



Benutzerhandbuch Workshops (Auszug)

IP-Workshops

Copyright© Version 01/2020 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.	3
1.3	Ergebnis.	6
1.4	Kontrolle.	6
1.5	Konfigurationsschritte im Überblick	6
Kapitel 2	IP - Konfiguration eines bintec Routers hinter einem Provider-Router	9
2.1	Einleitung	9
2.2	Konfiguration der Ports	10
2.3	Konfiguration des Internetzugangs	12
2.4	Konfiguration der DMZ	13
2.4.1	Aktivierung von NAT auf der DMZ-Schnittstelle	13
2.4.2	Konfiguration der Portweiterleitung	13
2.5	Überprüfen der Konfiguration.	15
2.5.1	Überprüfen der Portweiterleitung	15
2.5.2	Überprüfen der Funktionalität.	16
2.6	Konfigurationsschritte im Überblick	16
Kapitel 3	IP - IPTV am xDSL (ADSL/VDSL) T-Home Entertainment Anschluss	19
3.1	Einleitung	19

3.2	Konfiguration	21
3.2.1	Konfiguration des bintec RS120	21
3.2.2	Konfiguration des IPTV Multicast-Daten Zugangs	23
3.2.3	Konfiguration eines DHCP IP- Adress-Pools auf der LAN-Schnittstelle	28
3.2.4	Bootfähige Sicherung der Konfiguration	29
3.3	Konfigurationsschritte im Überblick	29
Kapitel 4	IP - Routing-Protokoll OSPF über IPsec-Verbindung	32
4.1	Einleitung	32
4.2	Konfiguration	33
4.2.1	Konfiguration des Gateways in der Zentrale	33
4.2.2	Konfiguration des Gateways am Standort A	38
4.2.3	Konfiguration des Gateways am Standort B	42
4.3	OSPF-Monitoring	46
4.4	Konfigurationsschritte im Überblick	51
Kapitel 5	IP - Routing-Protokoll RIPv2 über IPsec-Verbindung.	54
5.1	Einleitung	54
5.2	Konfiguration	55
5.2.1	Konfiguration des bintec R1202 am Standort B (Zentrale)	55
5.2.2	Konfiguration des bintec RS120 am Standort A (Außenstelle).	59
5.3	Kontrolle der Funktion	63
5.4	Konfigurationsschritte im Überblick	65
Kapitel 6	IP - ULA - Unique Local Addresses	67
6.1	Einleitung	67
6.2	Konfiguration	68

6.3	Konfigurationsschritte im Überblick	71
Kapitel 7	IP - IPv6 LAN-Routing	72
7.1	Einleitung	72
7.2	Konfiguration.	73
7.3	Konfigurationsschritte im Überblick	76
Kapitel 8	IP - Tunnel Broker SixXS mit dem ::/48-Präfix	79
8.1	Einleitung	79
8.2	Konfiguration	80
8.3	Konfigurationsschritte im Überblick	83
Kapitel 9	IP - Tunnel Broker SixXS mit ::/48-Präfix und Verteilung durch einen IPSec-Tunnel	85
9.1	Einleitung	85
9.2	Konfiguration	86
9.3	Konfigurationsschritte im Überblick	94
9.3.1	Konfiguration in der Zentrale	94
9.3.2	Konfiguration in der Außenstelle	96
Kapitel 10	IP - Lastverteilung von zwei parallel genutzten Internetzugän- gen	98
10.1	Einleitung	98
10.2	Konfiguration	99
10.2.1	Konfiguration der Internetzugänge	99
10.2.2	Einrichtung der IP-Lastverteilung	101
10.2.3	Spezielle Lastverteilungs-Behandlung von verschlüsselten Verbindungen	103
10.2.4	Hinweis zur DNS-Server Konfiguration	104

10.3	Konfigurationsschritte im Überblick	105
Kapitel 11	IP - Lastverteilung von zwei VPN IPSec-Tunneln über separate Internetzugänge	107
11.1	Einleitung	107
11.2	Konfiguration	108
11.2.1	Konfiguration des Gateways in der Zentrale	108
11.2.2	Konfiguration des Gateways in der Filiale	123
11.3	Konfigurationsschritte im Überblick	140
Kapitel 12	IP - Mit Drop In eine Filiale durch einen VPN-Tunnel mit der Zentrale verbinden	149
12.1	Einleitung	149
12.2	Konfiguration	150
12.3	Konfigurationsschritte im Überblick	155
Kapitel 13	IP - Einrichtung einer DMZ mit der Funktionalität der Drop-In-Gruppe	158
13.1	Einleitung	158
13.2	Konfiguration	159
13.2.1	Konfiguration der Ports	159
13.2.2	Konfiguration der Drop-In-Gruppe.	160
13.2.3	Einrichten der Standardroute	162
13.2.4	Network Address Translation (NAT) aktivieren	163
13.2.5	Konfiguration der Firewall	163
13.3	Konfigurationsschritte im Überblick	169
Kapitel 14	IP - DSL-Backup über LTE (bintec 4e-LE).	173

14.1	Einleitung	173
14.2	Router konfigurieren	173
14.2.1	IP-Konfiguration der Schnittstelle	173
14.2.2	DHCP-Server für bintec 4Ge-LE einrichten	176
14.2.3	Virtuelle Schnittstelle löschen	177
14.2.4	Virtuelle Schnittstelle konfigurieren	177
14.2.5	NAT aktivieren	179
14.3	Optionale Einstellungen: Telefonie an die DSL-Verbindung binden	180
14.4	Konfigurationsschritte im Überblick	181

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.

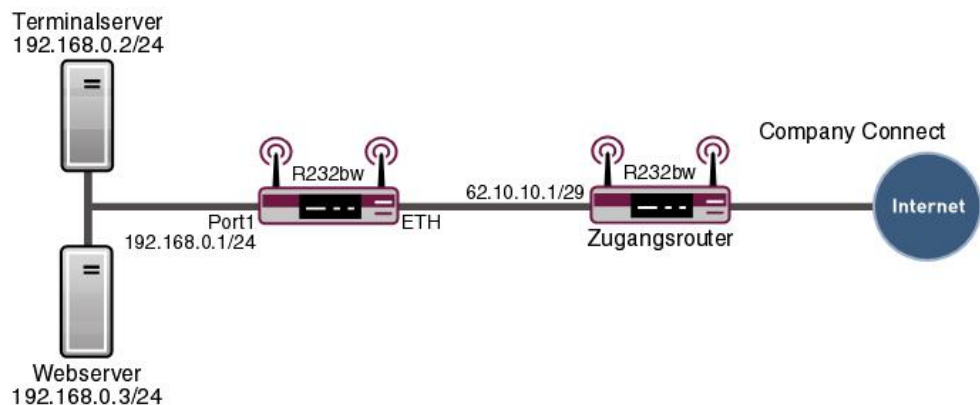


Abb. 1: Beispielszenario NAT

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Gateways
- Ein Bootimage der Version 7.10.1
- 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**.



Abb. 2: **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, 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 externen Port `8080` an.

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

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

Basisparameter	
Beschreibung	GUI
Schnittstelle	LAN_EN5-0
Art des Datenverkehrs	eingehend (Ziel-NAT)
Ursprünglichen Datenverkehr angeben	
Dienst	Benutzerdefiniert
Protokoll	TCP
Quell-IP-Adresse/Netzmaske	Host 62.10.10.2
Quell-Port/Bereich	Port angeben 8080 bis
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 <input type="checkbox"/> 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_EN5-0`.
- (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** geben Sie die externe IP-Adresse des Gateways ein, z. B. `62.10.10.2`.
- (7) Den **Quell-Port/Bereich** stellen Sie auf `Port angeben` ein und geben in das erste Eingabefeld z. B. `8080` ein.

- (8) Unter **Neuer Ziel-Port** deaktivieren Sie **Original** und geben in das Eingabefeld *80* ein.
- (9) 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**.

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_EN5-0*.
- (3) Die **Art des Datenverkehrs** wählen Sie *eingehend (Ziel-NAT)* aus.
- (4) Den **Dienst** stellen Sie auf *http*.
- (5) Unter **Quell-IP-Adresse/Netzmaske** geben Sie die IP-Adresse des internen Webserver ein, hier z. B. *62.10.10.3*.
- (6) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** 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

ver 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**.

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_EN5-0*.
- (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** geben Sie die IP-Adresse des internen Terminal-Servers ein, hier z. B. *62.10.10.4*.
- (7) Den **Port** stellen Sie auf *Port angeben* ein und geben in das erste Eingabefeld z. B. *5000* ein.
- (8) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** tragen die interne IP-Adresse, hier z. B. *192.168.0.2* ein.
- (9) Bei **Neuer Ziel-Port** deaktivieren Sie **Original** und geben in das Eingabefeld *3389* an.
- (10) 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_EN5-0
Verwerfen ohne Rückmeldung	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für LAN_EN5-0

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_EN5-0</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-	<i>TCP</i>

Feld	Menü	Wert
	Konfiguration -> Neu	
Quell-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>62.10.10.2</i>
Quell-Port/Bereich	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>Port angeben</i> mit <i>8080</i>
Neuer Ziel-Port	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>80</i>

Webserver

Feld	Menü	Wert
Beschreibung	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>Webserver</i>
Schnittstelle	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>LAN_EN5-0</i>
Art des Datenverkehrs	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>eingehend</i> (<i>Ziel-NAT</i>)
Dienst	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>http</i>
Quell-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>62.10.10.3</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>192.168.0.3</i>

Terminal Server

Feld	Menü	Wert
Beschreibung	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>Terminal-Server</i>
Schnittstelle	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>LAN_EN5-0</i>
Art des Datenverkehrs	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>eingehend</i> (<i>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>62.10.10.4</i>

Feld	Menü	Wert
Port	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>Port angeben z. B. 5000</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>z. B. 192.168.0.2</i>
Neuer Ziel-Port	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 RS232bw** 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.

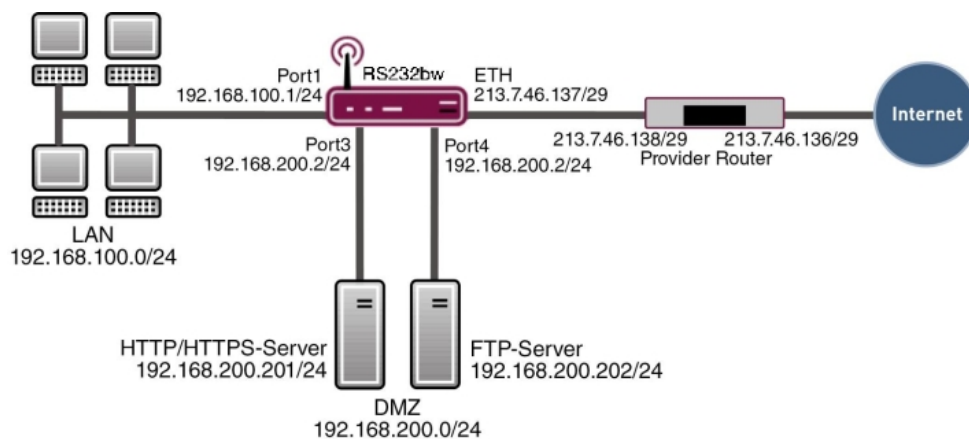


Abb. 6: Beispielszenario DMZ

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein **bintec RS232bw** Gateway
- Ein Bootimage der Version 9.1.5
- 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 RS232bw** 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**.

Portkonfiguration

Automatisches Aktualisierungsintervall: 300 Sekunden **Übernehmen**

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

Portkonfiguration

Schnittstelle	Konfigurierte Geschwindigkeit/konfigurierter Modus	Aktuelle Geschwindigkeit / Aktueller Modus
en5-0	Vollständige automatische Aushandlung	Inaktiv

OK **Abbrechen**

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>** .

The screenshot shows the configuration page for interface `en1-0`. On the left is a navigation menu with options like 'Assistenten', 'Systemverwaltung', 'Physikalische', 'Schnittstellen', 'LAN', 'IP-Konfiguration', 'VLAN', 'Wireless LAN', 'Netzwerk', 'Routing-Protokolle', 'Multicast', 'WAN', 'VPN', and 'Firewall'. The 'IP-Konfiguration' section is expanded, and 'Schnittstellen' is selected. The main area is titled 'Schnittstellen' and contains a form with the following fields:

- Basisparameter**
- Adressmodus**: Statisch DHCP
- IP-Adresse / Netzmaske**: IP-Adresse: 192.168.100.1, Netzmaske: 255.255.255.0. A 'Hinzufügen' button is below the input fields.
- Schnittstellenmodus**: Untagged Tagged (VLAN)
- MAC-Adresse**: 00:a0:f9:09:68:b6. A checkbox 'Voreingestellte verwenden' is checked.

At the bottom, there is a section for 'Erweiterte Einstellungen' with 'OK' and 'Abbrechen' buttons.


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**.

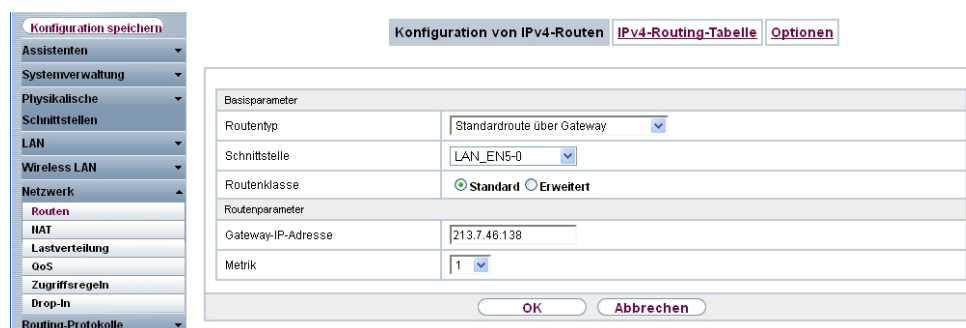


Abb. 9: **Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu**

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**.



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.**

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) Tragen Sie bei **Original Ziel-IP-Adresse/Netzmaske** die statische öffentliche IP-Adresse des Gateways ein, hier *213.7.46.137*.
- (6) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** 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) Tragen Sie bei **Original Ziel-IP-Adresse/Netzmaske** die statische öffentliche IP-Adresse des Gateways ein, hier *213.7.46.137*.
- (7) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** 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) Tragen Sie bei **Original Ziel-IP-Adresse/Netzmaske** die statische öffentliche IP-Adresse des Gateways ein, hier *213.7.46.137*.
- (7) Im Feld **Neue Ziel-IP-Adresse/Netzmaske** 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**.

The screenshot shows the 'NAT-Konfiguration' window with a table of configured rules. The left sidebar shows the navigation menu with 'Netzwerk' selected. The table has columns for description, direction, service/protocol, source IP/mask, destination IP/mask, and target IP/mask. Three rules are listed: FTP, HTTP, and HTTPS.

