IP-Sitzungen über diesen VPN IPsec-Tunnel aufgebaut.
- (5) Klicken Sie auf **Übernehmen**.
- (6) Fügen Sie mit **Hinzufügen** die zweite VPN IPsec-Schnittstelle hinzu.
- (7) Wählen Sie bei **Schnittstelle** *IPSEC\_Zentrale\_PEER-2* aus.
- (8) Bei **Verteilungsverhältnis** geben Sie *50 %* ein.
- (9) Wählen Sie die **IP-Adresse zur Nachverfolgung** aus, z. B. *2.0.0.1*.
- (10) Klicken Sie auf **Übernehmen**.

Ergebnis:

**Basisparameter**

Gruppenbeschreibung  
IPSec\_Zentrale

Verteilungsrichtlinie Sitzungs-Round-Robin ▾

Verteilungsmodus  Immer  Nur aktive Schnittstellen verwenden

**Schnittstellenauswahl für Verteilung**

Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung	
IPSEC_ZENTRALE_PEER-1	50 %		1.0.0.1	🗑️ ✎
IPSEC_ZENTRALE_PEER-2	50 %		2.0.0.1	🗑️ ✎
HINZUFÜGEN				

Abb. 77: Netzwerk -> Lastverteilung -> Lastverteilungsgruppen

## 6.3 Konfigurationsschritte im Überblick

### Konfiguration der Internetverbindungen (Zentrale)

Feld	Menü	Wert
Verbindungstyp	Assistenten -> Internet -> Internetverbindungen -> Neu	<i>Internes ADSL-Modem</i>
Beschreibung	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ADSL-1</i>
Typ	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	<i>Benutzerdefiniert über PPPoE (PPP über Ethernet)</i>
Benutzername	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ADSL-Benutzername</i>
Passwort	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>test12345</i>
Immer aktiv	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	<i>Aktiviert</i>
Verbindungstyp	Assistenten -> Internet -> Internetverbindungen -> Neu	<i>Externes ADSL-Modem</i>
Beschreibung	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ADSL-2</i>
Physischer Ethernet-Port	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	<i>ETH5</i>
Benutzername	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ADSL-Benutzername2</i>
Passwort	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>test12345</i>
Immer aktiv	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	<i>Aktiviert</i>



### Lastverteilungsgruppe anlegen

Feld	Menü	Wert
Gruppenbeschreibung	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	z. B. <i>Internetzugang</i>
Verteilungsrichtlinie	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	<i>Sitzung-Round-Robin</i>
Schnittstelle	Netzwerk -> Lastverteilung -> Lastver-	<i>WAN_ADSL-1</i>

Feld	Menü	Wert
	teilungsguppen -> Hinzufügen	
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsguppen -> Hinzufügen	50 %
Schnittstelle	Netzwerk -> Lastverteilung -> Lastverteilungsguppen -> Hinzufügen	WAN_ADSL-2
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsguppen -> Hinzufügen	50 %

#### Einrichtung der VPN IPSec-Verbindungen

Feld	Menü	Wert
Administrativer Status	VPN -> IPSec -> IPSec-Peers -> Neu	Aktiv
Beschreibung	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. <i>Filiale1_Peer-1</i>
Peer-ID	VPN -> IPSec -> IPSec-Peers -> Neu	E-Mail-Adresse und z. B. <i>Filiale1_Peer-1@bintec-elmeg.com</i>
IKE (Internet Key Exchange)	VPN -> IPSec -> IPSec-Peers -> Neu	<i>IKEv1</i>
Preshared Key	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. <i>test12345</i>
IPv4-Adressvergabe	VPN -> IPSec -> IPSec-Peers -> Neu	<i>Statisch</i>
Lokale IP-Adresse	VPN -> IPSec -> IPSec-Peers -> Neu	<i>1.0.0.1</i>
Routeneinträge	VPN -> IPSec -> IPSec-Peers -> Neu	<i>1.0.0.2/ 255.255.255.255 und 192.168.1.0/ 255.255.255.0</i>
Phase-1-Profil	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	<i>Keines (Standardprofil verwenden)</i>
Phase-2-Profil	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	<i>Keines (Standardprofil verwenden)</i>
Administrativer Status	VPN -> IPSec -> IPSec-Peers -> Neu	<i>Aktiv</i>
Beschreibung	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. <i>Filiale1_Peer-2</i>
Peer-ID	VPN -> IPSec -> IPSec-Peers -> Neu	E-Mail-Adresse und

Feld	Menü	Wert
		z. B. <i>Filia- le1_Peer-2@bintec- elmeg.com</i>
<b>IKE (Internet Key Exchange)</b>	<b>VPN -&gt; IPSec -&gt; IPSec-Peers -&gt; Neu</b>	<i>IKEv1</i>
<b>Preshared Key</b>	<b>VPN -&gt; IPSec -&gt; IPSec-Peers -&gt; Neu</b>	z. B. <i>test12345</i>
<b>IPv4-Adressvergabe</b>	<b>VPN -&gt; IPSec -&gt; IPSec-Peers -&gt; Neu</b>	<i>Statisch</i>
<b>Lokale IP-Adresse</b>	<b>VPN -&gt; IPSec -&gt; IPSec-Peers -&gt; Neu</b>	<i>2.0.0.1</i>
<b>Routeneinträge</b>	<b>VPN -&gt; IPSec -&gt; IPSec-Peers -&gt; Neu</b>	<i>2.0.0.2/ 255.255.255.255 und 192.168.1.0/ 255.255.255.0</i>
<b>Phase-1-Profil</b>	<b>VPN -&gt; IPSec -&gt; IPSec-Peers -&gt; Neu -&gt; Erweiterte Einstellungen</b>	<i>Keines (Standardprofil verwenden)</i>
<b>Phase-2-Profil</b>	<b>VPN -&gt; IPSec -&gt; IPSec-Peers -&gt; Neu -&gt; Erweiterte Einstellungen</b>	<i>Keines (Standardprofil verwenden)</i>
<b>Lokaler ID-Typ</b>	<b>VPN -&gt; IPSec -&gt; Phase-1-Profile -&gt; &lt;Multi-Proposal&gt;</b> 	<i>E-Mail-Adresse</i>
<b>Lokaler ID-Wert</b>	<b>VPN -&gt; IPSec -&gt; Phase-1-Profile -&gt; &lt;Multi-Proposal&gt;</b> 	z. B. <i>cen- tral@bintec-elmeg. com</i>

### Überwachungsaufgaben einzurichten

Feld	Menü	Wert
<b>Überwachte IP-Adresse</b>	<b>Lokale Dienste -&gt; Überwachung -&gt; Hosts -&gt; Neu</b>	<i>Spezifisch/ z. B. 1.0.0.2</i>
<b>Quell-IP-Adresse</b>	<b>Lokale Dienste -&gt; Überwachung -&gt; Hosts -&gt; Neu</b>	<i>Spezifisch/ z. B. 1.0.0.1</i>
<b>Intervall</b>	<b>Lokale Dienste -&gt; Überwachung -&gt; Hosts -&gt; Neu</b>	z. B. <i>3 Sekunden</i>
<b>Erfolgreiche Versuche</b>	<b>Lokale Dienste -&gt; Überwachung -&gt; Hosts -&gt; Neu</b>	z. B. <i>3</i>
<b>Fehlgeschlagene Versuche</b>	<b>Lokale Dienste -&gt; Überwachung -&gt; Hosts -&gt; Neu</b>	z. B. <i>3</i>
<b>Auszuführende Ak-</b>	<b>Lokale Dienste -&gt; Überwachung -&gt;</b>	<i>Überwachen</i>



Feld	Menü	Wert
tion	Hosts -> Neu	
Überwachte IP-Adresse	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. 2.0.0.2
Quell-IP-Adresse	Lokale Dienste -> Überwachung -> Hosts -> Neu	Spezifisch / z. B. 2.0.0.1
Intervall	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. 3 Sekunden
Erfolgreiche Versuche	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. 3
Fehlgeschlagene Versuche	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. 3
Auszuführende Aktion	Lokale Dienste -> Überwachung -> Hosts -> Neu	Überwachen

#### Konfiguration der IP-Lastverteilung

Feld	Menü	Wert
Gruppenbeschreibung	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	z. B. VPN_Filiale1
Verteilungsrichtlinie	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	Sitzung-Round-Robin
Schnittstelle	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	IP-SEC_FILIALE_PEER-1
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	50 %
Routenselektor	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen -> Erweiterte Einstellungen	Keiner
IP-Adresse zur Nachverfolgung	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	z. B. 1.0.0.2
Schnittstelle	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	IP-SEC_FILIALE_PEER-2
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	50 %
Routenselektor	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen -> Erweiterte Einstellungen	Keiner
IP-Adresse zur	Netzwerk -> Lastverteilung -> Lastver-	z. B. 2.0.0.2

Feld	Menü	Wert
Nachverfolgung	teilungsgruppen -> Hinzufügen	

#### Konfiguration der Internetverbindungen (Filiale)

Feld	Menü	Wert
Verbindungstyp	Assistenten -> Internet -> Internetverbindungen -> Neu	<i>Internes ADSL-Modem</i>
Beschreibung	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>PPPoE1</i>
Typ	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	<i>Benutzerdefiniert über PPPoE (PPP über Ethernet)</i>
Benutzername	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ADSL-Benutzername</i>
Passwort	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>test12345</i>
Immer aktiv	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	<i>Aktiviert</i>

#### Einrichtung der VPN IPSec-Verbindungen

Feld	Menü	Wert
Beschreibung	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>Filiale1_Peer1</i>
Proposals	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>AES / SHA1</i>
DH-Gruppe	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>2 (1024 Bit)</i>
Lebensdauer	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>14400</i>
Authentifizierungsmethode	VPN -> IPSec -> Phase-1-Profil -> Neu	<i>Preshared Key</i>
Modus	VPN -> IPSec -> Phase-1-Profil -> Neu	<i>Aggressiv</i>
Lokaler ID-Typ	VPN -> IPSec -> Phase-1-Profil -> Neu	<i>E-Mail-Adresse</i>
Lokaler ID-Wert	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>Filiale1_Peer1@bintec-elmeg.com</i>
Beschreibung	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>Filiale1_Peer2</i>
Proposals	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>AES / SHA1</i>
DH-Gruppe	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>2 (1024 Bit)</i>
Lebensdauer	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. <i>14400</i>
Authentifizierungsmethode	VPN -> IPSec -> Phase-1-Profil -> Neu	<i>Preshared Key</i>

Feld	Menü	Wert
methode		
Modus	VPN -> IPSec -> Phase-1-Profil -> Neu	Aggressiv
Lokaler ID-Typ	VPN -> IPSec -> Phase-1-Profil -> Neu	E-Mail-Adresse
Lokaler ID-Wert	VPN -> IPSec -> Phase-1-Profil -> Neu	z. B. Filiale1_Peer1@bintec-elmeg.com

#### IPSec-Verbindungen hinzufügen

Feld	Menü	Wert
Administrativer Status	VPN -> IPSec -> IPSec-Peers -> Neu	Aktiv
Beschreibung	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. Zentrale_Peer-1
Peer-Adresse	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. 62.146.53.200
Peer-ID	VPN -> IPSec -> IPSec-Peers -> Neu	E-Mail-Adresse und z. B. central@bintec-elmeg.com
IKE (Internet Key Exchange)	VPN -> IPSec -> IPSec-Peers -> Neu	IKEv1
Preshared Key	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. test12345
IPv4-Adressvergabe	VPN -> IPSec -> IPSec-Peers -> Neu	Statisch
Lokale IP-Adresse	VPN -> IPSec -> IPSec-Peers -> Neu	1.0.0.2
Routeneinträge	VPN -> IPSec -> IPSec-Peers -> Neu	1.0.0.1/ 255.255.255.255 und 192.168.0.0/ 255.255.255.0
Phase-1-Profil	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	Filiale1_Peer1
Phase-2-Profil	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	*Multi-Proposal
Anzahl erlaubter Verbindungen	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	Ein Benutzer
Startmodus	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	Immer aktiv
Administrativer Status	VPN -> IPSec -> IPSec-Peers -> Neu	Aktiv

Feld	Menü	Wert
Beschreibung	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. <i>Zentrale_Peer-2</i>
Peer-Adresse	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. <i>62.146.53.201</i>
Peer-ID	VPN -> IPSec -> IPSec-Peers -> Neu	<i>E-Mail-Adresse</i> und z. B. <i>central@bintec-elmeg.com</i>
IKE (Internet Key Exchange)	VPN -> IPSec -> IPSec-Peers -> Neu	<i>IKEv1</i>
Preshared Key	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. <i>test12345</i>
IPv4-Adressvergabe	VPN -> IPSec -> IPSec-Peers -> Neu	<i>Statisch</i>
Lokale IP-Adresse	VPN -> IPSec -> IPSec-Peers -> Neu	<i>2.0.0.2</i>
Routeneinträge	VPN -> IPSec -> IPSec-Peers -> Neu	<i>2.0.0.1 / 255.255.255.255</i> und <i>192.168.0.0 / 255.255.255.0</i>
Phase-1-Profil	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	<i>*Filiale1_Peer2</i>
Phase-2-Profil	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	<i>*Multi-Proposal</i>
Anzahl erlaubter Verbindungen	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	<i>Ein Benutzer</i>
Startmodus	VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen	<i>Immer aktiv</i>

#### Überwachungsaufgaben einzurichten

Feld	Menü	Wert
Überwachte IP-Adresse	Lokale Dienste -> Überwachung -> Hosts -> Neu	<i>Spezifisch / z. B. 1.0.0.1</i>
Quell-IP-Adresse	Lokale Dienste -> Überwachung -> Hosts -> Neu	<i>Spezifisch / z. B. 1.0.0.2</i>
Intervall	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. <i>3 Sekunden</i>
Erfolgreiche Versuche	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. <i>3</i>
Fehlgeschlagene Versuche	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. <i>3</i>

Feld	Menü	Wert
Auszuführende Aktion	Lokale Dienste -> Überwachung -> Hosts -> Neu	Überwachen
Überwachte IP-Adresse	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. 2.0.0.1
Quell-IP-Adresse	Lokale Dienste -> Überwachung -> Hosts -> Neu	Spezifisch / z. B. 2.0.0.2
Intervall	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. 3 Sekunden
Erfolgreiche Versuche	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. 3
Fehlgeschlagene Versuche	Lokale Dienste -> Überwachung -> Hosts -> Neu	z. B. 3
Auszuführende Aktion	Lokale Dienste -> Überwachung -> Hosts -> Neu	Überwachen

#### Konfiguration der IP-Lastverteilung

Feld	Menü	Wert
Gruppenbeschreibung	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	z. B. IPSec_Zentrale
Verteilungsrichtlinie	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu	Sitzung-Round-Robin
Schnittstelle	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	IP-SEC_Zentrale_PEER-1
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	50 %
Routenselektor	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen -> Erweiterte Einstellungen	Keiner
IP-Adresse zur Nachverfolgung	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	z. B. 1.0.0.1
Schnittstelle	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	IP-SEC_Zentrale_PEER-2
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	50 %
Routenselektor	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen -> Er	Keiner

Feld	Menü	Wert
	<b>weiterte Einstellungen</b>	
<b>IP-Adresse zur Nachverfolgung</b>	<b>Netzwerk -&gt; Lastverteilung -&gt; Lastverteilungsgruppen -&gt; Hinzufügen</b>	z. B. <i>2.0.0.1</i>

## Kapitel 7 IP - Mit Drop In eine Filiale durch einen VPN-Tunnel mit der Zentrale verbinden

### 7.1 Einleitung

In diesem Beispiel wird beschrieben wie die Funktionalität der Drop-In-Gruppe dazu verwendet werden kann um eine Filiale durch einen VPN-Tunnel mit der Zentrale zu verbinden.

Die Verwendung einer Drop-In-Gruppe bietet sich an, wenn der bestehende Internetzugang in der Filiale die Einrichtung eines VPN-Tunnels nicht zuläßt und nicht ersetzt werden kann. Der Vorteil der Drop-In-Gruppe besteht darin, das die Netzstruktur und die Konfigurationen der einzelnen Rechner in der Filiale nicht geändert werden muß.

Ein **bintec**-Router wird zwischen das Provider-Gateway und das bestehende Netzwerk in der Filiale gesetzt. Er baut den Tunnel zur Zentrale auf und leitet alle Pakete für die Zentrale durch diesen, während alle übrigen normal zum Provider-Gateway weitergeleitet werden.

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

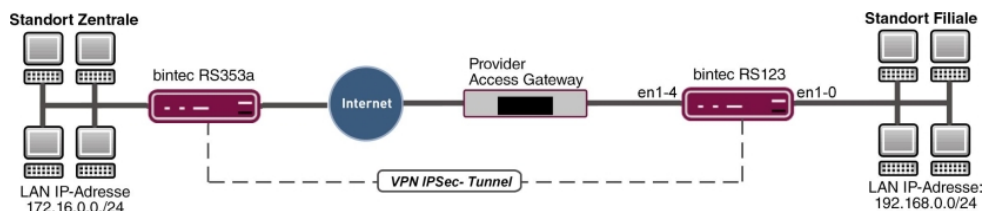


Abb. 78: Beispielszenario

### Voraussetzungen

- Ein **bintec**-Router, z. B. **bintec RS123**
- Firmware Version mindestens 10.2.5
- Filiale mit einem dynamischen Internetzugang
- Zentrale mit einem VPN-fähigen Gateway das über eine statische IP-Adresse zu erreichen ist z. B. **bintec RS353a**

## 7.2 Konfiguration

Öffnen Sie einen Web-Browser und stellen Sie eine http-Verbindung zu dem Gerät her. In unserem Beispiel ist das lokale Netz in der Filiale identisch zum voreingestellten Standard-Netz des Gerätes.