Beschr.	Richtung.	Dienst/Protokoll	Quell-IP/Maske/Port	Ziel-IP/Maske/Port	Neur. Quell-IP/Maske/Port (Q) Neur. Ziel-IP/Maske/Port (Z)			
ethoa50-0								
FTP	Eingehend	ftp (TCP)	0.0.0.0/ 0.0.0.0:-	213.7.46.137/ 255.255.255.255:21	(Z)192.168.200.201/ 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:> 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 -> Konfigura-	<i>LAN_EN5-0</i>

Feld	Menü	Wert
	tion von IPv4-Routen -> Neu	
Gateway	Netzwerk -> Routen -> Konfiguration von IPv4-Routen -> Neu	213.7.46.138

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>

Feld	Menü	Wert
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-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 (SSL)</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>

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.

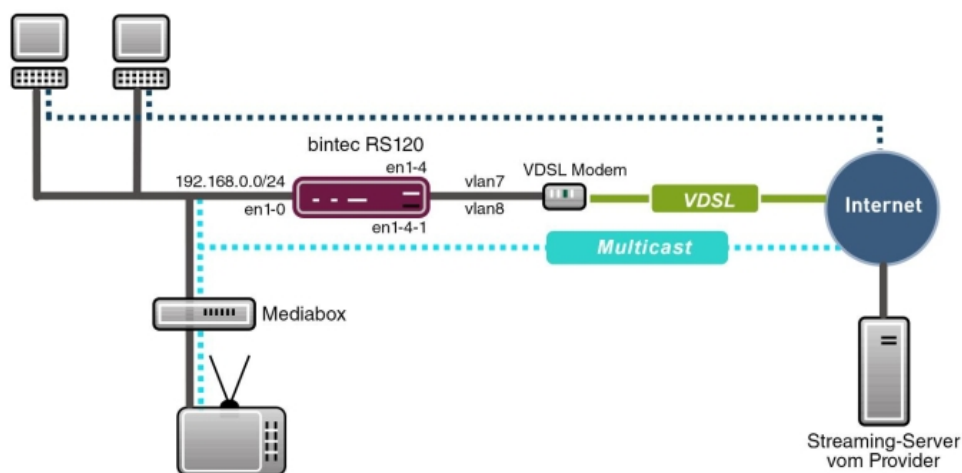


Abb. 13: Beispielszenario

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 RS120** mit Software Version 7.9.4 Patch 5 verwendet.
- Die Konfiguration ist für andere bintec Routertypen identisch. Die folgende Liste zeigt den Mindeststand der hierbei zu verwendenden Softwareversionen:

TR200: 7.9.1 Patch 5

RS12x: 7.9.1 Patch 5

RS23x: 7.9.1 Patch 5

R120x: 7.9.1 Patch 5

R300x: 7.9.1 Patch 5

R400x: 7.9.1 Patch 5

- Die Konfiguration erfolgt über das **GUI** Web-Konfigurations-Tool.

3.2 Konfiguration

3.2.1 Konfiguration des bintec RS120

Zur Konfiguration öffnen Sie einen Internet Browser und starten eine Web (HTTP)-Verbindung zum **bintec RS120** Router. Soweit nicht anders konfiguriert, verwenden Sie hierzu die Standard IP-Adresse *192.168.0.254*. Nach erfolgreichem Aufbau der HTTP-Verbindung loggen Sie sich über folgende Zugangsdaten ein.

User *admin* **Password** *funkwerk* (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** -> **Internetzugang** -> **Internetverbindungen** -> **Neu**.



Abb. 14: Assistenten -> Internetzugang -> 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.

Abb. 15: Assistenten -> Internetzugang -> 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 **Internet Service Provider** wählen Sie für unseren VDSL-Anschluss das Profil *Germany - T-Home - VDSL* aus.
- (4) Bei **Benutzername** geben Sie die Zugangsdaten ein, die Sie von Ihrem Provider erhalten haben.
- (5) Geben Sie das **Paswort** ein, das Sie von Ihrem Provider erhalten haben.
- (6) 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.
- (7) 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	
Basierend auf Ethernet-Schnittstelle	en1-4
Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> DHCP
IP-Adresse / Netzmaske	<input type="text" value="IP-Adresse"/> <input type="text" value="Netzmaske"/> <input type="button" value="Hinzufügen"/>
Schnittstellenmodus	<input type="radio"/> Manuell <input checked="" type="radio"/> VLAN
MAC-Adresse	<input type="text" value="00:a0:f9"/> <input checked="" type="checkbox"/> Voreingestellte verwenden
VLAN-ID	<input type="text" value="8"/>

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

Abb. 16: 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 physikalischen Ethernet-Port zugeordnet ist. Für den Ethernet-Port ETH5 ist das die Schnittstelle *en1-4* (siehe dazu die Erläuterung im Anschluss).
- (2) Stellen Sie den **Adressmodus** auf *DHCP*. Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
- (3) Den **Schnittstellenmodus** stellen Sie auf *VLAN*. Mit dieser Option weisen Sie die Schnittstelle einem VLAN zu.
- (4) Im Eingabefeld **VLAN-ID** geben Sie die zu verwendende VLAN-ID *8* ein.
- (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

ETH1 bis ETH4

ETH5

Logische Ethernet-Schnittstelle

en1-0

en1-4

Genauere Informationen über die bei Ihnen konfigurierte Zuordnung finden Sie im Menü **Physikalische Schnittstellen**. Für den im Workshop verwendeten **bintec RS120** Router sieht dies im Auslieferungszustand wie folgt aus:

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

Portkonfiguration

Automatisches Aktualisierungsintervall Sekunden

Switch-Port	Ethernet-Schnittstellenauswahl	Konfigurierte Geschwindigkeit/konfigurierter Modus	Aktuelle Geschwindigkeit / Aktueller Modus
1	en1-0	Vollständige automatische Aushandlung	100 Mbit/s / Full Duplex
2	en1-0	Vollständige automatische Aushandlung	1000 Mbit/s / Full Duplex
3	en1-0	Vollständige automatische Aushandlung	100 Mbit/s / Full Duplex
4	en1-0	Vollständige automatische Aushandlung	Inaktiv
5	en1-4	Vollständige automatische Aushandlung	100 Mbit/s / Full Duplex

Abb. 17: **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 **Routing -> Multicast -> IGMP -> Neu**.

Abb. 18: Routing -> Multicast -> IGMP -> 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 `LEASED_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. 19: Routing -> Multicast -> 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 **Routing -> Multicast -> Optionen**.

Grundeeinstellungen	
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	64
Maximale Quellen	64
Maximale Anzahl der IGMP-Statusmeldungen	0 Meldungen pro Sekunde

Abb. 20: **Routing -> Multicast -> 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 **Routing -> NAT -> NAT-Schnittstellen**.

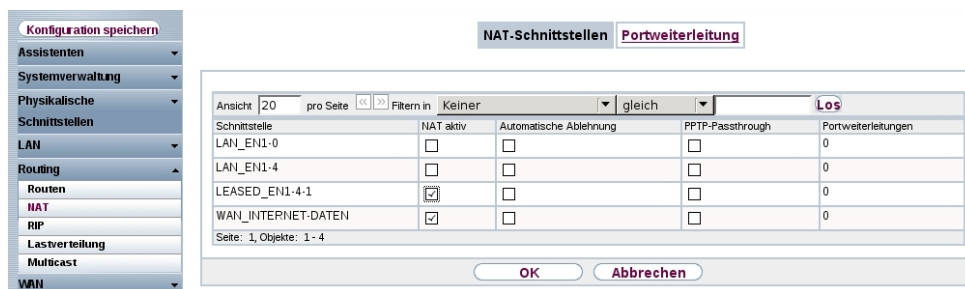


Abb. 21: Routing -> NAT -> NAT-Schnittstellen

Gehen Sie folgendermaßen vor:

- (1) Aktivieren Sie unter **NAT aktiv** die Schnittstelle `LEASED_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 **bintec RS120** Routers als **Router** auf dem DHCP-Server ein. In unserem Beispiel ist die LAN IP-Adresse des **bintec RS120** `192.168.0.254`.

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

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

Abb. 22: Lokale Dienste -> DHCP-Server -> DHCP Pool -> Neu

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

- (1) Bei **Schnittstelle** wählen Sie die logische Schnittstelle `en1-0` 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-Netzgebietes liegen.

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
Schnittstelle	Assistenten -> Internetzugang -> Internetverbindungen	<i>Externes xDSL-Modem</i>

Internetverbindung einrichten

Feld	Menü	Wert
Beschreibung	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>Internet-Daten</i>
Physischer Ethernet-Port	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>ETH5</i>
Internet Service Provider	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>Germany-T-Home-VDSL</i>
Benutzername	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>123456789#0001@t-online.de</i>
Paswort	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>geheim</i>
Immer aktiv	Assistenten -> Internetzugang -> 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>
Adressmodus	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>DHCP</i>
Schnittstellenmodus	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>VLAN</i>
VLAN-ID	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>8</i>
DHCP Broadcast Flag	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>Deaktiviert</i>

IGMP-Proxy konfigurieren

Feld	Menü	Wert
Schnittstelle	Routing -> Multicast -> IGMP -> Neu	<i>LAN_EN1-0</i>
Modus	Routing -> Multicast -> IGMP -> Neu	<i>Routing</i>
IGMP Proxy	Routing -> Multicast -> IGMP -> Neu	<i>Aktiviert</i>
Proxy-Schnittstelle	Routing -> Multicast -> IGMP -> Neu	<i>LEASED_EN1-4-1</i>

Multicast Routing Funktion aktivieren

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

NAT aktivieren

Feld	Menü	Wert
Schnittstelle LEA-SED_EN1-4-1	Routing -> NAT -> NAT-Schnittstellen	NAT aktiv <i>Aktiviert</i>

DHCP IP-Adress-Pool konfigurieren

Feld	Menü	Wert
Schnittstelle	Lokale Dienste -> DHCP-Server -> DHCP Pool -> Neu	<i>en1-0</i>
IP-Adressbereich	Lokale Dienste -> DHCP-Server -> DHCP Pool -> Neu	<i>z. B. 192.168.0.100 - 192.168.0.150</i>
Pool-Verwendung	Lokale Dienste -> DHCP-Server -> DHCP Pool -> Neu	<i>Lokal</i>

Kapitel 4 IP - Routing-Protokoll OSPF über IP-Sec-Verbindung

4.1 Einleitung

Die vorliegende Lösung zeigt die sternförmige Vernetzung dreier Standorte über IPsec-Verbindungen, bei dem das Routingprotokoll OSPF zur Übermittlung der in den Filial-Standorten konfigurierten IP-Netzbereichen 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.

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

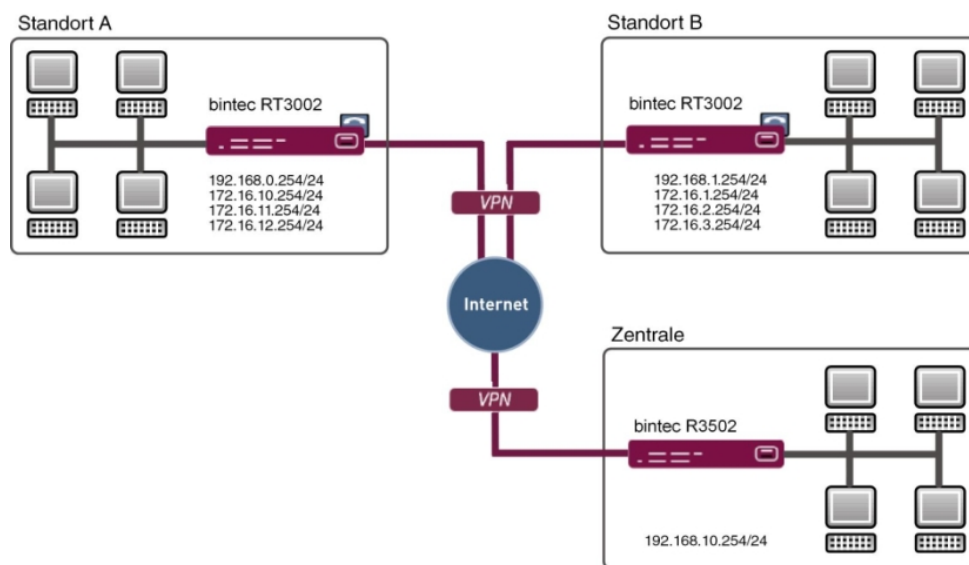


Abb. 23: Beispielszenario

In unserem Beispiel werden an den Standorten A und B mehrere Netzwerke verwendet. Bei statisch konfiguriertem Routing hätte dies zur Folge, dass alle Netzwerke von allen Standorten in sämtlichen VPN-Gateways konfiguriert werden müßten. Bei der Nutzung eines Routing-Protokolls entfällt dies. Konfiguriert werden muss in diesem Fall nur ein VPN-Tunnel der die Kommunikation zum Gateway der Zentrale ermöglicht.

Konkret muss der Administrator bei der VPN-Konfiguration nur das jeweils erste Netzwerk

der LAN-Schnittstelle des jeweiligen VPN-Gateways beachten. Alles weitere wird vom Routing-Protokoll übernommen. Das Routing Protokoll propagiert in diesem Beispiel sämtliche Netzwerke der Standorte A und B zum Gateway der Zentrale. Wodurch alle Standorte miteinander kommunizieren können. Beim Ändern einer LAN IP-Adresse bzw. beim Hinzufügen eines neuen Netzwerks an einem der Gateways werden die Routing Informationen automatisch an die anderen Gateways weiter gegeben. Die VPN-Gateways unterstützen die Verwendung von Routing-Protokollen auch in Verbindung mit IPsec-Verbindungen.

Voraussetzungen

- Je ein bintec VPN-Gateway der Rxxx2- oder RTxxx2-Serie an allen Standorten
- Alle Gateways benötigen eine unabhängige Verbindung zum Internet
- Mindestens eine statische IP-Adresse oder ein DynDNS-Account für die Erreichbarkeit des Gateways der Zentrale

4.2 Konfiguration

4.2.1 Konfiguration des Gateways in der Zentrale

Konfiguration des Internetzugangs am Gateway der Zentrale

Der Internetzugang am Gateway in der Zentrale kann mit Hilfe des **Assistenten** konfiguriert werden. In diesem Workshop wird am Standort der Zentrale ein Internetzugang mit einer statischer IP-Adresse verwendet.

- (1) Gehen Sie zu **Assistenten** -> **Internetzugang** -> **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.