### Konfiguration der Drop-In-Gruppe

Als erstes wird eine neue **Drop-In-Gruppe** für das lokale Nebenstellennetz angelegt.

(1) Gehen Sie zu **Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu**.



### Basisparameter

Gruppenbeschreibung  
DropIn-Gruppe

Modus Transparent ▾

Vom NAT ausnehmen (DMZ)

Netzwerkconfiguration Statisch ▾

Netzwerkadresse  
192.168.0.0

Netzmaske  
255.255.255.0

Lokale IP-Adresse  
192.168.0.254

ARP Lifetime  
3600 Sekunden

DNS-Zuweisung über DHCP Unverändert ▾

Schnittstellenauswahl



Schnittstelle	
<span>LAN_EN1-0 ▾</span>	
<span>LAN_EN1-4 ▾</span>	

Abb. 79: Netzwerk -&gt; Drop In -&gt; Drop-In-Gruppen -&gt; Neu

Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine eindeutige **Gruppenbeschreibung** für die Drop-In-Gruppe ein, z. B. *DropIn-Gruppe*.
- (2) Bei **Modus** wählen Sie *Transparent* aus. ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden transparent (unverändert) weitergeleitet.
- (3) Unter **Netzwerkconfiguration** wählen Sie aus, auf welche Weise den Netzwerkkomponenten eine IP-Adresse zugewiesen wird, hier *Statisch*.
- (4) Geben Sie die **Netzwerkadresse** des Drop-In-Netzwerks ein, hier z. B. *192.168.0.0*.
- (5) Geben Sie die zugehörige **Netzmaske** ein, hier z. B. *255.255.255.0*.
- (6) Geben Sie die **Lokale IP-Adresse** der Drop-In-Gruppe ein, hier z. B. *192.168.0.254*.
- (7) Bei **Schnittstellenauswahl** wählen Sie alle Ports aus, die in der Drop-In-Gruppe (im Netzwerk) enthalten sein sollen, z. B. *LAN\_EN1-0* und *LAN\_EN1-4*.
- (8) Bestätigen Sie mit **OK**.

## Einrichten der Standardroute

Im nächsten Schritt wird eine Standardroute zum Provider-Gateway eingerichtet. Dabei muß die Schnittstelle der Drop-In-Gruppe ausgewählt werden, an der später das Gateway angeschlossen ist.

- (1) Gehen Sie zu **Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu**.

The screenshot shows a configuration window for IPv4 routes, divided into two main sections: 'Basisparameter' (Basic parameters) and 'Routenparameter' (Route parameters).

- Basisparameter:**
  - Routentyp:** Standardroute über Gateway (dropdown menu)
  - Schnittstelle:** LAN\_EN1-4 (dropdown menu)
  - Routenklasse:** Standard (selected with radio button), Erweitert (unselected)
- Routenparameter:**
  - Gateway-IP-Adresse:** 192.168.0.1 (text input field)
  - Metrik:** 1 (text input field)

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

Gehen Sie folgendermaßen vor:

- (1) Bei **Routentyp** wählen Sie *Standardroute über Gateway* aus.
- (2) Wählen Sie die **Schnittstelle** aus, welche für diese Route verwendet werden soll, hier *LAN\_EN1-4*.
- (3) Bei **Gateway-IP-Adresse** geben Sie die IP-Adresse des Provider-Gateways ein, hier z. B. *192.168.0.1*.
- (4) Bestätigen Sie mit **OK**.

## Einrichtung des VPN-Tunnel Endpunktes in der Filiale

Zur Konfiguration eines Endpunktes der VPN (IPSec)-Verbindung in der Filiale verfügt das **GUI** über einen **Assistenten**.

Hierfür muß die statische Adresse unter der die Gegenstelle in der Zentrale erreichbar ist bekannt sein. Der **Assistent** legt automatisch eine Route für das durch den Tunnel zu erreichende Netz der Zentrale an. Gehen Sie dazu in folgendes Menü:

- (1) Gehen Sie zu **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**.
- (2) Wählen Sie bei **VPN-Szenario** *IPSec - LAN-zu-LAN-Verbindung* aus.
- (3) Klicken Sie auf **Weiter**, um eine neue VPN-Verbindung zu konfigurieren.

Ausgewähltes Szenario: LAN-zu-LAN-Verbindung

Verbindungsdetails	IP-Einstellungen eingeben:
Beschreibung IPSec_Connection_1	IPsec Peer IPv4-Adresse 213.7.46.137
Lokale IPsec ID Filiale	Entferntes IPv4-Netzwerk 172.16.0.0 255.255.255.0
Entfernte IPsec ID Zentrale	
Preshared Key *****	
IP-Version des Tunnelnetzwerks IPv4	
Lokale IP-Adresse 192.168.0.254	
Diese Verbindung als Standardroute definieren <input type="checkbox"/> Deaktiviert	

Abb. 81: **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) Bei **Lokale IPsec ID** geben Sie die ID Ihres eigenen IPsec-Gateways ein, z. B. *Filiale*.
- (3) Bei **Entfernte IPsec ID** geben Sie die ID des entfernten IPsec-Gateways ein, z. B. *Zentrale*.
- (4) Für die Authentifizierung geben Sie ein **Preshared Key** an. Der Preshared Key muss auf beiden Seiten identisch konfiguriert werden.
- (5) Wählen Sie die **Lokale IP-Adresse** *192.168.0.254* aus.
- (6) Bei **IPsec-Peer IPv4-Adresse** geben Sie die IP-Adresse des entfernten IPsec-Partners ein, hier z. B. *213.7.46.137*.

- (7) Geben Sie die IP-Adresse des **Entfernten IPv4-Netzwerks** ein, hier z. B. *172.16.0.0*.
- (8) Geben Sie die entsprechende **Netzmaske** des Zielnetzwerks ein, hier z. B. *255.255.255.0*.
- (9) Bestätigen Sie Ihre Angaben mit **OK**.

## Einrichten des VPN-Tunnel Endpunktes in der Zentrale

Konfigurieren Sie die entsprechende Gegenseite des VPN-Tunnels in der Zentrale.

- (1) Gehen Sie zu **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**.
- (2) Wählen Sie bei **VPN-Szenario** *IPSec - LAN-zu-LAN-Verbindung* aus.
- (3) Klicken Sie auf **Weiter**, um eine neue VPN-Verbindung zu konfigurieren.

Ausgewähltes Szenario: LAN-zu-LAN-Verbindung

Verbindungsdetails	IP-Einstellungen eingeben:
Beschreibung IPSec_Connection_1	IPsec Peer IPv4-Adresse
Lokale IPsec ID Zentrale	Entferntes IPv4-Netzwerk 192.168.0.0 255.255.255.0
Entfernte IPsec ID Filiale	
Preshared Key *****	
IP-Version des Tunnelnetzwerks IPv4	
Lokale IP-Adresse 172.16.0.254	
Diese Verbindung als Standardroute definieren <input type="checkbox"/> Deaktiviert	

Abb. 82: **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) Bei **Lokale IPsec ID** geben Sie die ID Ihres eigenen IPsec-Gateways ein, z. B. *Zentrale*.
- (3) Bei **Entfernte IPsec ID** geben Sie die ID des entfernten IPsec-Gateways ein, z. B. *Filiale*.
- (4) Für die Authentifizierung geben Sie ein **Preshared Key** an. Der Preshared Key muss auf beiden Seiten identisch konfiguriert werden.
- (5) Wählen Sie die erforderliche **Lokale IP-Adresse** des Gateways aus, z. B. *172.16.0.254* aus.

- (6) Da der Drop-In-Router in der Filiale nicht von außen zu erreichen ist muß der Tunnel immer von der Filiale initiiert werden. In der Zentrale bleibt daher das Feld **IPSec-Peer-Adresse** leer.
- (7) Geben Sie die IP-Adresse des **Entfernte IPv4-Netzwerks** ein, hier z. B.  
*192.168.0.0.*
- (8) Geben Sie die entsprechende **Netzmaske** des Zielnetzwerks ein, hier z. B.  
*255.255.255.0.*
- (9) Bestätigen Sie Ihre Angaben mit **OK**.

Die Konfiguration ist somit abgeschlossen. Speichern Sie die Konfiguration mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

## 7.3 Konfigurationsschritte im Überblick

### Drop-In-Gruppe konfigurieren

Feld	Menü	Wert
Gruppenbeschreibung	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>DropIn-Gruppe</i>
Modus	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	<i>Transparent</i>
Netzwerkkonfiguration	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	<i>Statisch</i>
Netzwerkadresse	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>192.168.0.0</i>
Netzmaske	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>255.255.255.0</i>
Lokale IP-Adresse	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>192.168.0.254</i>
Schnittstellenauswahl	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>LAN_EN1-0,</i> <i>LAN_EN1-4</i>

### Standardroute einrichten

Feld	Menü	Wert
Routentyp	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	<i>Standardroute über Gateway</i>
Schnittstelle	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	<i>LAN_EN1-4</i>
Gateway-IP-Adresse	Netzwerk -> Routen -> Konfigurati-	z. B. <i>192.168.0.1</i>

Feld	Menü	Wert
	on von IPv4-Routen -> Neu	

#### VPN-Verbindung einrichten (Filiale)

Feld	Menü	Wert
VPN-Szenario	Assistenten -> VPN -> VPN-Verbindungen -> Neu	IPSec - LAN-zu-LAN-Verbindung
Beschreibung	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. IP-Sec_Connection_1
Lokale IPSec ID	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	Filiale
Entfernte IPSec ID	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	Zentrale
Preshared Key	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	Passwort eingeben
Lokale IP-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. 192.168.0.254
IPSec-Peer IPv4-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. 213.7.46.137
Entferntes IPv4-Netzwerk	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. 172.16.0.0
Netzmaske	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. 255.255.255.0

#### VPN-Verbindung einrichten (Zentrale)

Feld	Menü	Wert
VPN-Szenario	Assistenten -> VPN -> VPN-Verbindungen -> Neu	IPSec - LAN-zu-LAN-Verbindung
Beschreibung	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. IP-Sec_Connection_1
Lokale IPSec ID	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	Zentrale
Entfernte IPSec ID	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	Filiale
Preshared Key	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	Passwort eingeben
Lokale IP-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. 172.16.0.254

Feld	Menü	Wert
Entferntes IPv4-Netzwerk	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. 192.168.0.0
Netzmaske	Assistenten -> VPN -> VPN-Verbindungen -> Neu -> Weiter	z. B. 255.255.255.0

## Kapitel 8 IP - Einrichtung einer DMZ mit der Funktionalität der Drop-In-Gruppe

### 8.1 Einleitung

Im Folgenden wird die Einrichtung einer DMZ (Demilitarized Zone) mit der Funktionalität der Drop-In-Gruppe beschrieben.

Die Lösung kann zum Beispiel dann sinnvoll sein, wenn einem ein kleines IP-Netzwerk mit öffentlichen Adressen zur Verfügung steht. Der Anschluß an das Internet erfolgt dabei über ein vom Provider gemanagtes Gateway ohne eigenen administrativen Zugang.

Ein **bintec**-Router mit der Drop-In-Funktionalität wird zwischen das Provider-Gateway und die Hosts der DMZ platziert. Die Drop-In-Gruppe stellt nun die Verbindung zwischen dem Gateway und der DMZ her, ohne dass dabei das gemeinsame IP-Netz getrennt wird. Zusätzlich wird ein privates LAN-Netzwerk über das Gateway angebunden.

Der Verkehr zwischen den Schnittstellen des Gateways und damit zwischen dem Provider-Gateway, der DMZ und dem LAN kann dann mit Firewall-Regeln kontrolliert werden. Für das Gateway wird eine Adresse aus dem öffentlichen IP-Netz benötigt.

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

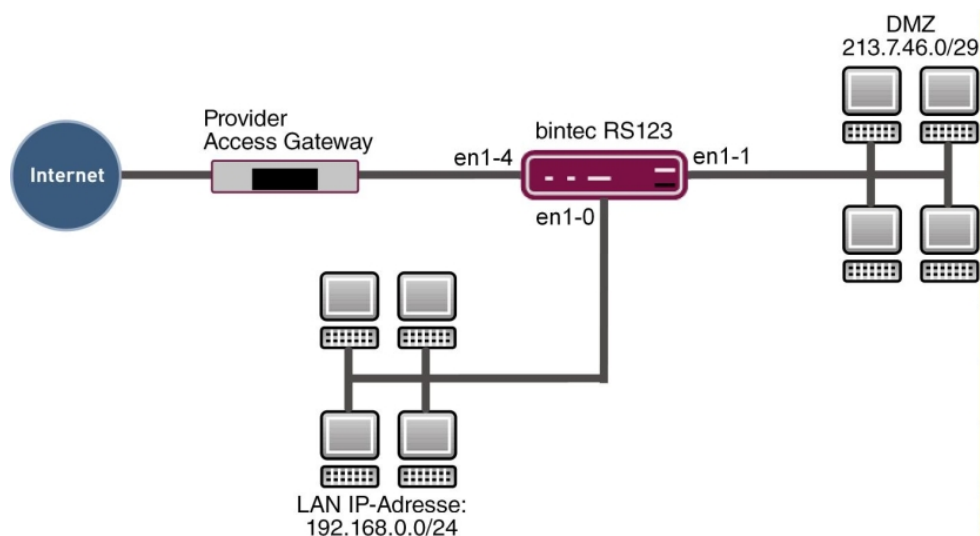


Abb. 83: Beispielszenario



## Voraussetzungen

- Ein **bintec**-Router, z. B. **bintec RS123**
- Firmware Version mindestens 10.2.5
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang mit öffentlichen Adressen. Hier als Beispiel **Company Connect** mit acht IP-Adressen.

## 8.2 Konfiguration

In unserem Beispiel wird für das private LAN das auf dem Gateway voreingestellte IP-Netz verwendet. Öffnen Sie einen Web-Browser und stellen Sie eine http-Verbindung zu dem Gerät her.

### 8.2.1 Konfiguration der Ports

Als erstes wird eine zusätzliche Ethernet-Schnittstelle benötigt. Eine Ethernet-Schnittstelle ist eine physikalische Schnittstelle zur Anbindung an das lokale Netzwerk oder zu externen Netzwerken.

Weisen Sie einem Switch-Port eine neue Ethernet-Schnittstelle zu.

- (1) Gehen Sie zu **Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration**.

Switch-Konfiguration				
Automatisches Aktualisierungsintervall <input type="text" value="60"/>		Sekunden		ÜBERNEHMEN
Switch-Port	Ethernet-Schnittstellenauswahl	Konfigurierte Geschwindigkeit / Konfigurierter Modus	Aktuelle Geschwindigkeit / Aktueller Modus	Flusskontrolle
1	<input type="text" value="en1-0"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	Inaktiv	<input type="text" value="Deaktiviert"/>
2	<input type="text" value="en1-0"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	Inaktiv	<input type="text" value="Deaktiviert"/>
3	<input type="text" value="en1-0"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	Inaktiv	<input type="text" value="Deaktiviert"/>
4	<input type="text" value="en1-1"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	100 Mbit/s / Full Duplex	<input type="text" value="Deaktiviert"/>
5	<input type="text" value="en1-4"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	Inaktiv	<input type="text" value="Deaktiviert"/>

Abb. 84: **Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration**

Gehen Sie folgendermaßen vor, um den Port der Schnittstelle zuzuordnen:

- (1) Wählen Sie bei **Ethernet-Schnittstellenauswahl** für den **Switch-Port 4** *en1-1* im Dropdown-Menü aus.

- (2) Bestätigen Sie mit **OK**.

## 8.2.2 Konfiguration der Drop-In-Gruppe

Im nächsten Schritt wird eine Drop-In-Gruppe angelegt.

- (1) Gehen Sie zu **Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu**.

### Basisparameter

Gruppenbeschreibung  
DropIn-Gruppe

Modus Transparent ▾

Vom NAT ausnehmen (DMZ)  Aktiviert

Netzwerkconfiguration Statisch ▾

Netzwerkadresse  
213.7.46.0

Netzmaske  
255.255.255.248

Lokale IP-Adresse  
213.7.46.6

ARP Lifetime  
3600 Sekunden

DNS-Zuweisung über DHCP Unverändert ▾

Schnittstellenauswahl



Schnittstelle	
<span>LAN_EN1-4 ▾</span>	
<span>LAN_EN1-1 ▾</span>	

Abb. 85: **Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine eindeutige **Gruppenbeschreibung** für die Drop-In-Gruppe ein, z. B. *DropIn-Gruppe*.
- (2) Bei **Modus** wählen Sie *Transparent* aus. ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden transparent (unverändert) weitergeleitet.
- (3) Unter **Netzwerkconfiguration** wählen Sie aus, auf welche Weise den Netzwerkkomponenten eine IP-Adresse zugewiesen wird, hier *Statisch*.
- (4) Geben Sie die **Netzwerkadresse** des Drop-In-Netzwerks ein, hier z. B. *213.7.46.0*.
- (5) Geben Sie die zugehörige **Netzmaske** ein, hier z. B. *255.255.255.248*.
- (6) Geben Sie die **Lokale IP-Adresse** der Drop-In-Gruppe ein, hier z. B. *213.7.46.6*.
- (7) Bei **Schnittstellenauswahl** wählen Sie alle Ports aus, die in der Drop-In-Gruppe (im Netzwerk) enthalten sein sollen, hier z. B. *LAN\_EN1-1* und *LAN\_EN1-4*.
- (8) Bestätigen Sie mit **OK**.