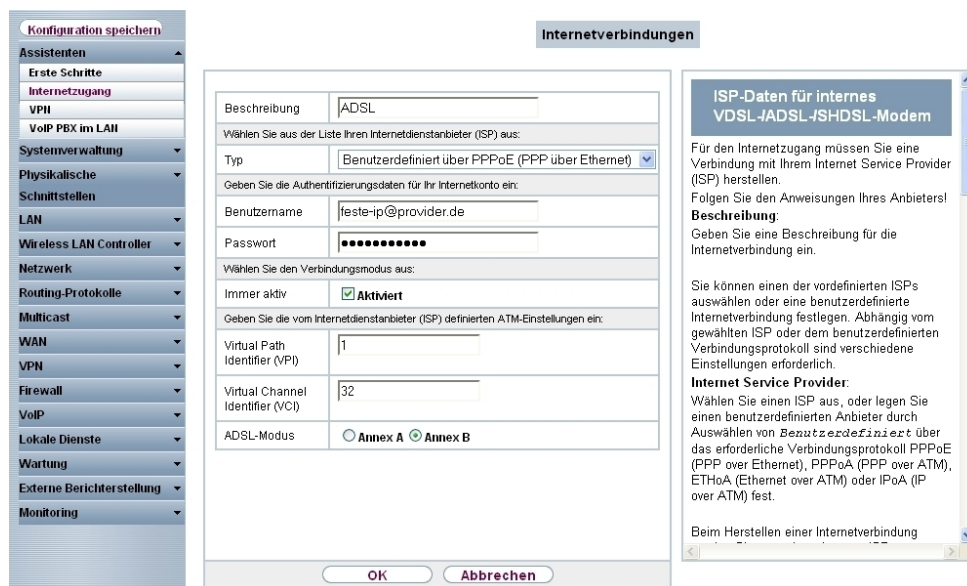


Abb. 24: Assistenten -> Internetzugang -> Internetverbindungen -> Weiter

Gehen Sie folgendermaßen vor, um einen Internetzugang zu konfigurieren:

- (1) Bei **Beschreibung** tragen Sie z. B. *ADSL* ein.
- (2) Bei **Typ** wählen Sie *Benutzerdefiniert über PPPoE (PPP über Ethernet)* aus.
- (3) Als **Benutzer** geben Sie den Namen ein, welches Sie von Ihrem Provider erhalten haben z. B. *feste-ip@provider.de*.
- (4) Geben Sie das **Passwort** ein, welches Sie von Ihrem Provider erhalten haben, z. B. *test12345*.
- (5) Aktivieren Sie die Option **Immer aktiv**.
- (6) Bei **ADSL-Modus** wählen Sie *Annex B* aus für Anwendungsgebiete in Europa (Provider-abhängig).
- (7) Bestätigen Sie Ihre Angaben mit **OK**.

Konfiguration der VPN IPsec-Verbindungen am Gateway der Zentrale

In unserem Beispiel werden die VPN-Tunnel immer von den Filial-Gateways zum Zentral-Gateway hin aufgebaut. Aus diesem Grund ist es nicht notwendig die IPsec-Peer-Adresse am Zentral-Gateway zu konfigurieren. In diesem Workshop werden die VPN-IPsec-Tunnel zum Standort-A und zum Standort-B mit Hilfe des **Assistenten** konfiguriert.

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

Abb. 25: Assistenten -> VPN -> VPN-Verbindungen -> Weiter

Gehen Sie folgendermaßen vor, um die VPN-Verbindung zum Standort A hinzuzufügen:

- (1) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Standort-A*.
- (2) Bei **Lokale IPsec ID** geben Sie die IPsec-ID des Gateways der Zentrale ein z. B. *zentrale@bintec-elmeg.com*.
- (3) Bei **Entfernte IPsec ID** geben Sie die IPsec-ID des Gateways am Standort A ein z. B. *rt3002-0@bintec-elmeg.com*.



Hinweis

Diese ID muss eindeutig sein.

- (4) Im Feld **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung ein, z. B. *test12345*.
- (5) Die **Lokale IP-Adresse** legt die IP-Adresse der IPsec-Schnittstelle fest z. B. *192.168.10.254*.
- (6) Bei **IPsec-Peer-Adresse** muss nichts hinterlegt werden, da der VPN-Tunnel immer von dem Filial-Gateway zum Zentral-Gateway aufgebaut wird.
Bei **IP-Adresse des Remote-Netzwerks** muss die Netzwerkadresse von einem der

am Standort A verwendeten IP-Netzwerke konfiguriert werden z. B. `192.168.0.0` und die **Netzmaske** `255.255.255.0`.

(7) Bestätigen Sie mit **OK**.

Fügen Sie nun die VPN-Verbindung zum Standort B hinzu.

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

Konfiguration speichern

- Assistenten
 - Erste Schritte
 - Internetzugang
 - VPI
 - VoIP PBX im LAN
- Systemverwaltung
 - Physikalische Schnittstellen
 - LAN
 - Wireless LAN Controller
 - Netzwerk
 - Routing-Protokolle
 - Multicast
 - WAN
 - VPN
 - Firewall
 - VoIP
 - Lokale Dienste
 - Wartung
 - Externe Berichterstellung
 - Monitoring

VPN-Verbindungen

Ausgewähltes Szenario: LAN-zu-LAN-Verbindung

IPsec-Szenario: LAN-zu-LAN-Verbindung

Verbindungsdetails

Beschreibung: Standort-B

Lokale IPsec ID: zentrale@bintec-elmeg.com

Entfernte IPsec ID: rt3002_1@bintec-elmeg.com

Preshared Key:

Lokale IP-Adresse: 192.168.10.254

Diese Verbindung als Standardroute definieren: Aktiviert

IP-Einstellungen eingeben:

IPsec-Peer-Adresse:

IP-Adresse des Remote-Netzwerks: 192.168.1.0

Netzmaske: 255.255.255.0

OK Abbrechen

Da Sie verschiedene VPN-Verbindungen konfigurieren können, müssen Sie eine Beschreibung festlegen, um die VPN-Verbindung eindeutig zu identifizieren.

Beschreibung:
Geben Sie einen Namen für die Verbindung ein.

Die IPsec-Partner müssen sich gegenseitig identifizieren und authentifizieren, um eine IPsec-Verbindung herzustellen.

Die Identität des IPsec-Partners wird durch eine eindeutige ID belegt (vergleichbar mit dem Benutzernamen). Zum Herstellen einer IPsec-Verbindung muss jedes IPsec-Gateway in der Lage sein, die ID des anderen Gateways zu identifizieren. Deshalb müssen beide IDs auf beiden IPsec-Gateways konfiguriert sein. Bei der ID kann es sich um einen beliebigen Namen handeln. In der Regel handelt es sich um einen Namen, der den Verbindungsort klar bezeichnet.

Lokale IPsec ID:
Geben Sie die ID Ihres eigenen IPsec-Gateways ein.

Entfernte IPsec ID:
Geben Sie die ID des entfernten IPsec-Gateways ein.

Preshared Key:

Abb. 26: **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Weiter**

Gehen Sie folgendermaßen vor, um die VPN-Verbindung zum Standort B hinzuzufügen:

- (1) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Standort-B*.
- (2) Bei **Lokale IPsec ID** geben Sie die IPsec-ID des Gateways der Zentrale ein z. B. *zentrale@bintec-elmeg.com*.
- (3) Bei **Entfernte IPsec ID** geben Sie die IPsec-ID des Gateways am Standort B ein z. B. *rt3002-1@bintec-elmeg.com*.



Hinweis

Diese ID muss eindeutig sein.

- (4) Im Feld **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung ein, z. B. *test12345*.
- (5) Die **Lokale IP-Adresse** legt die IP-Adresse der IPsec-Schnittstelle fest z. B. *192.168.10.254*.
- (6) Bei **IPsec-Peer-Adresse** muss nichts hinterlegt werden, da der VPN-Tunnel immer von dem Filial-Gateway zum Zentral-Gateway aufgebaut wird.
Bei **IP-Adresse des Remote-Netzwerks** muss die Netzwerkadresse von einem der am Standort B verwendeten IP-Netzwerke konfiguriert werden z. B. *192.168.1.0* und die **Netzmaske** *255.255.255.0*.
- (7) Bestätigen Sie mit **OK**.

Im nächsten Schritt wird das Routing-Protokoll OSPF aktiviert. Damit werden die Routing-Einträge über die VPN-IPsec-Tunnel an die Standorte propagiert.

- (1) Gehen Sie zu **Routing Protokolle -> OSPF -> Globale Einstellungen**.

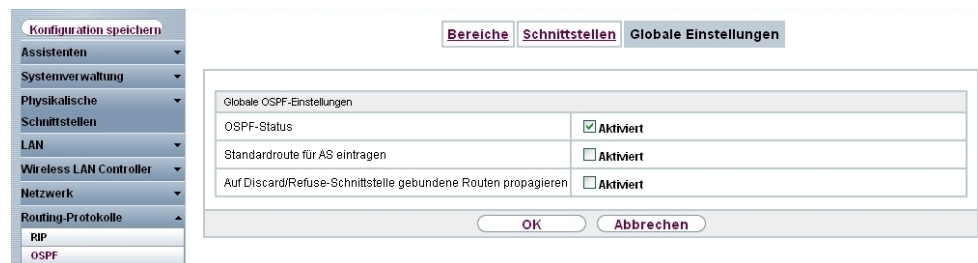


Abb. 27: Routing Protokolle -> OSPF -> Globale Einstellungen

Gehen Sie folgendermaßen vor:

- (1) Aktivieren Sie die Option **OSPF-Status**.
- (2) Bestätigen Sie mit **OK**.

Im Menü **Schnittstellen** wird bestimmt auf welcher Schnittstelle IP-Routing-Informationen propagiert werden.

- (1) Gehen Sie zu **Routing Protokolle -> OSPF -> Schnittstellen -> <Standort-A/Standort-B>** .

Konfiguration speichern

Assistenten
Systemverwaltung
Physikalische
Schnittstellen
LAN
Wireless LAN Controller
Netzwerk
Routing-Protokolle
RIP
OSPF
Multicast
WAN
VPN
Firewall

Bereiche Schnittstellen Globale Einstellungen

OSPF-Schnittstellenkonfiguration

Admin-Status: Aktiv

Bereichs-ID: 0.0.0.0

Metrikbestimmung: Auto (Schnittstellengeschwindigkeit)

Metrik (Direkte Routen): 10

Authentifizierungstyp: Keiner

Indirekte, statische Routen exportieren: Aktiviert

Demand Circuit Options: Aktiviert

OK Abbrechen

Abb. 28: Routing Protokolle -> OSPF -> Schnittstellen -> <Standort-A/Standort-B>

Gehen Sie folgendermaßen vor:

- (1) Setzen Sie den OSPF **Admin-Status** für die VPN-IPsec-Schnittstellen auf *Aktiv* um auf diesen Schnittstellen Routing-Information zu propagieren. Für alle weiteren Schnittstellen wird der Standardwert *Passiv* verwendet um deren Routing-Informationen auf den beiden VPN-IPsec-Schnittstellen bekannt zu geben.
- (2) Bestätigen Sie mit **OK**.

Die fertige Konfiguration sieht nun wie folgt aus:

Konfiguration speichern

Assistenten
Systemverwaltung
Physikalische
Schnittstellen
LAN
Wireless LAN Controller
Netzwerk
Routing-Protokolle
RIP
OSPF

Bereiche Schnittstellen Globale Einstellungen

Ansicht: 20 pro Seite Filtern in: Keiner gleich Los

Schnittstelle	Bereichs-ID	IP-Adresse	Admin-Status	Status	Metrik	
en1-0	0.0.0.0	192.168.10.254	Passiv	Inaktiv	1	
en1-4	0.0.0.0	0.0.0.0	Passiv	Inaktiv	10	
Standort-B	0.0.0.0	192.168.10.254	Aktiv	Punkt-zu-Punkt	10	
Standort-A	0.0.0.0	192.168.10.254	Aktiv	Punkt-zu-Punkt	10	

Seite: 1, Objekte: 1 - 4

Abb. 29: Routing Protokolle -> OSPF -> Schnittstellen

4.2.2 Konfiguration des Gateways am Standort A

Konfiguration des Internetzugangs am Gateway von Standort A

Der Internetzugang am Gateway des Standorts A kann mit Hilfe des **Assistenten** konfiguriert werden.

- (1) Gehen Sie zu **Assistenten -> Internetzugang -> 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.

Konfiguration speichern

Assistenten

- Erste Schritte
- Internetzugang
- VPN
- VoIP PBX im LAN

Systemverwaltung

- Physikalische Schnittstellen
- LAN
- Wireless LAN Controller
- Netzwerk
- Routing-Protokolle
- Multicast
- WAN
- VPN
- Firewall
- VoIP
- Lokale Dienste
- Wartung
- Externe Berichterstellung
- Monitoring

Internetverbindungen

Beschreibung: ADSL

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

Typ: Benutzerdefiniert über PPPoE (PPP über Ethernet)

Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:

Benutzername: feste-ip@provider.de

Passwort: ●●●●●●●●

Wählen Sie den Verbindungsmodus aus:

Immer aktiv: Aktiviert

Geben Sie die vom Internetdienstanbieter (ISP) definierten ATM-Einstellungen ein:

Virtual Path Identifier (VPI): 1

Virtual Channel Identifier (VCI): 32

ADSL-Modus: Annex A Annex B

ISP-Daten für internes VDSL-/ADSL-/SHDSL-Modem

Für den Internetzugang müssen Sie eine Verbindung mit Ihrem Internet Service Provider (ISP) herstellen. Folgen Sie den Anweisungen Ihres Anbieters!

Beschreibung: Geben Sie eine Beschreibung für die Internetverbindung ein.

Sie können einen der vordefinierten ISPs auswählen oder eine benutzerdefinierte Internetverbindung festlegen. Abhängig vom gewählten ISP oder dem benutzerdefinierten Verbindungsprotokoll sind verschiedene Einstellungen erforderlich.

Internet Service Provider: Wählen Sie einen ISP aus, oder legen Sie einen benutzerdefinierten Anbieter durch Auswählen von *Benutzerdefiniert* über das erforderliche Verbindungsprotokoll PPPoE (PPP über Ethernet), PPPoA (PPP über ATM), ETHoA (Ethernet über ATM) oder IPoA (IP über ATM) fest.

Beim Herstellen einer Internetverbindung

OK Abbrechen

Abb. 30: Assistenten -> Internetzugang -> Internetverbindungen -> Weiter

Gehen Sie folgendermaßen vor, um einen Internetzugang zu konfigurieren:

- (1) Bei **Beschreibung** tragen Sie z. B. *ADSL* ein.
- (2) Bei **Typ** wählen Sie *Benutzerdefiniert über PPPoE (PPP über Ethernet)* aus.
- (3) Als **Benutzer** geben Sie den Namen ein, welches Sie von Ihrem Provider erhalten haben z. B. *feste-ip@provider.de*.
- (4) Geben Sie das **Passwort** ein, welches Sie von Ihrem Provider erhalten haben, z. B. *test12345*.
- (5) Aktivieren Sie die Option **Immer aktiv**.
- (6) Bei **ADSL-Modus** wählen Sie *Annex B* aus für Anwendungsgebiete in Europa (Provider-abhängig).
- (7) Bestätigen Sie Ihre Angaben mit **OK**.

Konfiguration der VPN-IPSec-Verbindung am Gateway von Standort A

In unserem Beispiel werden die VPN-Tunnel immer vom Filial-Gateway zum Zentral-Gateway aufgebaut. Die VPN-IPSec-Konfiguration wird mit Hilfe des Assistenten konfiguriert.

- (1) Gehen Sie zu **Assistenten -> VPN -> VPN-Verbindungen -> Neu**.
- (2) Wählen Sie bei **IPSec-Szenario** *IPSec-LAN-zu-LAN-Verbindung* aus.

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

Abb. 31: Assistenten -> VPN -> VPN-Verbindungen -> Weiter

Gehen Sie folgendermaßen vor, um die VPN-Verbindung zum Zentral-Gateway hinzuzufügen:

- (1) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Zentrale*.
- (2) Bei **Lokale IPsec ID** geben Sie die IPsec-ID des Gateways von Standort A ein z. B. *rt3002_0@bintec-elmeg.com*.
- (3) Bei **Entfernte IPsec ID** geben Sie die IPsec-ID des Gateways der Zentrale ein z. B. *zentrale@bintec-elmeg.com*.