### 8.2.3 Einrichten der Standardroute

Als Nächstes wird eine Standardroute auf dem Gateway eingerichtet. Dabei muß die Schnittstelle der Drop-In-Gruppe ausgewählt werden, an der später das Gateway angeschlossen ist.

- (1) Gehen Sie zu **Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu**.

The screenshot shows a configuration window for IPv4 routes, divided into two main sections: 'Basissparameter' (Basic parameters) and 'Routenparameter' (Route parameters). In the 'Basissparameter' section, 'Routentyp' is set to 'Standardroute über Gateway', 'Schnittstelle' is set to 'LAN\_EN1-4', and 'Routenklasse' has 'Standard' selected with a radio button. In the 'Routenparameter' section, 'Gateway-IP-Adresse' is set to '213.7.46.1' and 'Metrik' is set to '1'.

Abb. 86: **Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu**

Gehen Sie folgendermaßen vor:

- (1) Bei **Routentyp** wählen Sie *Standardroute über Gateway* aus.
- (2) Wählen Sie die **Schnittstelle** aus, welche für diese Route verwendet werden soll, hier *LAN\_EN1-4*.
- (3) Bei **Gateway-IP-Adresse** geben Sie die IP-Adresse des Provider-Gateways ein, hier z. B. *213.7.46.1*.
- (4) Bestätigen Sie mit **OK**.

## 8.2.4 Network Address Translation (NAT) aktivieren

NAT wird auf der Schnittstelle der Drop-In-Gruppe aktiviert, die mit dem Gateway verbunden ist. Nur der Verkehr aus dem privaten LAN wird das NAT durchlaufen, aufgrund der bei der Drop-In-Gruppen-Konfiguration gesetzten Option **Vom NAT ausnehmen (DMZ)**.

Im Menü NAT-Schnittstellen wird eine Liste aller IP-Schnittstellen angezeigt.

Gehen Sie in folgendes Menü, um NAT für ihre Schnittstelle einzuschalten:

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

NAT-Schnittstellen					
Schnittstelle	NAT aktiv	Loopback aktiv	Verwerfen ohne Rückmeldung	PPTP-Passthrough	Portweiterleitungen
LAN_EN1-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0

Abb. 87: **Netzwerk -> NAT -> NAT-Schnittstellen**

Gehen Sie folgendermaßen vor:

- (1) Für die Schnittstelle `LAN_EN1-4` setzen Sie bei **NAT aktiv** einen Haken. Damit schalten Sie das Feature NAT für die Schnittstelle ein.
- (2) Setzen Sie bei **Verwerfen ohne Rückmeldung** auch einen Haken. Wenn diese Funktion aktiviert wird, werden Zugriffsversuche von außen auf das LAN ohne Rückmeldung verworfen.
- (3) Bestätigen Sie mit **OK**.

## 8.2.5 Konfiguration der Firewall

Es wird nun die Firewall aktiviert um den Verkehr zwischen den einzelnen Zonen (LAN, DMZ und Internet) zu kontrollieren.

Dabei sollen vom LAN ausgehende Verbindungen überall hin, sowie von der DMZ ausgehende Verbindungen ins Internet generell erlaubt sein. Der übrige Verkehr ist standardmäßig blockiert.

Für die Dienste auf den Servern in der DMZ, die vom Internet aus erreichbar sein sollen, wird jeweils eine Filterregel erstellt. In unserem Beispiel sind dies ein Web-Server und zusätzlich ein E-Mail-Server, der E-Mails empfangen soll, und zusätzlich die Möglichkeit bietet, von außen über eine verschlüsselte Verbindung E-Mails mit pop3 oder imap abzurufen.

Die Grundeinstellung der Firewall ist es, den Verkehr auf allen Schnittstellen zu blockieren. Daher ist alles verboten, was nicht explizit erlaubt ist.

In der Standardeinstellung wird die Firewall aktiv wenn die erste Regel konfiguriert ist. Daher ist es wichtig, dass die erste Regel auch den Konfigurationszugriff auf den Router selbst erlaubt.

### Konfiguration der Alias-Namen für die IP-Adressen der Server

Um die Server bei der Konfiguration der Filterregeln identifizieren zu können, werden Alias-Namen für die IP-Adressen des Web- und E-Mail-Servers angelegt.

Gehen Sie in folgendes Menü, um Aliasnamen zu erstellen:

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

The screenshot shows a configuration window titled 'Basisparameter' with a dark red header. Below the header, there are several input fields and controls:

- Beschreibung:** A text input field containing 'WebServer'.
- IPv4:** A toggle switch that is turned on, labeled 'Aktiviert'.
- Adresstyp:** Two radio button options: 'Adresse/Subnetz' (which is selected) and 'Adressbereich'.
- Adresse/Subnetz:** Two text input fields. The first contains '213.7.46.2' and the second contains '255.255.255.255', separated by a slash.
- IPv6:** A toggle switch that is turned off, labeled 'Deaktiviert'.

Abb. 88: Firewall -> Adressen -> Adressliste -> Neu

Gehen Sie folgendermaßen vor:

- (1) Tragen Sie bei **Beschreibung** den Namen des Aliases ein, z. B. *WebServer*.
- (2) Wählen Sie bei **Adresstyp** *Adresse/Subnetz*.
- (3) Tragen Sie bei **Adresse/Subnetz** die IP-Adresse und die zugehörige Subnetzmaske ein, hier z. B. *213.7.46.2* und *255.255.255.255*.
- (4) Bestätigen Sie mit **OK**.

Verfahren Sie analog für die Konfiguration des Aliasnamens für den E-Mail-Server.

- (1) Gehen Sie zu **Firewall -> Adressen -> Adressliste -> Neu**.
- (2) Tragen Sie bei **Beschreibung** den Namen des Alias ein, z. B. *EMailServer*.
- (3) Wählen Sie bei **Adresstyp** *Adresse/Subnetz*.
- (4) Tragen Sie bei **Adresse/Subnetz** die IP-Adresse und die zugehörige Subnetzmaske ein, hier z. B. *213.7.46.3* und *255.255.255.255*.
- (5) Bestätigen Sie mit **OK**.

### Konfiguration von Dienstgruppen

Die Server sollen jeweils mehrere Dienste zur Verfügung stellen. Um die Konfiguration der Filterregeln zu vereinfachen, können Sie mehrere Dienste zu Gruppen zusammenfassen.

Gehen Sie in folgendes Menü, um eine Gruppe zu erstellen:

- (1) Gehen Sie zu **Firewall -> Dienste -> Gruppen -> Neu**.

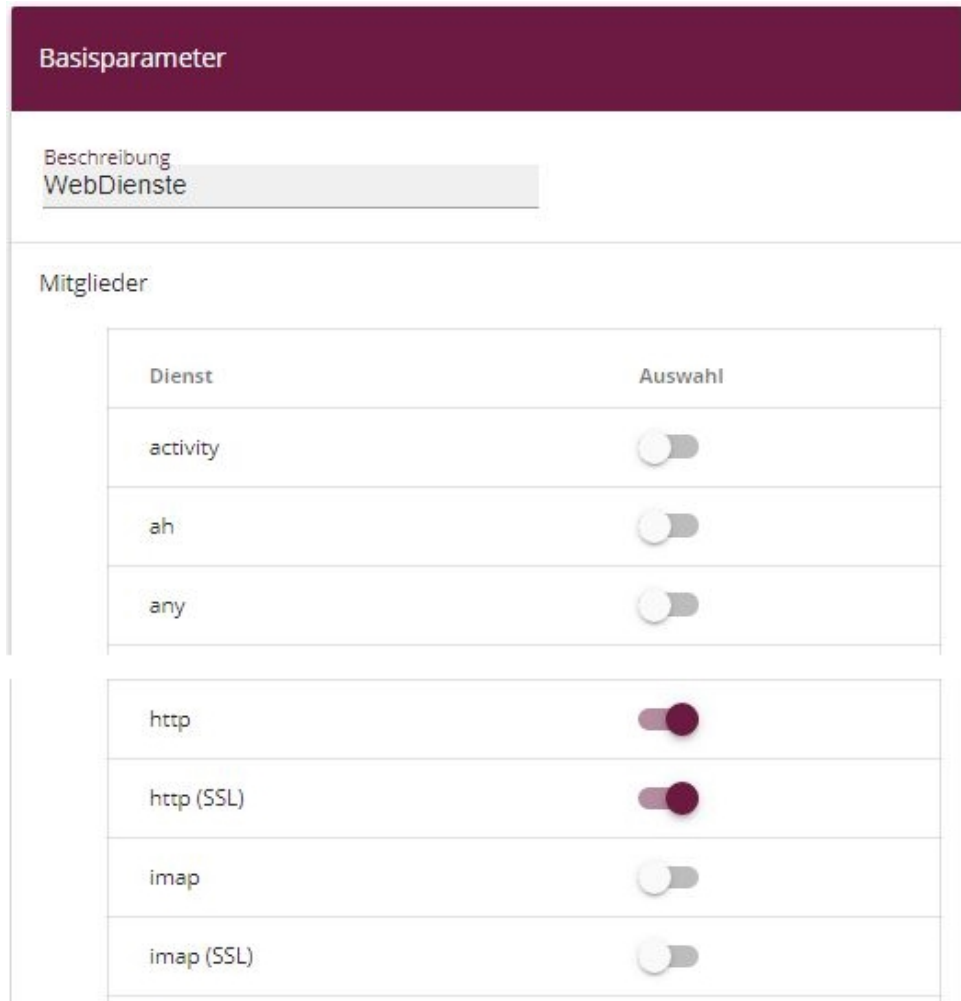


Abb. 89: Firewall -> Dienste -> Gruppen -> Neu

Gehen Sie folgendermaßen vor, um eine Gruppe zu erstellen:

- (1) Tragen Sie bei **Beschreibung** einen Namen für die Gruppe ein, z. B. *WebDienste*.
- (2) Setzen Sie den Haken bei den Diensten, die Mitglieder dieser Gruppe sein sollen, hier *http* und *http (SSL)*.
- (3) Bestätigen Sie mit **OK**.

Verfahren Sie analog für die Konfiguration der Dienstgruppe für den E-Mail-Server.

- (1) Gehen Sie zu **Firewall -> Dienste -> Gruppen -> Neu**.
- (2) Tragen Sie bei **Beschreibung** einen Namen des Gruppe ein, z. B. *EMailDienste*.



- (3) Setzen Sie den Haken bei den Diensten, die Mitglieder dieser Gruppe sein sollen, hier *smtp* , *pop3 (SSL)* und *imap (SSL)*.
- (4) Bestätigen Sie mit **OK**.

### Konfiguration der Richtlinien



#### Hinweis

Die korrekte Konfiguration der Filterregeln und die richtige Anordnung in der Filterregelkette sind entscheidend für die Funktion der Firewall. Eine fehlerhafte Konfiguration kann unter Umständen dazu führen, dass keine Kommunikation mit dem Router mehr möglich ist!

Nachdem die Konfiguration der Aliasnamen für IP-Adressen und Dienste abgeschlossen ist, können Sie nun die Filterregeln definieren.

Zur Konfiguration der ersten Regel gehen Sie folgendermaßen vor:

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

Basisparameter	
Quelle	LAN_EN1-0
Ziel	ANY
Dienst	any
Aktion	Zugriff

Abb. 90: Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie die **Quelle** des Pakets aus, hier *LAN\_EN1-0*.
- (2) Wählen Sie als **Ziel** *ANY* aus. Weder Ziel-Schnittstelle noch Ziel-Adresse werden überprüft.
- (3) Bei **Dienst** wählen Sie *any* aus.
- (4) Wählen Sie die **Aktion** aus, die angewendet werden soll, hier *Zugriff*. Die Pakete werden entsprechend den Angaben weitergeleitet.

- (5) Bestätigen Sie mit **OK**.

Mit diesen Einstellungen sind ausgehende Verbindungen vom LAN zur DMZ und zum Internet erlaubt, einschließlich des LAN-seitigen Zugriffs auf den Router.

Konfigurieren Sie die zweite Filterregel analog zur Konfiguration der ersten Regel.

- (1) Gehen Sie zu **Firewall -> Richtlinien ->IPv4- Filterregeln -> Neu**.
- (2) Wählen Sie die **Quelle** des Pakets aus, hier *LAN\_EN1-1*.
- (3) Wählen Sie als **Ziel** *LAN\_EN1-4* aus. Quell- und Ziel-Schnittstelle werden überprüft.
- (4) Bei **Dienst** wählen Sie *any* aus.
- (5) Wählen Sie die **Aktion** aus, die angewendet werden soll, hier *Zugriff*. Die Pakete werden entsprechend den Angaben weitergeleitet.
- (6) Bestätigen Sie mit **OK**.  
Mit diesen Einstellungen sind ausgehende Verbindungen von der DMZ zum Internet erlaubt.

Nun kann die Regel für den Zugriff vom Internet zum Web-Server erstellt werden.

- (1) Gehen Sie zu **Firewall -> Richtlinien ->IPv4- Filterregeln -> Neu**.
- (2) Wählen Sie die **Quelle** des Pakets aus, hier *LAN\_EN1-4*.
- (3) Wählen Sie als **Ziel** *WebServer* aus.
- (4) Bei **Dienst** wählen Sie *WebDienste* aus.
- (5) Wählen Sie die **Aktion** aus, die angewendet werden soll, hier *Zugriff*. Die Pakete werden entsprechend den Angaben weitergeleitet.
- (6) Bestätigen Sie mit **OK**.

Anschließend wird noch die Regel für den Zugriff vom Internet zum E-Mail-Server erstellt.

- (1) Gehen Sie zu **Firewall -> Richtlinien ->IPv4- Filterregeln -> Neu**.
- (2) Wählen Sie die **Quelle** des Pakets aus, hier *LAN\_EN1-4*.
- (3) Wählen Sie als **Ziel** *EMailServer* aus.
- (4) Bei **Dienste** wählen Sie *EMailDienste* aus.
- (5) Wählen Sie die **Aktion** aus, die angewendet werden soll, hier *Zugriff* . Die Pakete werden entsprechend den Angaben weitergeleitet.
- (6) Bestätigen Sie mit **OK**.

Die Liste der konfigurierten Filterregeln sollte nun wie folgt aussehen:

Gehen Sie zu **Firewall -> Richtlinien ->IPv4- Filterregeln**.

Filterregeln						
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv	
1	LAN_EN1-0	ANY	any	Zugriff	<input checked="" type="checkbox"/> Aktiviert	⌵ ⌵ ⌵ ✎
2	LAN_EN1-1	LAN_EN1-4	any	Zugriff	<input checked="" type="checkbox"/> Aktiviert	⌵ ⌵ ⌵ ✎
3	LAN_EN1-4	WebServer	WebDienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert	⌵ ⌵ ⌵ ✎
4	LAN_EN1-4	E-Mail-Server	E-Mail-Dienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert	⌵ ⌵ ⌵ ✎

Abb. 91: Firewall -> Richtlinien -> IPv4- Filterregeln

Die Konfiguration ist somit abgeschlossen. Speichern Sie die Konfiguration mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

## 8.3 Konfigurationsschritte im Überblick

### Schnittstelle zuweisen

Feld	Menü	Wert
Switch-Port 4	Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration	en1-1

### Drop-In-Gruppe konfigurieren

Feld	Menü	Wert
Gruppenbeschreibung	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>DropIn-Gruppe</i>
Modus	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	<i>Transparent</i>
Netzwerkconfiguration	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	<i>Statisch</i>
Netzwerkadresse	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>213.7.46.0</i>
Netzmaske	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>255.255.255.248</i>
Lokale IP-Adresse	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>213.7.46.6</i>
Schnittstellenauswahl	Netzwerk -> Drop In -> Drop-In-Gruppen -> Neu	z. B. <i>LAN_EN1-4, LAN_EN1-1</i>

### Standardroute einrichten

Feld	Menü	Wert
Routentyp	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	Standardroute über Gateway
Schnittstelle	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	LAN_EN1-4
Gateway-IP-Adresse	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	z. B. 213.7.46.1

#### Aktivierung von NAT

Feld	Menü	Wert
NAT aktiv	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für LAN_EN1-4
Verwerfen ohne Rückmeldung	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für LAN_EN1-4

#### Konfiguration der Alias-Namen

Feld	Menü	Wert
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	WebServer
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	Adresse/Subnetz
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. 213.7.46.2 / 255.255.255.255
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	EMailServer
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	Adresse/Subnetz
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. 213.7.46.3 / 255.255.255.255

#### Konfiguration von Dienstgruppen

Feld	Menü	Wert
Beschreibung	Firewall -> Dienste -> Gruppen -> Neu	z. B. WebDienste
Mitglieder	Firewall -> Dienste -> Gruppen -> Neu	http, http (SSL)
Beschreibung	Firewall -> Dienste -> Gruppen -> Neu	z. B. EMailDienste
Mitglieder	Firewall -> Dienste -> Gruppen ->	smtp, pop3 (SSL),

Feld	Menü	Wert
	Neu	<i>imap (SSL)</i>

#### Konfiguration der Richtlinien

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>LAN_EN1-0</i>
Ziel	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>ANY</i>
Dienst	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>LAN_EN1-1</i>
Ziel	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>LAN_EN1-4</i>
Dienst	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>LAN_EN1-4</i>
Ziel	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>WebServer</i>
Dienst	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>WebDienste</i>
Aktion	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>LAN_EN1-4</i>
Ziel	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>EMailServer</i>
Dienst	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>EMailDienste</i>
Aktion	Firewall -> Richtlinien -> IPv4- Filterregeln -> Neu	<i>Zugriff</i>



# Kapitel 9 IP - DSL-Backup über LTE (bintec 4e-LE)

## 9.1 Einleitung

Im Folgenden beschreiben wir die Konfiguration, die notwendig ist, um im Fall eines Ausfalls der DSL-Verbindung mit einer **bintec 4GE-LE** automatisch eine Internetverbindung über das Mobilfunknetz aufzubauen. Der Anschluss des **bintec 4GE-LE** erfolgt am blauen LAN5-Anschluss des Routers.