Hinweis

Diese ID muss eindeutig sein.

- (4) Im Feld **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung ein, z. B. *test12345*.
- (5) Die **Lokale IP-Adresse** legt die IP-Adresse der IPsec-Schnittstelle fest z. B. *192.168.0.254*.
- (6) Bei **IPsec-Peer-Adresse** muss die IP-Adresse oder der DNS-Name hinterlegt werden mit der das Gateway der Zentrale per Internet erreichbar ist. In unserem Beispiel wird

die Statische WAN IP-Adresse des Gateways der Zentrale verwendet, z. B. 62.63.64.65.

- (7) Bei **IP-Adresse des Remote-Netzwerks** muss die Netzwerkadresse von einem in der Zentrale verwendeten IP-Netzwerke konfiguriert werden z. B. 192.168.10.0 und die **Netzmaske** 255.255.255.0.
- (8) Bestätigen Sie mit **OK**.

Im nächsten Schritt wird das Routing-Protokoll OSPF aktiviert. Damit werden die Routing-Einträge über die VPN-IPsec-Tunnel an die Standorte propagiert.

- (1) Gehen Sie zu **Routing Protokolle -> OSPF -> Globale Einstellungen**.

Abb. 32: Routing Protokolle -> OSPF -> Globale Einstellungen

Gehen Sie folgendermaßen vor:

- (1) Aktivieren Sie die Option **OSPF-Status**.
- (2) Bestätigen Sie mit **OK**.

Im Menü **Schnittstellen** wird bestimmt auf welcher Schnittstelle IP-Routing-Informationen propagiert werden.


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

Abb. 33: Routing Protokolle -> OSPF -> Schnittstellen -> <Zentrale> 

Gehen Sie folgendermaßen vor:

- (1) Setzen Sie den OSPF **Admin-Status** für die beiden neu konfigurierten VPN-IP-Sec-Schnittstellen auf *Aktiv* um auf diesen Schnittstellen Routing-Information zu propagieren. Für alle weiteren Schnittstellen wird der Standardwert *Passiv* verwendet um deren Routing-Informationen auf den beiden VPN-IPsec-Schnittstellen bekannt zu geben.
- (2) Bestätigen Sie mit **OK**.

Die fertige Konfiguration sieht nun wie folgt aus:

The screenshot shows a web-based configuration interface for OSPF. On the left is a navigation menu with categories like 'Assistenten', 'Systemverwaltung', 'Schnittstellen', 'LAN', 'Wireless LAN Controller', 'Netzwerk', 'Routing-Protokolle', 'RIP', 'OSPF', and 'Multicast'. The 'OSPF' option is selected. At the top, there are tabs for 'Bereiche', 'Schnittstellen', and 'Globale Einstellungen'. Below the tabs is a table with columns: Schnittstelle, Bereichs-ID, IP-Adresse, Admin-Status, Status, and Metrik. The table contains five rows of data, including interfaces en1-0, en1-4, ADSL, ethoa50-0, and Zentrale. The 'Zentrale' interface is highlighted in blue, indicating it is selected. The 'Admin-Status' for 'Zentrale' is 'Aktiv', while others are 'Passiv'. The 'Status' for 'Zentrale' is 'Punkt-zu-Punkt', while others are 'Inaktiv'.

Schnittstelle	Bereichs-ID	IP-Adresse	Admin-Status	Status	Metrik
en1-0	0.0.0.0	192.168.0.254	Passiv	Inaktiv	1
en1-4	0.0.0.0	0.0.0.0	Passiv	Inaktiv	10
ADSL	0.0.0.0	0.0.0.0	Passiv	Inaktiv	1562
ethoa50-0	0.0.0.0	0.0.0.0	Passiv	Inaktiv	65535
Zentrale	0.0.0.0	192.168.0.254	Aktiv	Punkt-zu-Punkt	10

Abb. 34: Routing Protokolle -> OSPF -> Schnittstellen

4.2.3 Konfiguration des Gateways am Standort B

Konfiguration des Internetzugangs am Gateway von Standort B

Der Internetzugang am Gateway des Standorts B kann mit Hilfe des **Assistenten** konfiguriert werden.

- (1) Gehen Sie zu **Assistenten** -> **Internetzugang** -> **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.

Konfiguration speichern

Assistenten

- Erste Schritte
- Internetzugang
- VPN
- VoIP PBX im LAN

Systemverwaltung

- Systemverwaltung
- Physikalische Schnittstellen
- LAN
- Wireless LAN Controller
- Netzwerk
- Routing-Protokolle
- Multicast
- WAN
- VPN
- Firewall
- VoIP
- Lokale Dienste
- Wartung
- Externe Berichterstellung
- Monitoring

Internetverbindungen

Beschreibung: ADSL

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

Typ: Benutzerdefiniert über PPPoE (PPP über Ethernet)

Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:

Benutzername: feste-ip@provider.de

Passwort:

Wählen Sie den Verbindungsmodus aus:

Immer aktiv: Aktiviert

Geben Sie die vom Internetdienstanbieter (ISP) definierten ATM-Einstellungen ein:

Virtual Path Identifier (VPI): 1

Virtual Channel Identifier (VCI): 32

ADSL-Modus: Annex A Annex B

OK Abbrechen

ISP-Daten für internes VDSL-/ADSL-/SHDSL-Modem

Für den Internetzugang müssen Sie eine Verbindung mit Ihrem Internet Service Provider (ISP) herstellen. Folgen Sie den Anweisungen Ihres Anbieters!

Beschreibung:
Geben Sie eine Beschreibung für die Internetverbindung ein.

Sie können einen der vordefinierten ISPs auswählen oder eine benutzerdefinierte Internetverbindung festlegen. Abhängig vom gewählten ISP oder dem benutzerdefinierten Verbindungsprotokoll sind verschiedene Einstellungen erforderlich.

Internet Service Provider:
Wählen Sie einen ISP aus, oder legen Sie einen benutzerdefinierten Anbieter durch Auswählen von *Benutzerdefiniert* über das erforderliche Verbindungsprotokoll PPPoE (PPP über Ethernet), PPPoA (PPP über ATM), ETHoA (Ethernet over ATM) oder IPoA (IP over ATM) fest.

Beim Herstellen einer Internetverbindung

Abb. 35: Assistenten -> Internetzugang -> Internetverbindungen -> Weiter

Gehen Sie folgendermaßen vor, um einen Internetzugang zu konfigurieren:

- (1) Bei **Beschreibung** tragen Sie z. B. *ADSL* ein.
- (2) Bei **Typ** wählen Sie *Benutzerdefiniert über PPPoE (PPP über Ethernet)* aus.
- (3) Als **Benutzer** geben Sie den Namen ein, welches Sie von Ihrem Provider erhalten haben z. B. *feste-ip@provider.de*.
- (4) Geben Sie das **Passwort** ein, welches Sie von Ihrem Provider erhalten haben, z. B. *test12345*.
- (5) Aktivieren Sie die Option **Immer aktiv**.
- (6) Bei **ADSL-Modus** wählen Sie *Annex B* aus für Anwendungsgebiete in Europa (Provider-abhängig).
- (7) Bestätigen Sie Ihre Angaben mit **OK**.

Konfiguration der VPN-IPsec-Verbindung am Gateway von Standort B

In unserem Beispiel werden die VPN-Tunnel immer vom Filial-Gateway zum Zentral-Gateway aufgebaut. Die VPN-IPsec-Konfiguration wird mit Hilfe des Assistenten konfiguriert.

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

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

Konfiguration speichern

VPN-Verbindungen

Ausgewähltes Szenario
IPsec-Szenario: LAN-zu-LAN-Verbindung

Verbindungsdetails

Beschreibung	Zentrale
Lokale IPsec ID	rt3002_1@bintec-elmeg.com
Entfernte IPsec ID	zentrale@bintec-elmeg.com
Preshared Key	••••••••
Lokale IP-Adresse	192.168.1.254
Diese Verbindung als Standardroute definieren	<input type="checkbox"/> Aktiviert
IP-Einstellungen eingeben:	
IPsec-Peer-Adresse	62.63.64.65
IP-Adresse des Remote-Netzwerks	192.168.10.0
Netzmaske	255.255.255.0

OK Abbrechen

IPsec LAN-zu-LAN-Verbindung

Geben Sie die erforderlichen Daten für das IPsec-Szenario der "LAN-zu-LAN-Verbindung" ein.

IPsec-Szenario:
Dient als Erinnerung an das ausgewählte Szenario.

Da Sie verschiedene VPN-Verbindungen konfigurieren können, müssen Sie eine Beschreibung festlegen, um die VPN-Verbindung eindeutig zu identifizieren.

Beschreibung:
Geben Sie einen Namen für die Verbindung ein.

Die IPsec-Partner müssen sich gegenseitig identifizieren und authentifizieren, um eine IPsec-Verbindung herzustellen.

Die Identität des IPsec-Partners wird durch eine eindeutige ID belegt (vergleichbar mit dem Benutzernamen). Zum Herstellen einer IPsec-Verbindung muss jedes IPsec-Gateway in der Lage sein, die ID des anderen Gateways zu identifizieren. Deshalb müssen

Abb. 36: Assistenten -> VPN -> VPN-Verbindungen -> Weiter

Gehen Sie folgendermaßen vor, um die VPN-Verbindung zum Zentral-Gateway hinzuzufügen:

- (1) Bei **Beschreibung** geben Sie eine Beschreibung des Peers, die diesen identifiziert ein, z. B. *Zentrale*.
- (2) Bei **Lokale IPsec ID** geben Sie die IPsec-ID des Gateways von Standort B ein z. B. *rt3002_1@bintec-elmeg.com*.
- (3) Bei **Entfernte IPsec ID** geben Sie die IPsec-ID des Gateways der Zentrale ein z. B. *zentrale@bintec-elmeg.com*.



Hinweis

Diese ID muss eindeutig sein.

- (4) Im Feld **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung ein, z. B. *test12345*.
- (5) Die **Lokale IP-Adresse** legt die IP-Adresse der IPsec-Schnittstelle fest z. B. *192.168.1.254*.
- (6) Bei **IPsec-Peer-Adresse** muss die IP-Adresse oder der DNS-Name hinterlegt werden mit der das Gateway der Zentrale per Internet erreichbar ist. In unserem Beispiel wird die Statische WAN IP-Adresse des Gateways der Zentrale verwendet, z. B.

62.63.64.65.

- (7) Bei **IP-Adresse des Remote-Netzwerks** muss die Netzwerkadresse von einem in der Zentrale verwendeten IP-Netzwerke konfiguriert werden z. B. *192.168.10.0* und die **Netzmaske** *255.255.255.0*.
- (8) Bestätigen Sie mit **OK**.

Im nächsten Schritt wird das Routing-Protokoll OSPF aktiviert. Damit werden die Routing-Einträge über die VPN-IPsec-Tunnel an die Standorte propagiert.

- (1) Gehen Sie zu **Routing Protokolle -> OSPF -> Globale Einstellungen**.

Abb. 37: Routing Protokolle -> OSPF -> Globale Einstellungen

Gehen Sie folgendermaßen vor:

- (1) Aktivieren Sie die Option **OSPF-Status**.
- (2) Bestätigen Sie mit **OK**.

Im Menü **Schnittstellen** wird bestimmt auf welcher Schnittstelle IP-Routing-Informationen propagiert werden.


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

Abb. 38: Routing Protokolle -> OSPF -> Schnittstellen -> <Zentrale> 

Gehen Sie folgendermaßen vor:

- (1) Setzen Sie den OSPF **Admin-Status** für die VPN-IPsec-Schnittstellen auf *Aktiv* um auf diesen Schnittstellen Routing-Information zu propagieren. Für alle weiteren Schnittstellen wird der Standardwert *Passiv* verwendet um deren Routing-Informationen auf den beiden VPN-IPsec-Schnittstellen bekannt zu geben.
- (2) Bestätigen Sie mit **OK**.

Die fertige Konfiguration sieht nun wie folgt aus:

Schnittstelle	Bereichs-ID	IP-Adresse	Admin-Status	Status	Metrik
en1-0	0.0.0.0	192.168.1.254	Passiv	Inaktiv	1
en1-4	0.0.0.0	0.0.0.0	Passiv	Inaktiv	10
ADSL	0.0.0.0	0.0.0.0	Passiv	Inaktiv	1562
ethoa50-0	0.0.0.0	0.0.0.0	Passiv	Inaktiv	65535
Zentrale	0.0.0.0	192.168.1.254	Aktiv	Punkt-zu-Punkt	10

Abb. 39: Routing Protokolle -> OSPF -> Schnittstellen

4.3 OSPF-Monitoring

Mit der VPN IPsec-Konfiguration wurde das Netzwerk der Zentrale (192.168.10.0/24) mit den beiden Standorten A und B (192.168.0.0/24 und 192.168.1.0/24) verbunden. Wie im Beispielszenario gezeigt werden auf den beiden Standorten der Filiale noch weitere IP-Netzwerke (z. B. 172.16.1.0/24 bzw. 172.16.10.0/24 und weitere) verwendet. Um die Kommunikation zwischen Standort A und Standort B zu ermöglichen und um alle weiteren Netzwerke von allen Standorten erreichbar zu machen tauschen die Gateways sämtliche Routing-Informationen mit Hilfe des Routing-Protokolls OSPF aus. Diese Routing-Informationen werden mit Hilfe des VPN IPsec-Tunnels verschlüsselt übertragen und periodisch aktualisiert.

In der Spalte **Protokoll** sehen Sie ob der Routing-Eintrag manuell konfiguriert wurde oder ob ein Routing-Eintrag mit Hilfe des Routing-Protocolls OSPF erstellt wurde.

- (1) Gehen Sie zu **Netzwerk -> Routen -> IP-Routen**.

Save configuration

IP Routes [Options](#)

View 20 per page Filter in None equal Go

Destination IP Address	Netmask	Gateway	Interface	Metric	Extended Route	Type	Protocol
10.1.1.254	255.255.255.255	10.1.1.4	WAN_ADSL	0	<input type="checkbox"/>	Direct	Other
10.1.1.254	255.255.255.255	192.168.1.254	IPSEC_IPSEC_1	96	<input type="checkbox"/>	Indirect	OSPF
172.16.1.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	11	<input type="checkbox"/>	Indirect	OSPF
172.16.2.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	11	<input type="checkbox"/>	Indirect	OSPF
172.16.3.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	11	<input type="checkbox"/>	Indirect	OSPF
172.16.10.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	11	<input type="checkbox"/>	Indirect	OSPF
172.16.11.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	11	<input type="checkbox"/>	Indirect	OSPF
172.16.12.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	11	<input type="checkbox"/>	Indirect	OSPF
192.168.0.0	255.255.255.0	192.168.10.254	IPSEC_IPSEC_0	1	<input type="checkbox"/>	Direct	Local
192.168.0.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	11	<input type="checkbox"/>	Indirect	OSPF
192.168.1.0	255.255.255.0	192.168.10.254	IPSEC_IPSEC_1	1	<input type="checkbox"/>	Direct	Local
192.168.1.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	11	<input type="checkbox"/>	Indirect	OSPF
192.168.10.0	255.255.255.0	192.168.10.254	LAN_EN1-0	0	<input type="checkbox"/>	Direct	Local
192.168.10.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	20	<input type="checkbox"/>	Indirect	OSPF
192.168.10.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	20	<input type="checkbox"/>	Indirect	OSPF
0.0.0.0	0.0.0.0	0.0.0.0	WAN_ADSL	1	<input type="checkbox"/>	Indirect	Local

Page: 1, Items: 1 - 16

Abb. 40: Netzwerk -> Routen -> IP-Routen

Die OSPF-Status-Informationen können per GUI eingesehen werden.