### Hinweis

Die Bezeichnung der Anschlüsse des Routers unterscheidet sich in Abhängigkeit davon, wo sie verwendet wird: So bezeichnet *LAN5* die Buchse, in die Sie das Kabel stecken, *ETH5* (Ethernet 5) die Art der Verbindung (Ethernet), die über die Buchse realisiert wird. Schließlich bezeichnet *en1-4* eine sog. "Schnittstelle", eine logische Verbindung, von denen ggf. z. B. auch mehrere über eine Ethernet-Verbindung realisiert werden können.

## Voraussetzungen

- Ein Router z. B. **bintec be.IP** in der **Ansicht** = *Vollzugriff* mit Firmwareversion 10.2.01 oder höher.
- Ein **bintec 4Ge-LE**.

## 9.2 Router konfigurieren

### 9.2.1 IP-Konfiguration der Schnittstelle

Zunächst konfigurieren Sie die IP-Adresse der ausgewählten Ethernet-Schnittstelle (LAN5 = ETH5 = en1-4).

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

**Basisparameter**

Schnittstellenmodus  Untagged  Tagged (VLAN)

MAC-Adresse   Voreingestellte verwenden

**Grundlegende IPv4-Parameter**

Sicherheitsrichtlinie  Nicht Vertrauenswürdig  Vertrauenswürdig

Adressmodus  Statisch  DHCP

IP-Adresse / Netzmaske

IP-Adresse	Netzmaske
<input type="text" value="192.168.43.41"/>	<input type="text" value="255.255.255.252"/> <input type="button" value="🗑️"/>

HINZUFÜGEN

**Grundlegende IPv6-Parameter**

IPv6

- (2) Fügen Sie eine neue **IP-Adresse / Netzmaske** hinzu, z. B. *192.168.43.41 / 255.255.255.252*.
- (3) Bestätigen Sie Ihre Einstellungen mit **OK**.



### Hinweis

Die Netzmaske für en1-4 wurde bewusst mit 255.255.255.252 gewählt, da nur ein Bereich von zwei Adressen benötigt wird.

bintec be.IP: 192.168.43.41

bintec 4Ge-LE: 192.168.43.42

Netzwerkadresse ist damit die 192.168.43.40, Broadcastadresse ist 192.168.43.43



## 9.2.2 DHCP-Server für bintec 4Ge-LE einrichten

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

The screenshot shows a web form titled "Basisparameter" for configuring a new DHCP IP pool. The form has a dark red header. Below the header, there are three main sections:

- IP-Poolname:** A text input field containing "bintec 4GE-LE".
- IP-Adressbereich:** Two text input fields for start and end IP addresses, both containing "192.168.43.42", separated by a hyphen.
- DNS-Server:** Two text input fields labeled "Primär" and "Sekundär", both of which are currently empty.

- (2) Geben Sie einen **IP-Poolnamen** ein, z. B. *bintec 4GE-LE*.
- (3) Tragen Sie im **IP-Adressbereich** die Start- und End-Adresse des bintec 4GE-LE ein, hier z. B. *192.168.43.42 - 192.168.43.42*.
- (4) Bestätigen Sie Ihre Einstellungen mit **OK**.
- (5) Gehen Sie in das Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu.**

The screenshot shows a web form titled "Basisparameter" for configuring a new DHCP configuration. The form has a dark red header. Below the header, there are four main sections:

- Schnittstelle:** A dropdown menu with "en1-4" selected.
- IP-Poolname:** A dropdown menu with "bintec 4GE-LE" selected.
- Pool-Verwendung:** A dropdown menu with "Lokal" selected.
- Beschreibung:** A text input field containing "bintec 4GE-LE APN/PIN".

- (6) Im Bereich **Basisparameter** wählen Sie die **Schnittstelle** *en1-4* aus.
- (7) Bei **IP-Poolname** wählen Sie den zuvor erstellten Pool *bintec 4GE-LE* aus.
- (8) Geben Sie eine **Beschreibung** ein, z. B. *bintec 4GE-LE APN/PIN*.

- (9) Klicken Sie auf **Erweiterte Einstellungen**.

- (10) Klicken Sie auf **Hersteller-String hinzufügen**.

- (11) In dem Popup-Menü wählen Sie bei **Hersteller auswählen** *bintec 4Ge* aus.
- (12) Tragen Sie den **APN** (Access Point Namen) ein, hier z. B. *internet.telekom* Erfragen Sie den APN Ihres LTE-Vertrags ggf. bei Ihrem Mobilfunkbetreiber.
- (13) Gebe Sie die **PIN** der SIM-Karte ein, z. B. *1234*.
- (14) Klicken Sie auf **Übernehmen**.
- (15) Bestätigen Sie Ihre Einstellungen mit **OK**.
- (16) Schließen Sie nun den vorbereiteten bintec 4Ge-LE an den blauen LAN5-Anschluss des Routers an.
- (17) Um zu vermeiden, dass ein anderes Gerät eine IP-Adresse bekommt, kann nach der ersten Vergabe einer IP-Adresse an den bintec 4Ge-LE eine IP/MAC-Bindung eingerichtet werden. Gehen Sie dazu in das Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung**.

- (18) Aktivieren Sie bei dem Eintrag des bintec 4Ge-LE die Option **Statische Bindung**.

## 9.2.3 Virtuelle Schnittstelle löschen

Sollte eine virtuelle Schnittstelle en1-4-1 (VLAN-ID8) angelegt worden sein, muss diese gelöscht werden.

Gehen Sie dazu in das Menü **LAN->IP-Konfiguration->Schnittstellen**. Mithilfe des  - Symbols löschen Sie die virtuelle Schnittstelle en1-4-1 (VLAN-ID8).

Ethernet-/VLAN-Ports					
Schnittstelle	IPv4-Adresse/Netzmaske	IPv6-Adresse/Länge	Status	Aktion	
en1-4	192.168.43.41/255.255.255.252	-	<span style="color: red;">✘</span>	^ v	
efm35-50	Nicht konfiguriert/Nicht konfiguriert	-	<span style="color: red;">✘</span>	^ v	
ethoa35-5	Nicht konfiguriert/Nicht konfiguriert	-	<span style="color: red;">✘</span>	^ v	
br0	192.168.0.100/255.255.255.0	Präfix: Germany - Telekom Entertain:0 Host: eui64	<span style="color: green;">✔</span>	^ v	
ethoa35-5-1(VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	<span style="color: red;">✘</span>	^ v	
efm35-50-1(VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	<span style="color: red;">✘</span>	^ v	
en1-4-1 (VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	<span style="color: red;">✘</span>	^ v	

## 9.2.4 Virtuelle Schnittstelle konfigurieren

Im nächsten Schritt konfigurieren Sie die virtuelle Schnittstelle en1-4-1 für LTE-Verbindung.

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

Basisparameter

Basierend auf Ethernet-Schnittstelle en1-4

Schnittstellenmodus  Untagged  Tagged (VLAN)

VLAN-ID

MAC-Adresse   Voreingestellte verwenden

Grundlegende IPv4-Parameter

Sicherheitsrichtlinie  Nicht Vertrauenswürdig  Vertrauenswürdig

Adressmodus  Statisch  DHCP

IP-Adresse / Netzmaske

HINZUFÜGEN

Grundlegende IPv6-Parameter

IPv6

- (2) Wähle Sie unter **Basierend auf Ethernet-Schnittstelle** die Schnittstelle *en1-4* aus.
- (3) Den **Schnittstellenmodus** legen Sie als *Tagged (VLAN)* fest.
- (4) Weisen Sie die Schnittstelle einem VLAN zu. Geben Sie bei **VLAN-ID** *463* ein.