(1) Gehen Sie zu **Monitoring -> OSPF -> Status**.

Save configuration

- Assistants
- System Management
- Physical Interfaces
- LAN
- Wireless LAN Controller
- Networking
- Routing Protocols
- Multicast
- WAN
- VPN
- Firewall
- VoIP
- Local Services
- Maintenance
- External Reporting
- Monitoring
 - Internal Log
 - IPSec
 - ISDN/Modem
 - Interfaces
 - HotSpot Gateway
 - QoS
 - OSPF**
 - PIM

Status Statistics

View All

OSPF Interfaces

View 20 per page << >> Filter in None equal Go

Interface	Designated Router	Backup Designated Router	Admin Status	State
en1-0	0.0.0.0	0.0.0.0	Disabled	Valid
en1-4	0.0.0.0	0.0.0.0	Disabled	Valid
efmoa70-0	0.0.0.0	0.0.0.0	Disabled	Valid
ADSL	0.0.0.0	0.0.0.0	Disabled	Valid
ethoa50-0	0.0.0.0	0.0.0.0	Disabled	Valid
IPSec_1	0.0.0.0	0.0.0.0	Enabled	Valid
IPSec_0	0.0.0.0	0.0.0.0	Enabled	Valid

Page: 1, Items: 1 - 7

OSPF Neighbors

View 20 per page << >> Filter in None equal Go

Neighbor	Router ID	Interface	State
192.168.0.254	192.168.0.254	IPSec_0	Complete
192.168.1.254	192.168.1.254	IPSec_1	Complete

Page: 1, Items: 1 - 9

OSPF Link State Database

View 20 per page << >> Filter in None equal Go

Area	Type	Link State ID	Router ID	Sequence Age
0.0.0.0	Router Link	192.168.10.254	192.168.10.254	1660
0.0.0.0	Router Link	192.168.0.254	192.168.0.254	821
0.0.0.0	Router Link	192.168.1.254	192.168.1.254	1681

Page: 1, Items: 1 - 12

Abb. 41: Monitoring -> OSPF -> Status

Die OSPF-Status-Informationen können auch per Konsolenbefehl eingesehen werden.

```

Datei Bearbeiten Ansicht Terminal Hilfe
Welcome to R3502 version V.7.10 Rev. 1 (Patch 3) IPsec from 2011/08/26 00:00:00
systemname is r3502, location

such / Dictio RouterForum DevWiki
Login: admin
Password:
View Online Help Logout
Password not changed. Call "setup" for quick configuration.

r3502:> ospfmon db
Area 0.0.0.0
Status Statistics

Router Link Age 861 Options 0x22 LsId 192.168.0.254
RtrId 192.168.0.254 Seq 0x8000001f Checksum 0x917d Len 108
options 0x0 links 7
Point to Point id 192.168.10.254 data 192.168.0.254 metric 10
Stub Network id 192.168.10.0 data 255.255.255.0 metric 10
Stub Network id 10.1.1.254 data 255.255.255.255 metric 164
Stub Network id 172.16.12.0 data 255.255.255.0 metric 1
Stub Network id 172.16.11.0 data 255.255.255.0 metric 1
Stub Network id 172.16.10.0 data 255.255.255.0 metric 1
Stub Network id 192.168.0.0 data 255.255.255.0 metric 1

Router Link Age 1721 Options 0x22 LsId 192.168.1.254
RtrId 192.168.1.254 Seq 0x8000002a Checksum 0xe583 Len 108
options 0x0 links 7
Point to Point id 192.168.10.254 data 192.168.1.254 metric 10
Stub Network id 192.168.10.0 data 255.255.255.0 metric 10
Stub Network id 10.1.1.254 data 255.255.255.255 metric 86
Stub Network id 172.16.3.0 data 255.255.255.0 metric 1
Stub Network id 172.16.2.0 data 255.255.255.0 metric 1
Stub Network id 172.16.1.0 data 255.255.255.0 metric 1
Stub Network id 192.168.1.0 data 255.255.255.0 metric 1

Router Link Age 1700 Options 0x22 LsId 192.168.10.254
RtrId 192.168.10.254 Seq 0x8000000b Checksum 0xa9bf Len 96
options 0x0 links 6
Point to Point id 192.168.0.254 data 192.168.10.254 metric 10
Stub Network id 192.168.0.0 data 255.255.255.0 metric 10
Point to Point id 192.168.1.254 data 192.168.10.254 metric 10
Stub Network id 192.168.1.0 data 255.255.255.0 metric 10
Stub Network id 10.1.1.254 data 255.255.255.255 metric 92
Stub Network id 192.168.10.0 data 255.255.255.0 metric 1

r3502:>

```

Abb. 42: Status-Informationen

4.4 Konfigurationsschritte im Überblick

Konfiguration des Gateways in der Zentrale

Feld	Menü	Wert
Verbindungstyp	Assistenten -> Internetzugang -> Internetverbindungen -> Neu	<i>Internes ADSL-Modem</i>
Beschreibung	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>ADSL</i>
Typ	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Benutzerdefiniert über PPPoE (PPP über Ethernet)</i>
Benutzername	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>feste-ip@provider.de</i>
Passwort	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>test12345</i>
Immer aktiv	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Aktiviert</i>
ADSL-Modus	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Annex B</i>
VPN-Szenario	Assistenten -> VPN -> VPN-Verbindungen -> Neu	<i>IPsec-LAN-zu-LAN-Verbindung</i>
Beschreibung	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>Standort-A</i>
Lokale IPsec ID	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>zentrale@bintec-elmeg.com</i>
Entfernte IPsec ID	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>rt3002_0@bintec-elmeg.com</i>
Preshared Key	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>test12345</i>
Lokale IP-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>192.168.10.254</i>
IP-Adresse des Remote-Netzwerks	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>192.168.0.0</i>
Netzmaske	Assistenten -> VPN -> VPN-	z. B. <i>255.255.255.0</i>

Feld	Menü	Wert
	Verbindungen -> Weiter	
Beschreibung	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>Standort-B</i>
Lokale IPsec ID	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>zentrale@bintec-elmeg.com</i>
Entfernte IPsec ID	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>rt3002_1@bintec-elmeg.com</i>
Preshared Key	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>test12345</i>
Lokale IP-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>192.168.10.254</i>
IP-Adresse des Remote-Netzwerks	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>192.168.1.0</i>
Netzmaske	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>255.255.255.0</i>
OSPF-Status	Routing Protokolle -> OSPF -> Globale Einstellungen	<i>Aktiviert</i>
Admin-Status	Routing Protokolle -> OSPF -> Schnittstellen -> <Standort-A> 	<i>Aktiv</i>
Admin-Status	Routing Protokolle -> OSPF -> Schnittstellen -> <Standort-B> 	<i>Aktiv</i>


Konfiguration des Gateways am Standort A

Feld	Menü	Wert
Verbindungstyp	Assistenten -> Internetzugang -> Internetverbindungen -> Neu	<i>Internes ADSL-Modem</i>
Beschreibung	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>ADSL</i>
Typ	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Benutzerdefiniert über PPPoE (PPP über Ethernet)</i>
Benutzername	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>feste-ip@provider.de</i>
Passwort	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>test12345</i>

Feld	Menü	Wert
Immer aktiv	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Aktiviert</i>
ADSL-Modus	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Annex B</i>
Verbindungstyp	Assistenten -> VPN -> VPN-Verbindungen -> Neu	<i>Internes ADSL-Modem</i>
Beschreibung	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	<i>z. B. Zentrale</i>
Lokale IPsec ID	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	<i>z. B. rt3002_0@bintec-elmeg.com</i>
Entfernte IPsec ID	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	<i>z. B. zentrale@bintec-elmeg.com</i>
Preshared Key	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	<i>z. B. test12345</i>
Lokale IP-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	<i>z. B. 192.168.0.254</i>
IPsec Peer-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	<i>z. B. 62.63.64.65</i>
IP-Adresse des Remote-Netzwerks	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	<i>z. B. 192.168.10.0</i>
Netzmaske	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	<i>z. B. 255.255.255.0</i>
OSPF-Status	Routing Protokolle -> OSPF -> Globale Einstellungen	<i>Aktiviert</i>
Admin-Status	Routing Protokolle -> OSPF -> Schnittstellen -> <Zentrale> 	<i>Aktiv</i>

Konfiguration des Gateways am Standort B

Feld	Menü	Wert
Verbindungstyp	Assistenten -> Internetzugang -> Internetverbindungen -> Neu	<i>Internes ADSL-Modem</i>
Beschreibung	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>z. B. ADSL</i>
Typ	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Benutzerdefiniert über PPPoE (PPP über Ethernet)</i>

Feld	Menü	Wert
Benutzername	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>feste-ip@provider.de</i>
Passwort	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	z. B. <i>test12345</i>
Immer aktiv	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Aktiviert</i>
ADSL-Modus	Assistenten -> Internetzugang -> Internetverbindungen -> Weiter	<i>Annex B</i>
Verbindungstyp	Assistenten -> VPN -> VPN-Verbindungen -> Neu	<i>Internes ADSL-Modem</i>
Beschreibung	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>Zentrale</i>
Lokale IPsec ID	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>rt3002_1@bintec-elmeg.com</i>
Entfernte IPsec ID	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>zentrale@bintec-elmeg.com</i>
Preshared Key	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>test12345</i>
Lokale IP-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>192.168.1.254</i>
IPsec Peer-Adresse	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>62.63.64.65</i>
IP-Adresse des Remote-Netzwerks	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>192.168.10.0</i>
Netzmaske	Assistenten -> VPN -> VPN-Verbindungen -> Weiter	z. B. <i>255.255.255.0</i>
OSPF-Status	Routing Protokolle -> OSPF -> Globale Einstellungen	<i>Aktiviert</i>
Admin-Status	Routing Protokolle -> OSPF -> Schnittstellen -> <Zentrale> 	<i>Aktiv</i>

Kapitel 5 IP - Routing-Protokoll RIPv2 über IP-Sec-Verbindung

5.1 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.

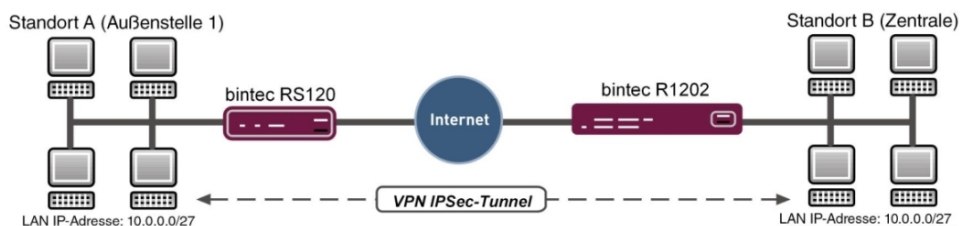


Abb. 43: Beispielszenario

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 z. B. **bintec R1202** in der Zentrale

- Ein VPN-Gateway z. B. **bintec RS120** in der Außenstelle
- Ein Bootimage der Version 7.10.1 auf beiden Gateways
- Beide Gateways benötigen eine unabhängige Verbindung zum Internet

Hinweise zum Test-Setup

RS120 Standort A (Außenstelle):

System-Name	RS120-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.)

R1202 Standort B (Zentrale):

System-Name	R1202-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.)

5.2 Konfiguration

5.2.1 Konfiguration des bintec R1202 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**.

The screenshot shows the configuration page for a new IPsec peer. The left sidebar contains a navigation menu with categories like 'Assistenten', 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN Controller', 'Netzwerk', 'Routing-Protokolle', 'Multicast', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe', and 'Monitoring'. The 'VPN' menu is expanded to show 'IPsec', 'L2TP', 'PPTP', and 'GRE'. The main content area has tabs for 'IPsec-Peers', 'Phase-1-Profil', 'Phase-2-Profil', 'XAUTH-Profil', 'IP Pools', and 'Optionen'. The 'IPsec-Peers' tab is active, showing the configuration form.

Abb. 44: 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. *RS120-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 R1202** 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 Subnetmask 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** -> .

Abb. 45: VPN -> IPsec -> Phase-1-Profil ->

Gehen Sie folgendermaßen vor:

- (1) Bei **Lokaler ID-Wert** geben Sie die ID Ihres Geräts ein, hier z. B. *R1202-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>**



Abb. 46: Routing-Protokolle -> RIP -> RIP-Schnittstellen -><Außenstelle-1>

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 verwen-

deute 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**.

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

Abb. 47: 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 R1202**-Gateways abgeschlossen.

5.2.2 Konfiguration des bintec RS120 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-Profilen verwendet.

Gehen Sie dazu in folgendes Menü:

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

Konfiguration speichern

- Assistenten
- Systemverwaltung
- Physikalische Schnittstellen
- LAN
- Wireless LAN
- Netzwerk
- Routing-Protokolle
- Multicast
- WAN
- VPN
 - IPSec
 - L2TP
 - PPTP
 - GRE
- Firewall
- VoIP
- Lokale Dienste
- Wartung
- Externe Berichterstellung
- Monitoring

IPSec-Peers
Phase-1-Profil
Phase-2-Profil
XAUTH-Profil
IP Pools
Optionen

Peer-Parameter

Administrativer Status	<input checked="" type="radio"/> Aktiv <input type="radio"/> Inaktiv
Beschreibung	Zentrale
Peer-Adresse	62.147.1.1
Peer-ID	Fully Qualified Domain Name (FQDN) R1202-Zentrale
IKE (Internet Key Exchange)	IKEv1
Preshared Key	••••••••
Schnittstellenrouten	
IP-Adressenvergabe	Statisch
Standardroute	<input type="checkbox"/> Aktiviert
Lokale IP-Adresse	1.0.0.1
Routeneinträge	
Entfernte IP-Adresse	Netzmaske
1.0.0.2	255.255.255.255
	Metrik
	1
<input type="button" value="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	<input checked="" type="radio"/> Ein Benutzer <input type="radio"/> Mehrere Benutzer
Startmodus	<input type="radio"/> Auf Anforderung <input checked="" type="radio"/> Immer aktiv
Erweiterte IP-Optionen	
Überprüfung der Rückroute	<input type="checkbox"/> Aktiviert
Proxy ARP	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Immer aktiv
IPsec-Callback	
Modus	Inaktiv

Abb. 48: 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. *R1202-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 RS120** 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 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** -> .

The screenshot shows the configuration page for the Phase-1-Profile of an IPsec VPN. The left sidebar contains a navigation menu with 'VPN' expanded and 'IPSec' selected. The main content area has tabs for 'IPSec-Peers', 'Phase-1-Profile', 'Phase-2-Profile', 'XAUTH-Profil', 'IP Pools', and 'Optionen'. The 'Phase-1-Parameter (IKE)' section includes:

- Beschreibung:** Multi-Proposal
- Proposals:** A table with columns for 'Verschlüsselung', 'Authentifizierung', and 'Aktiviert'.

Verschlüsselung	Authentifizierung	Aktiviert
AES	SHA1	<input type="checkbox"/>
AES	MD5	<input checked="" type="checkbox"/>
3DES	MD5	<input checked="" type="checkbox"/>
- DH-Gruppe:** Radio buttons for 1 (768 Bit), 2 (1024 Bit) (selected), and 5 (1536 Bit).
- Lebensdauer:** 14400 Sekunden, 0 kbytes, and a checkbox for 'Schlüssel erneut erstellen nach' with a value of 80%.
- Authentifizierungsmethode:** Preshared Keys
- Modus:** Radio buttons for Main Modus (ID Protect) (selected), Aggressiv, and Strikt.
- Lokaler ID-Typ:** Fully Qualified Domain Name (FQDN)
- Lokaler ID-Wert:** RS120-Aussenstelle-1

At the bottom, there is a section for 'Erweiterte Einstellungen' with 'OK' and 'Abbrechen' buttons.

Abb. 49: VPN -> IPsec -> Phase-1-Profil ->

Gehen Sie folgendermaßen vor:

- (1) Bei **Lokaler ID-Wert** geben Sie die ID Ihres Geräts ein, hier z. B. *RS120-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>** .

The screenshot shows the configuration page for the RIP protocol on the 'Zentrale' interface. The left sidebar has 'Routing-Protokolle' expanded and 'RIP' selected. The main content area has tabs for 'RIP-Schnittstellen', 'RIP-Filter', and 'RIP-Optionen'. The 'RIP-Parameter für: Zentrale' section includes:

- Version in Senderichtung:** RIP V2 Multicast
- Version in Empfangsrichtung:** RIP V2
- Routenankündigung:** Aktiv oder Ruhend

At the bottom, there are 'OK' and 'Abbrechen' buttons.

Abb. 50: 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 verwen-

deute 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**.

The screenshot shows the 'RIP-Optionen' configuration window. On the left is a navigation menu with 'Routing-Protokolle' expanded to 'RIP'. The main window has tabs for 'RIP-Schnittstellen', 'RIP-Filter', and 'RIP-Optionen'. The 'Globale RIP-Parameter' section contains the following settings:

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

At the bottom of the window are 'OK' and 'Abbrechen' buttons.

Abb. 51: **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 RS120**-Gateways abgeschlossen.

5.3 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 -> IP-Routen**.

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

Ergebnis: Standort B (Zentrale)

Konfiguration speichern

Assistenten

Systemverwaltung

Physikalische Schnittstellen

LAN

Wireless LAN Controller

Netzwerk

Routen

NAT

Lastverteilung

QoS

Zugriffsregeln

Routing-Protokolle

Multicast

WAN

IP-Routen Optionen

Ansicht 20 pro Seite << >> Filtern in Keiner gleich Los

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

Seite: 1, Objekte: 1 - 6

Neu

Abb. 52: Netzwerk -> Routen -> IP-Routen

Ergebnis: Standort A (Außenstelle)

Konfiguration speichern

Assistenten

Systemverwaltung

Physikalische Schnittstellen

LAN

Netzwerk

Routen

NAT

Lastverteilung

QoS

Zugriffsregeln

Routing-Protokolle

Multicast

WAN

VPN

IP-Routen Optionen

Ansicht 20 pro Seite << >> Filtern in Keiner gleich Los

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

Seite: 1, Objekte: 1 - 6

Neu

Abb. 53: Netzwerk -> Routen -> IP-Routen

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

5.4 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>RS120-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>R1202-Zentrale</i>

Routing-Protokoll konfigurieren

Feld	Menü	Wert
Version in Sende- richtung	Routing-Protokolle -> RIP -> RIP-Schnittstellen -><Außenstelle-1> 	<i>RIP V2 Multicast</i>
Version in Empfangsrichtung	Routing-Protokolle -> RIP -> RIP-Schnittstellen -><Außenstelle-1> 	<i>RIP V2</i>
Routenankündigung	Routing-Protokolle -> RIP -> RIP-Schnittstellen -><Außenstelle-1> 	<i>Nur aktiv</i>

RIP-Optionen einstellen

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

IPSec-Verbindung konfigurieren (Außenstelle)




Feld	Menü	Wert
Beschreibung	VPN -> IPSec -> IPSec-Peers -> Neu	z. B. <i>Zentrale</i>

Feld	Menü	Wert
Peer-Adresse	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. 62.147.1.1
Peer-ID	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. R1202-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. RS120-Aussenstelle-1

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
Routenankündigung	Routing-Protokolle -> RIP -> RIP- Schnittstellen -><Außenstelle-1> 	Aktiv oder Ruhend

RIP-Optionen einstellen

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

Kapitel 6 IP - ULA - Unique Local Addresses

6.1 Einleitung

Das Internet Protocol Version 6 (IPv6) wird als Nachfolger von IPv4 benötigt, da der Adressraum von IPv4 demnächst erschöpft ist.



Hinweis

IPv4-Adressen werden immer noch benötigt! Es wird empfohlen den Router direkt als Perimetersystem ohne einen Router davor zu betreiben. Der Grund ist die Verwendung von 6in4 und das Timeout der Sitzungen.

In unserem Beispiel wird die Vernetzung von IPv4 im WAN und IPv6 im LAN mit ULA (Unique Local Addresses) beschrieben.

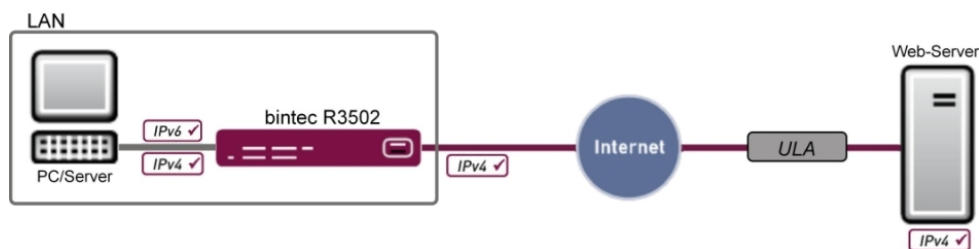


Abb. 54: Beispielszenario

WAN	LAN
WAN-Schnittstelle: en1-4	LAN-Schnittstelle: en1-0
IP-Adresse : 192.168.100.110/24	IP-Adresse : 192.168.0.254/24
Gateway IP-Adresse: 192.168.100.254	DHCP-Range: 192.168.0.10 - 192.168.0.39

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

Das GUI ist eine web-basierte grafische Benutzeroberfläche, die Sie von jedem PC aus mit einem aktuellen Web-Browser über eine HTTP- oder HTTPS-Verbindung bedienen können.

Um Ihr Gateway mit dem GUI konfigurieren zu können, müssen Sie über die serielle Schnittstelle, über LAN oder über eine ISDN-Verbindung auf das Gerät zugreifen. Sie müssen einen Web-Browser aufrufen, die IP-Adresse Ihres Geräts in die Adresszeile des Brow-

sers eingeben und sich mit Benutzername sowie Passwort einloggen.

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein bintec Gateway der RS-, der Rxxx2- oder der RXL-Serie z. B. **bintec R3502** mit Systemsoftware 8.2.1
- Eine funktionierende Verbindung zum Internet
- Internet Protocol Version 6 (IPv6) aktiv auf den entsprechenden Rechnern (bei Windows 7 ist IPv6 standardmäßig aktiviert)
- Grundkonfiguration aller benötigten Schnittstellen
- Eventuell ein eigener ULA-Bereich; dieser kann bei SixXS beantragt werden.

6.2 Konfiguration

Zuerst konfigurieren Sie die Schnittstelle, danach legen Sie einen Präfix an und lassen automatisch ein Subnetz erstellen. Eine Route wird ebenfalls automatisch angelegt.

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

The screenshot shows a web-based configuration interface for a network device. On the left is a navigation menu with categories like 'Assistenten', 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'IP-Konfiguration', 'VLAN', 'Wireless LAN Controller', 'Netzwerk', 'Routing-Protokolle', 'Multicast', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstattung', and 'Monitoring'. The 'IP-Konfiguration' section is expanded, showing 'VLAN' and 'Netzwerk' sub-sections. The main area is titled 'Schnittstellen' and shows the configuration for a new interface (VLAN-ID 1). The configuration is divided into several sections: 'Basisparameter' (Basic parameters), 'Grundlegende IPv4-Parameter' (Basic IPv4 parameters), 'Grundlegende IPv6-Parameter' (Basic IPv6 parameters), and 'Erweiterte Einstellungen' (Advanced settings). The 'Basisparameter' section includes 'Basierend auf Ethernet-Schnittstelle' (en1-0), 'Schnittstellenmodus' (Untagged), 'VLAN-ID' (1), and 'MAC-Adresse' (00:00:00:00:00:00). The 'Grundlegende IPv4-Parameter' section includes 'Adressmodus' (Statisch) and 'IP-Adresse / Netzmaske' (with a 'Hinzufügen' button). The 'Grundlegende IPv6-Parameter' section includes 'IPv6' (Aktiviert), 'Sicherheitsrichtlinie' (Sicher), 'Zusätzliche IPv6-Adresskonfiguration' (Aktiviert), 'IPv6-Modus' (Router), 'Rolle bei der Präfixdelegation' (Downstream), 'Router Advertisement übertragen' (Aktiviert), 'IPv6-Präfix/Länge' (with a 'Hinzufügen' button), and 'Standardrouter' (Aktiviert). The 'Erweiterte Einstellungen' section is currently empty. At the bottom are 'OK' and 'Abbrechen' buttons.

Abb. 55: LAN -> IP-Konfiguration -> Schnittstellen -> Neu

Gehen Sie folgendermaßen vor, um eine Schnittstelle für IPv6 zu konfigurieren:

- (1) Wählen Sie bei **Basierend auf Ethernet-Schnittstelle** die Schnittstelle aus, welche für IPv6 verwendet wird, hier z. B. *en1-0*.
- (2) Bei **IPv6** wählen Sie *Aktiviert* aus.
- (3) Bei **Sicherheitsrichtlinie** belassen Sie die Einstellung *Sicher*. Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.
- (4) Bei **IPv6-Modus** belassen Sie die Einstellung *Router*.
- (5) Bei **Rolle bei der Präfixdelegation** belassen Sie die Einstellung *Downstream*.
- (6) Für **Router Advertisement übertragen** belassen Sie *Aktiviert*. Router Advertisements werden über die gewählte Schnittstelle gesendet.
- (7) Klicken Sie unter **IPv6-Präfix/Länge** auf **Hinzufügen**, um einen Präfix anzulegen und ein Subnetz automatisch erstellen zu lassen.

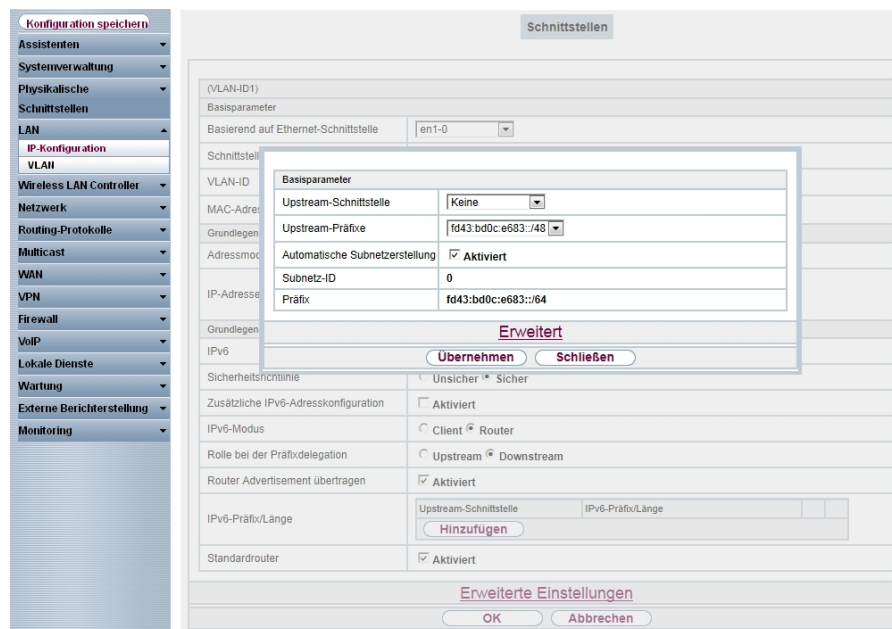


Abb. 56: LAN -> IP-Konfiguration -> Schnittstellen -> Neu -> Hinzufügen

- (8) Bei **Upstream-Schnittstelle** wählen Sie *Keine* aus.



Hinweis

Diese Einstellung ist wichtig, da es für Unique Local Addresses (ULAs) keine "Upstream"-Schnittstelle gibt, zu der Pakete transportiert werden können.

- (9) Bei **Upstream-Präfixe** wählen Sie den angezeigten Präfix *fd43:bd0c:e683::/48* aus.
- (10) Belassen Sie die Einstellung **Automatische Subnetzerstellung** *Aktiviert*.
Die automatisch erzeugte **Subnetz-ID** *0* und der automatisch erzeugte **Präfix** *fd43:bd0c:e683::/64* für das Subnetz werden angezeigt.
- (11) Bestätigen Sie Ihre Angaben mit **Übernehmen**.
- (12) Belassen Sie die Einstellung **Standardrouter** *Aktiviert*.
- (13) Bestätigen Sie Ihre Angaben mit **OK**.

Unter **Netzwerk->Routen ->IPv6-Routen** ist bereits eine Route automatisch angelegt, die nicht editiert werden kann. Sie brauchen keine weitere Route zu konfigurieren. Alle Geräte können über diese direkte Route erreicht werden.

6.3 Konfigurationsschritte im Überblick

Schnittstelle konfigurieren

Feld	Menü	Wert
Basierend auf Ethernet-Schnittstelle	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	z. B. <i>en1-0</i>
IPv6	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>Aktiviert</i>
Sicherheitsrichtlinie	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>Sicher</i>
IPv6-Modus	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>Router</i>
Rolle bei der Präfixdelegation	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>Downstream</i>
Router Advertisement übertragen	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>Aktiviert</i>
Standardrouter	LAN -> IP-Konfiguration -> Schnittstellen -> Neu	<i>Aktiviert</i>

Adressraum zuweisen

Feld	Menü	Wert
Upstream-Schnittstelle	LAN -> IP-Konfiguration -> Schnittstellen-> Neu -> Hinzufügen	<i>Keine</i>
Upstream-Präfixe	LAN -> IP-Konfiguration -> Schnittstellen-> Neu -> Hinzufügen	<i>fd43:bd0c:e683::/48</i>
Automatische Subnetzzerstellung	LAN -> IP-Konfiguration -> Schnittstellen-> Neu -> Hinzufügen	<i>Aktiviert</i>

Kapitel 7 IP - IPv6 LAN-Routing

7.1 Einleitung

In diesem Beispiel wird das IPv6-Routing zwischen zwei Netzwerken mit ULA-Präfixen beschrieben. Hierfür werden an einem Router an den zwei Schnittstellen en1-0 und en1-4 je ein ULA-Präfix mit Subnetz-ID konfiguriert. Hierbei ist es wichtig, dass keine Upstream-Schnittstelle ausgewählt wird, da es bei diesem Szenario keinen übergeordneten Präfix gibt.