- (5) Bei **Grundlegende IPv4-Parameter** wählen Sie die **Sicherheitsrichtlinie** *Nicht Vertrauenswürdig* aus.
- (6) Den **Adressmodus** stellen Sie auf *DHCP*.
- (7) Klicken Sie auf **Erweiterte Einstellungen**.

**Erweiterte IPv4-Einstellungen**

DHCP-MAC-Adresse   Voreingestellte verwenden

DHCP-Hostname

DHCP Broadcast Flag  Aktiviert

Standardroute erstellen

Proxy ARP

TCP-MSS-Clamping

- (8) Unter **Erweiterte IPv4-Einstellungen** schalten Sie die Option **Standardroute erstellen** aus.
- (9) Bestätigen Sie Ihre Einstellungen mit **OK**.  
Das Ergebnis sieht 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	192.168.0.100/255.255.255.0	Prefix: Germany - Telekom Enterstain0 Host: eu164	✔	^	∨
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)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✘	^	∨

### 9.2.4.1 Standardroute über bintec 4Ge-LE anlegen

- (1) Gehen Sie in das Menü **Netzwerk->Routen->Konfiguration von IPv4-Routen->Neu**, um die neue Standardroute zu konfigurieren.

Basisparameter		Parameter der Routing-Vorgabe	
Routentyp	(Vorlage für Standardroute per DHCP ▼)	Metrik	5 ▼
Schnittstelle	LAN_EN1-4-1 ▼		
Routenklasse	<input checked="" type="radio"/> Standard <input type="radio"/> Erweitert		

- (2) Wählen Sie den **Routentyp** *Vorlage für Standardroute per DHCP*.
- (3) Wählen Sie die **Schnittstelle** *LAN\_EN1-4-1*.
- (4) Wählen Sie die **Metrik** *5*.
- (5) Bestätigen Sie Ihre Einstellungen mit **OK**.

### 9.2.5 NAT aktivieren

Im nächsten Schritt aktivieren Sie NAT für die Schnittstelle *en1-4-1*.

Gehen Sie folgendermaßen vor:

- (1) Gehen Sie in das Menü **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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-4-1	<input checked="" type="checkbox"/>	<input 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_ETH0A35-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
WAN_ETH0A35-5-1	<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

- (2) Schalten Sie NAT für die Schnittstelle **LAN\_EN1-4-1** ein (**NAT aktiv**).
- (3) Aktivieren Sie die Option **Verwerfen ohne Rückmeldung**.
- (4) Bestätigen Sie Ihre Einstellungen mit **OK**.

## 9.3 Optionale Einstellungen: Telefonie an die DSL-Verbindung binden

In einem zusätzlichen Schritt können Sie Ihr VoIP-Konto an den DSL-Zugang binden. Dies hat den Vorteil, dass Telefonieverbindungen, die über LTE oftmals nicht möglich sind, über die Backup-Verbindung erst gar nicht versucht werden. Fragen Sie ggf. bei Ihrem LTE-Anbieter nach, ob VoIP-Verbindungen über LTE aufgebaut werden können.

Gehen Sie folgendermaßen vor:

- (1) Gehen Sie in das Menü **VoIP->Einstellungen->Standorte->Neu**

The screenshot shows the 'Grundeinstellungen' (Basic Settings) configuration page for a SIP account binding. The page is divided into several sections:

- Beschreibung:** A text input field containing 'SIP-Account-Bindung-WAN-Interface'.
- Beinhalteter Standort (Parent):** A dropdown menu set to 'Keiner'.
- Typ:** Radio buttons for 'Adressen' (unselected) and 'Schnittstellen' (selected).
- Schnittstellen:** A list of interfaces with a dropdown menu showing 'WAN\_GERMANY - TELEKOM ENTERTAIN' and a trash icon to the right.
- HINZUFÜGEN:** A button to add a new interface.
- Bandbreitenbegrenzung Upstream:** A toggle switch that is currently turned off.
- Bandbreitenbegrenzung Downstream:** A toggle switch that is currently turned off.


Abb. 104: **VoIP->Einstellungen->Standorte->Neu**

- (2) Geben Sie eine **Beschreibung** ein, z. B. *SIP-Account-Bindung-WAN-Interface*.
- (3) Wählen Sie den **Typ** *Schnittstellen*.
- (4) Klicken Sie unter **Schnittstellen** auf **Hinzufügen** und wählen Sie die gewünschte **Schnittstelle** aus, z. B. *WAN\_GERMANY - TELEKOM ENTERTAIN*
- (5) Bestätigen Sie Ihre Einstellungen mit **OK**.

Im nächsten Schritt passen Sie die Standortkonfiguration für alle konfigurierten VoIP-Konten an.

Gehen Sie folgendermaßen vor:

- (1) Gehen Sie in das Menü **VoIP->Einstellungen->SIP-Provider**.

- (2) Wenn die Liste mehrere Einträge enthält, wählen Sie den obersten Eintrag mit .
- (3) Klicken Sie auf **Erweiterte Einstellungen**.

### Weitere Einstellungen

From Domain

Anzahl der zulässigen gleichzeitigen Gespräche Uneingeschränkt ▼

**Standort** SIP-Account-Bindung-WAN-Interface ▼

Wahlendeüberwachungstimer  Sekunden

Halten im System  Aktiviert

Anrufweitschaltung extern (SIP 302)

Internationale Rufnummer erzeugen




Nationale Rufnummer erzeugen

- (4) Wählen Sie unter **Standort** den oben konfigurierten Standort, z. B. *SIP-Account-Bindung-WAN-Interface*.
- (5) Bestätigen Sie Ihre Einstellungen mit **OK**.
- (6) Wiederholen Sie den Vorgang gegebenenfalls für alle weiteren SIP-Account-Einträge in der Liste.
- (7) Klicken Sie auf die Schaltfläche **Konfiguration speichern** oben rechts, um Ihre Konfiguration zu speichern.

Die Konfiguration des Routers ist hiermit abgeschlossen. Speichern Sie die Konfiguration!

## 9.4 Konfigurationsschritte im Überblick

### IP-Konfiguration der LAN-Schnittstelle

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

### DHCP-Konfiguration

Feld	Menü	Wert
IP-Poolname	Lokale Dienste ->DHCP-Server ->IP-Pool-Konfiguration ->Neu	z. B. <i>bintec 4Ge-LE</i>
IP-Adressbereich	Lokale Dienste ->DHCP-Server ->IP-Pool-Konfiguration ->Neu	z. B. 192.168.43.42 - 192.168.43.42
Schnittstelle	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu	en1-4
IP-Poolname	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu	<i>bintec 4Ge-LE</i>
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	<i>bintec 4Ge</i>
APN	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu ->Erweiterte Einstellungen	z. B. <i>internet.telekom</i>
PIN	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration ->Neu ->Erweiterte Einstellungen	z. B. 1234
Statische Bindung	Lokale Dienste ->DHCP-Server ->IP/MAC-Bindung	Aktiviert



## Virtuelle Schnittstelle anlegen

Feld	Menü	Wert
Schnittstelle en1-4-1(VLAN-ID8)	LAN ->IP-Konfiguration ->Schnittstellen	Löschen
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
Standardroute erstellen	LAN ->IP-Konfiguration ->Schnittstellen ->Neu	Deaktiviert

## Route anlegen

Feld	Menü	Wert
Routentyp	Netzwerk ->Routen ->Konfiguration von IPv4-Routen ->Neu	Vorlage für Standardroute per DHCP
Schnittstelle	Netzwerk ->Routen ->Konfiguration von IPv4-Routen ->Neu	LAN-EN1-4-1
Metrik	Netzwerk ->Routen ->Konfiguration von IPv4-Routen ->Neu	z. B. 5

## NAT aktivieren

Feld	Menü	Wert
LAN_EN1-4-1	Netzwerk ->NAT ->NAT-Schnittstellen	NAT aktiv
LAN_EN1-4-1	Netzwerk ->NAT ->NAT-Schnittstellen	Verwerfen ohne Rückmeldung

## Account an Schnittstelle binden (Optional)

Feld	Menü	Wert
Beschreibung	VoIP ->Einstellungen ->Standorte ->Neu	z. B. SIP-Account-Bindung-WAN-Interface
Typ	VoIP ->Einstellungen ->Standorte -	Schnittstellen

Feld	Menü	Wert
	>Neu	
<b>Schnittstelle</b>	<b>VoIP -&gt;Einstellungen -&gt;Standorte -&gt;Neu</b>	z. B. <i>WAN_GERMANY - TELEKOM ENTERTAIN</i>
<b>Standort</b>	<b>VoIP -&gt;Einstellungen -&gt;SIP-Provider  Erweiterte Einstellungen</b>	<i>SIP-Account-Bindung-WAN-Interface</i>