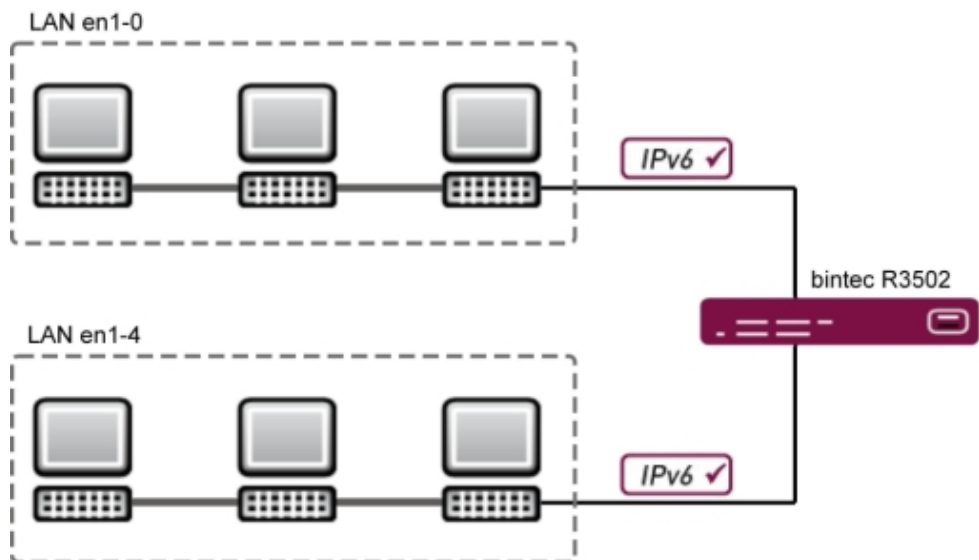


Abb. 57: Beispielszenario

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

Das GUI ist eine web-basierte grafische Benutzeroberfläche, die Sie von jedem PC aus mit einem aktuellen Web-Browser über eine HTTP- oder HTTPS-Verbindung bedienen können.

Um Ihr Gateway mit dem GUI konfigurieren zu können, müssen Sie über die serielle Schnittstelle, über LAN oder über eine ISDN-Verbindung auf das Gerät zugreifen. Sie müssen einen Web-Browser aufrufen, die IP-Adresse Ihres Geräts in die Adresszeile des Browsers eingeben und sich mit Benutzername sowie Passwort einloggen.

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

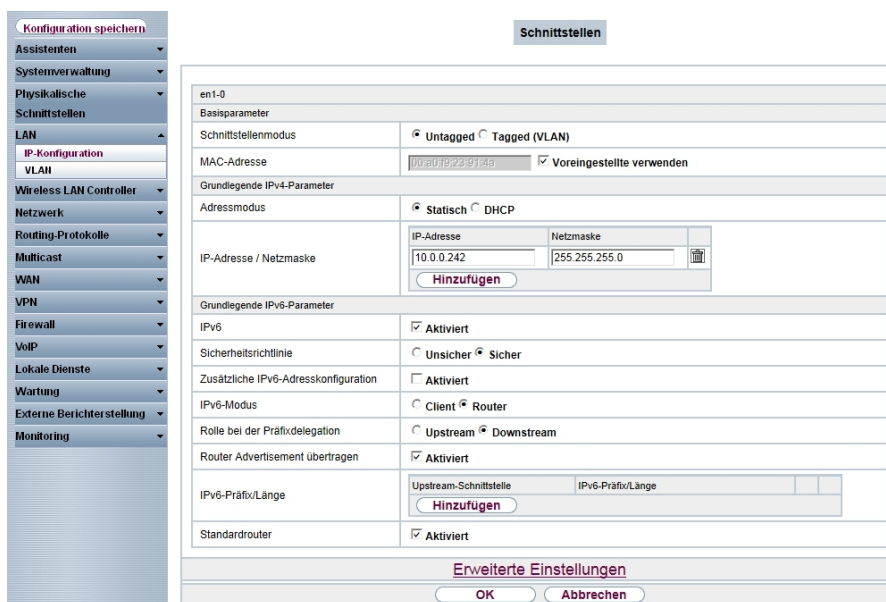
- Ein bintec Gateway der RS-, der Rxxx2- oder der RXL-Serie z. B. **bintec R3502** mit Systemsoftware 8.2.1
- Internet Protocol Version 6 (IPv6) aktiv auf den entsprechenden Rechnern (bei Windows 7 ist IPv6 standardmäßig aktiviert)
- Grundkonfiguration aller benötigten Schnittstellen
- Eventuell ein eigener ULA-Bereich; dieser kann bei einem Tunnel Brocker, z. B. bei SixXS, beantragt werden.

7.2 Konfiguration

Für die Konfiguration muss an der jeweiligen Schnittstelle ein ULA-Präfix angelegt werden.

Gehen Sie folgendermaßen vor, um für die Schnittstelle **<en1-0>** einen ULA-Präfix anzulegen:

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



The screenshot shows the configuration page for interface **en1-0**. The left sidebar contains a navigation menu with categories like 'Assistenten', 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN Controller', 'Netzwerk', 'Routing-Protokolle', 'Multicast', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstattung', and 'Monitoring'. The 'LAN' section is expanded, showing 'IP-Konfiguration' and 'VLAN'. The main content area is titled 'Schnittstellen' and shows the configuration for 'en1-0'. The 'Basisparameter' section includes 'Schnittstellenmodus' (Untagged selected), 'MAC-Adresse' (00:00:22:01:00:00), and 'Voreingestellte verwenden' (checked). The 'Grundlegende IPv4-Parameter' section shows 'Adressmodus' (Statisch selected) and 'IP-Adresse / Netzmaske' (10.0.0.242 / 255.255.255.0). The 'Grundlegende IPv6-Parameter' section shows 'IPv6' (Aktiviert checked), 'Sicherheitsrichtlinie' (Sicher selected), 'Zusätzliche IPv6-Adresskonfiguration' (not checked), 'IPv6-Modus' (Router selected), 'Rolle bei der Präfixdelegation' (Downstream selected), 'Router Advertisement übertragen' (checked), and 'IPv6-Präfix/Länge' (Upstream-Schnittstelle and IPv6-Präfix/Länge fields). The 'Standardrouter' is also checked. At the bottom, there are 'Erweiterte Einstellungen', 'OK', and 'Abbrechen' buttons.

Abb. 58: **LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0>** 

- (2) Bei **IPv6** wählen Sie *Aktiviert* aus.

- (3) Bei **Sicherheitsrichtlinie** belassen Sie die Einstellung *Sicher*. Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.
- (4) Bei **IPv6-Modus** belassen Sie die Einstellung *Router*.
- (5) Bei **Rolle bei der Prefixdelegation** belassen Sie die Einstellung *Downstream*.
- (6) Für **Router Advertisement übertragen** belassen Sie *Aktiviert*. Router Advertisements werden über die gewählte Schnittstelle gesendet.
- (7) Klicken Sie unter **IPv6-Präfix/Länge** auf **Hinzufügen**, um ein Subnetz automatisch erstellen zu lassen.

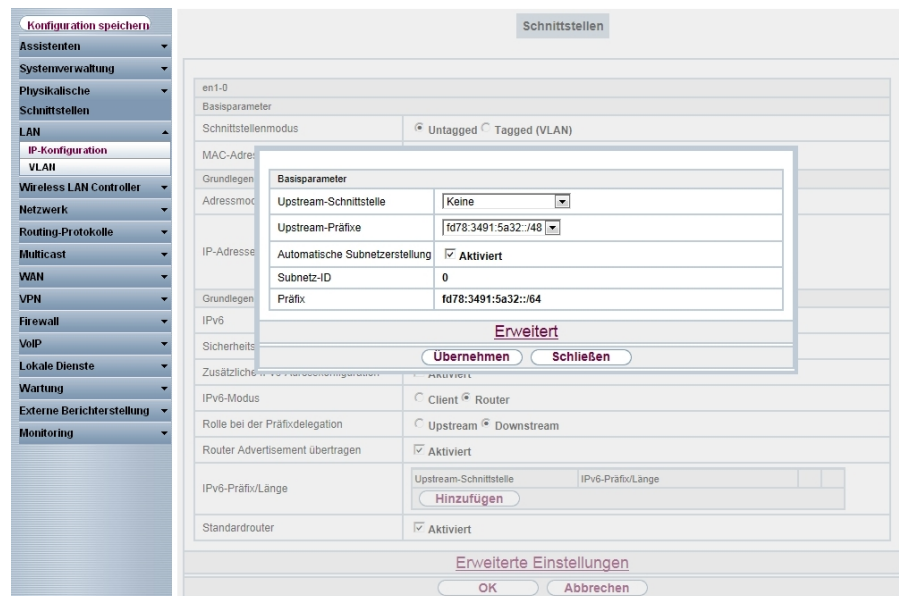
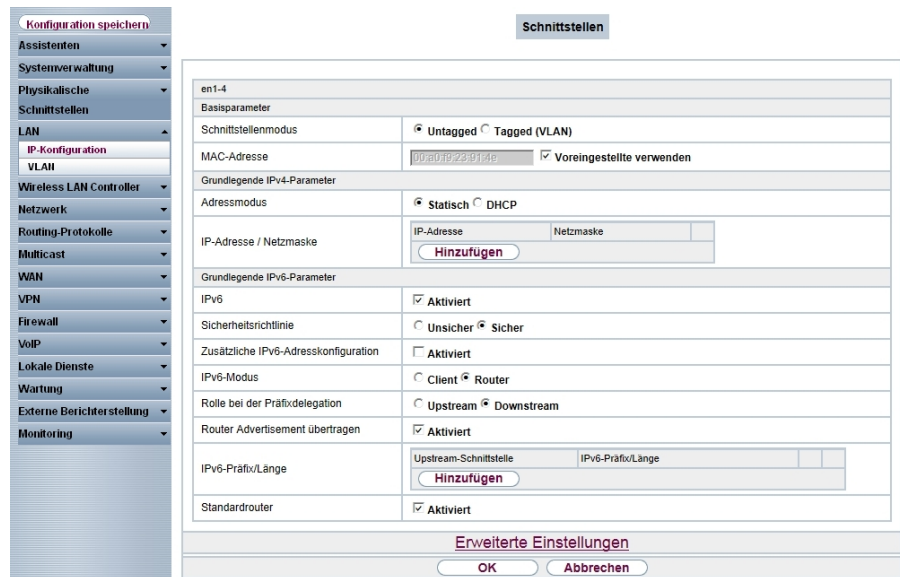


Abb. 59: LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0> -> Hinzufügen

- (8) Bei **Upstream-Schnittstelle** wählen Sie *Keine*.
- (9) Bei **Upstream-Präfixe** wählen Sie den angezeigten Präfix *fd78:3491:5a32::/48* aus.
- (10) Belassen Sie die Einstellung **Automatische Subnetzerstellung** *Aktiviert*. Die automatisch erzeugte **Subnetz-ID** *0* und der automatisch erzeugte Präfix *fd78:3491:5a32::/64* werden angezeigt.
- (11) Bestätigen Sie Ihre Angaben mit **Übernehmen**.
- (12) Belassen Sie die Einstellung **Standardrouter** *Aktiviert*.
- (13) Bestätigen Sie Ihre Angaben mit **OK**.

Gehen Sie folgendermaßen vor, um für die Schnittstelle <en1-4> einen ULA-Präfix anzulegen:

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



en1-4					
Basisparameter					
Schnittstellenmodus	<input checked="" type="radio"/> Untagged <input type="radio"/> Tagged (VLAN)				
MAC-Adresse	00:80:1B:23:91:4B <input checked="" type="checkbox"/> Voreingestellte verwenden				
Grundlegende IPv4-Parameter					
Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> DHCP				
IP-Adresse / Netzmaske	<table border="1"> <tr> <td>IP-Adresse</td> <td>Netzmaske</td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </table> <input type="button" value="Hinzufügen"/>	IP-Adresse	Netzmaske	<input type="text"/>	<input type="text"/>
IP-Adresse	Netzmaske				
<input type="text"/>	<input type="text"/>				
Grundlegende IPv6-Parameter					
IPv6	<input checked="" type="checkbox"/> Aktiviert				
Sicherheitsrichtlinie	<input type="radio"/> Unsicher <input checked="" type="radio"/> Sicher				
Zusätzliche IPv6-Adresskonfiguration	<input type="checkbox"/> Aktiviert				
IPv6-Modus	<input type="radio"/> Client <input checked="" type="radio"/> Router				
Rolle bei der Präfixdelegation	<input type="radio"/> Upstream <input checked="" type="radio"/> Downstream				
Router Advertisement übertragen	<input checked="" type="checkbox"/> Aktiviert				
IPv6-Präfix/Länge	<table border="1"> <tr> <td>Upstream-Schnittstelle</td> <td>IPv6-Präfix/Länge</td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </table> <input type="button" value="Hinzufügen"/>	Upstream-Schnittstelle	IPv6-Präfix/Länge	<input type="text"/>	<input type="text"/>
Upstream-Schnittstelle	IPv6-Präfix/Länge				
<input type="text"/>	<input type="text"/>				
Standardrouter	<input checked="" type="checkbox"/> Aktiviert				
Erweiterte Einstellungen					
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

Abb. 60: **LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4>** 

- (2) Bei **IPv6** wählen Sie *Aktiviert* aus.
- (3) Bei **Sicherheitsrichtlinie** belassen Sie die Einstellung *Sicher* . Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.
- (4) Bei **IPv6-Modus** belassen Sie die Einstellung *Router* .
- (5) Bei **Rolle bei der Präfixdelegation** belassen Sie die Einstellung *Downstream* .
- (6) Für **Router Advertisement übertragen** belassen Sie *Aktiviert* . Router Advertisements werden über die gewählte Schnittstelle gesendet.
- (7) Klicken Sie unter **IPv6-Präfix/Länge** auf **Hinzufügen**, um ein Subnetz automatisch erstellen zu lassen.

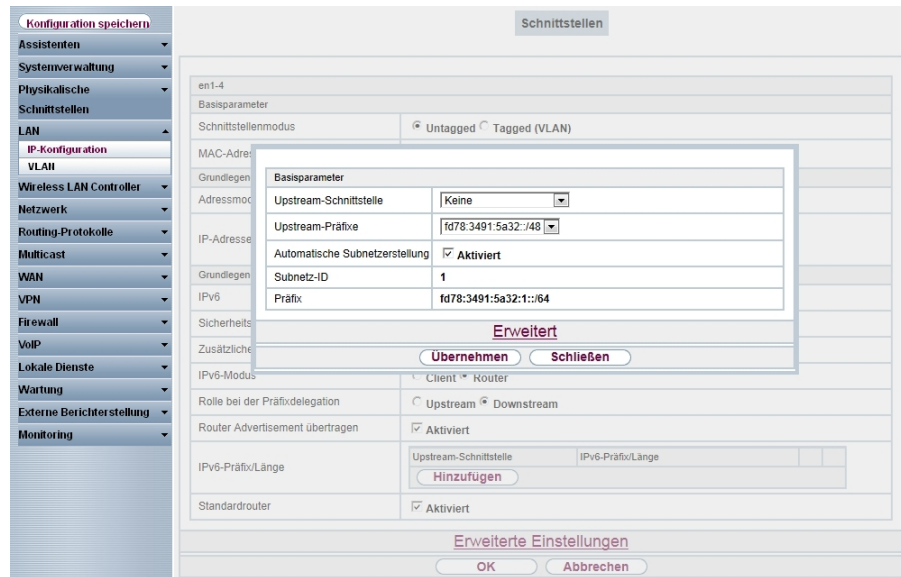


Abb. 61: LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4>  -> Hinzufügen

- (8) Bei **Upstream-Schnittstelle** wählen Sie *Keine*.
- (9) Bei **Upstream-Präfixe** wählen Sie den angezeigten Präfix *fd78:3491:5a32::/48* aus.
- (10) Belassen Sie die Einstellung **Automatische Subnetzerstellung** *Aktiviert*.
Die automatisch erzeugte **Subnetz-ID** *1* und der automatisch erzeugte Präfix *fd78:3491:5a32:1::/64* werden angezeigt.
- (11) Bestätigen Sie Ihre Angaben mit **Übernehmen**.
- (12) Belassen Sie die Einstellung **Standardrouter** *Aktiviert*.
- (13) Bestätigen Sie Ihre Angaben mit **OK**.






Durch das Konfigurieren der beiden Präfixe werden automatisch zwei neue Routen angelegt, welche die Kommunikation zwischen den beiden Netzwerken ermöglichen.

7.3 Konfigurationsschritte im Überblick




Schnittstelle <en1-0>

Schnittstelle konfigurieren

Feld	Menü	Wert
IPv6	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0> 	<i>Aktiviert</i>




Feld	Menü	Wert
Sicherheitsrichtlinie	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0> 	<i>Sicher</i>
IPv6-Modus	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0> 	<i>Router</i>
Rolle bei der Präfixdelegation	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0> 	<i>Downstream</i>
Router Advertisement übertragen	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0> 	<i>Aktiviert</i>
Standardrouter	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0> 	<i>Aktiviert</i>



Adressraum zuweisen

Feld	Menü	Wert
Upstream-Schnittstelle	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0>  ->Hinzufügen	<i>Keine</i>
Upstream-Präfixe	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0>  ->Hinzufügen	<i>fd78:3491:5a32::/48</i>
Automatische Subnetzerstellung	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-0>  ->Hinzufügen	<i>Aktiviert</i>




Schnittstelle <en1-4>

Schnittstelle konfigurieren

Feld	Menü	Wert
IPv6	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4> 	<i>Aktiviert</i>
Sicherheitsrichtlinie	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4> 	<i>Sicher</i>
IPv6-Modus	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4> 	<i>Router</i>
Rolle bei der Präfixdelegation	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4> 	<i>Downstream</i>
Router Advertisement	LAN -> IP-Konfiguration ->	<i>Aktiviert</i>

Feld	Menü	Wert
übertragen	Schnittstellen-> <en1-4> 	
Standardrouter	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4> 	<i>Aktiviert</i>

Adressraum zuweisen

Feld	Menü	Wert
Upstream-Schnittstelle	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4>  -> Hinzufügen	<i>Keine</i>
Upstream-Präfixe	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4>  -> Hinzufügen	<i>fd78:3491:5a32::/48</i>
Automatische Subnetzerstellung	LAN -> IP-Konfiguration -> Schnittstellen-> <en1-4>  -> Hinzufügen	<i>Aktiviert</i>

Kapitel 8 IP - Tunnel Broker SixXS mit dem ::/48-Präfix

8.1 Einleitung

In diesem Beispiel wird die Vernetzung von IPv4 im WAN und IPv4/IPv6 im LAN über einen Tunnel Broker mit dem ::/48-Präfix von SixXS beschrieben. Mit einem Tunnel und entsprechendem Präfix kann sich der Rechner im eigenen LAN mit gültigen IPv6-Adressen versorgen.

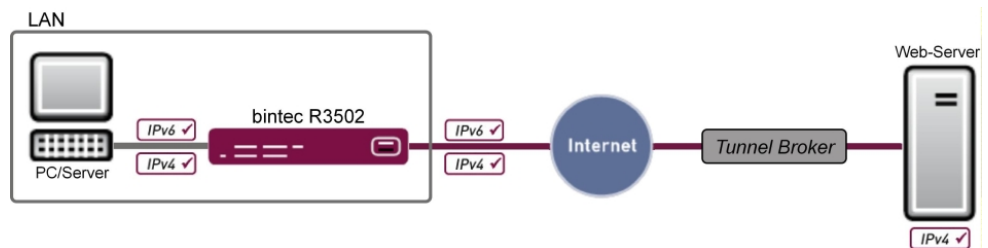


Abb. 62: Beispielszenario

WAN	LAN
WAN-Schnittstelle: Internet Service Provider über DSL	LAN-Schnittstelle: en1-0
IP-Adresse : Dynamische IP-Adresse	IP-Adresse : 192.168.0.254/24
	DHCP-Range: 192.168.0.10 - 192.168.0.39

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

Das GUI ist eine web-basierte grafische Benutzeroberfläche, die Sie von jedem PC aus mit einem aktuellen Web-Browser über eine HTTP- oder HTTPS-Verbindung bedienen können.

Um Ihr Gateway mit dem GUI konfigurieren zu können, müssen Sie über die serielle Schnittstelle, über LAN oder über eine ISDN-Verbindung auf das Gerät zugreifen. Sie müssen einen Web-Browser aufrufen, die IP-Adresse Ihres Geräts in die Adresszeile des Browsers eingeben und sich mit Benutzernamen sowie Passwort einloggen.

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein bintec Gateway der RS-, der Rxxx2- oder der RXL-Serie z. B. **bintec R3502** mit Systemsoftware 8.2.1
- Eine funktionierende Verbindung zum Internet
- Internet Protocol Version 6 (IPv6) aktiv auf den entsprechenden Rechnern (bei Windows 7 ist IPv6 standardmäßig aktiviert)
- Grundkonfiguration aller benötigten Schnittstellen
- Zugang sowie Netzwerk-Präfix bei einem Tunnel Broker, z. B. bei SixXS.

8.2 Konfiguration

Im ersten Schritt wird die Schnittstelle konfiguriert und der zugeteilte Präfix eingetragen.

Gehen Sie dazu in folgendes Menü:

- (1) Gehen Sie zu **WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu**.

Abb. 63: **WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu**

Gehen Sie folgendermaßen vor, um die Schnittstelle für IPv6 mit SixXS zu konfigurieren und den Präfix einzutragen:

- (1) Geben Sie eine **Beschreibung** für die Schnittstelle ein, z. B. *Mein_SIXXS_Account*.
- (2) Bei **Tunnelmodus** wählen Sie *SixXS* aus. Ein SixXS-Tunnel (SixXS-Konfigurationsprofil für eine 6in4-Tunnel-Konfiguration) wird verwendet.
- (3) Bei **Sicherheitsrichtlinie** belassen Sie die Einstellung *Unsicher*. Es werden nur IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert wurde. Verwenden Sie diese Einstellung, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.
- (4) Bei **Über Schnittstelle** wählen Sie die WAN-Schnittstelle aus, hier *WAN_SCHNITTSTELLE*.

- (5) Bei **Benutzername** geben Sie den SixXS-Benutzernamen ein, den Sie von SixXS erhalten haben, z. B. *PCP4-SIXXS*.
- (6) Bei **Passwort** geben Sie das Tunnelpasswort ein, das Sie für Ihren Tunnel bei SixXS konfiguriert haben.
- (7) Bei **Tunnel-ID** geben Sie die Tunnel-ID Ihres SixXS-Tunnels ein, die Ihnen SixXS zugeteilt hat.
- (8) Klicken Sie unter **Zugewiesener IPv6-Präfix/Länge** auf **Hinzufügen**.
- (9) Bei **IPv6-Präfix** und **Länge** geben Sie die Werte ein, die Sie von Ihrem Service Provider erhalten haben, z. B. *2001:4dd0:f829::* und *48*.
- (10) Bestätigen Sie Ihre Angaben mit **OK**.

Im nächsten Schritt wird die LAN-Schnittstelle konfiguriert und das Subnetz automatisch erzeugt.

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

The screenshot shows the 'Schnittstellen' configuration page. The left sidebar has a menu with 'IP-Konfiguration' selected. The main area is titled 'Schnittstellen' and contains a form for configuring a new interface (VLAN-ID1). The form is divided into several sections:

- Basisparameter:**
 - Basierend auf Ethernet-Schnittstelle:
 - Schnittstellenmodus: Untagged Tagged (VLAN)
 - VLAN-ID:
 - MAC-Adresse: Voreingestellte verwenden
- Grundlegende IPv4-Parameter:**
 - Adressmodus: Statisch DHCP
 - IP-Adresse / Netzmaske:
- Grundlegende IPv6-Parameter:**
 - IPv6: Aktiviert
 - Sicherheitsrichtlinie: Unsicher Sicher
 - Zusätzliche IPv6-Adresskonfiguration: Aktiviert
 - IPv6-Modus: Client Router
 - Rolle bei der Präfixdelegation: Upstream Downstream
 - Router Advertisement übertragen: Aktiviert
 - IPv6-Präfix/Länge:
 - Standardrouter: Aktiviert

At the bottom of the form, there is a section for 'Erweiterte Einstellungen' with 'OK' and 'Abbrechen' buttons.

Abb. 64: LAN -> IP-Konfiguration -> Schnittstellen -> Neu

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie bei **Basierend auf Ethernet-Schnittstelle** die Schnittstelle aus, hier z. B. *en1-0*.
- (2) Bei **IPv6** wählen Sie *Aktiviert* aus.

- (3) Bei **Sicherheitsrichtlinie** belassen Sie die Einstellung *Sicher*. Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.
- (4) Bei **IPv6-Modus** belassen Sie die Einstellung *Router*.
- (5) Bei **Rolle bei der Präfixdelegation** belassen Sie die Einstellung *Downstream*.
- (6) Für **Router Advertisement übertragen** belassen Sie *Aktiviert*. Router Advertisements werden über die gewählte Schnittstelle gesendet.
- (7) Klicken Sie unter **IPv6-Präfix/Länge** auf **Hinzufügen**, um ein Subnetz automatisch erstellen zu lassen.

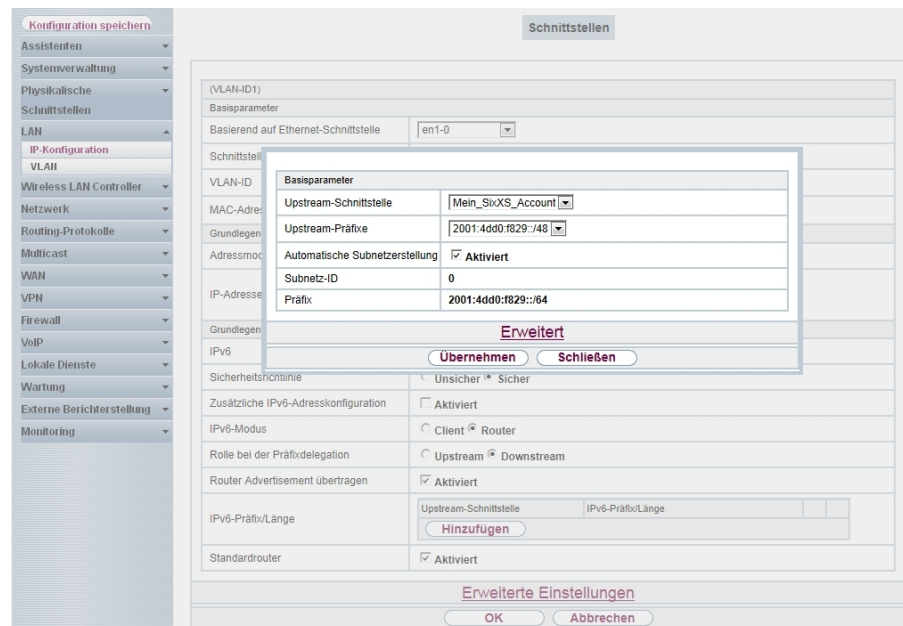


Abb. 65: LAN -> IP-Konfiguration -> Schnittstellen -> Neu -> Hinzufügen

- (8) Bei **Upstream-Schnittstelle** wählen Sie die bereits konfigurierte Schnittstelle aus, hier *Mein_SixXS_Account*.
- (9) Bei **Upstream-Präfix** wählen Sie den angelegten Präfix *2001:4dd0:f829::/48* aus.
- (10) Belassen Sie die Einstellung **Automatische Subnetzerstellung** *Aktiviert*. Die automatisch erzeugte **Subnetz-ID** *0* und der automatisch erzeugte **Präfix** *2001:4dd0:f829::/64* für das Subnetz werden angezeigt.
- (11) Bestätigen Sie Ihre Angaben mit **Übernehmen**.
- (12) Belassen Sie die Einstellung **Standardrouter** *Aktiviert*.
- (13) Bestätigen Sie Ihre Angaben mit **OK**.

8.3 Konfigurationsschritte im Überblick

Schnittstelle konfigurieren und Adressraum zuweisen

Feld	Menü	Wert
Beschreibung	WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu	z. B. <i>Mein_SIXXS_Account</i>
Tunnelmodus	WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>SixXS</i>
Sicherheitsrichtlinie	WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>Unsicher</i>
Über Schnittstelle	WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu	z. B. <i>WAN_SCHNITTSTELLE</i>
Benutzername	WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu	z. B. <i>PCP4-SIXXS</i>
Passwort	WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu	wird bei SixXS vergeben
Tunnel-ID	WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu	wird von SixXS vergeben
Zugewiesener IPv6-Präfix/Länge	WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu -> Hinzufügen	z. B. <i>2001:4dd0:f829::/48</i>

LAN konfigurieren und Subnetz erzeugen lassen

Feld	Menü	Wert
Basierend auf Ether- net-Schnittstelle	LAN-> IP-Konfiguration-> Schnitt- stellen-> Neu	z. B. <i>en1-0</i>
IPv6	LAN-> IP-Konfiguration-> Schnitt- stellen-> Neu	<i>Aktiviert</i>
Sicherheitsrichtlinie	LAN-> IP-Konfiguration-> Schnitt- stellen-> Neu	<i>Sicher</i>
IPv6-Modus	LAN-> IP-Konfiguration-> Schnitt- stellen-> Neu	<i>Router</i>
Rolle bei der Präfixde- legation	LAN-> IP-Konfiguration-> Schnitt- stellen-> Neu	<i>Downstream</i>
Router Advertisement übertragen	LAN-> IP-Konfiguration-> Schnitt- stellen-> Neu	<i>Aktiviert</i>
Upstream-Schnitt- stelle	LAN-> IP-Konfiguration-> Schnitt- stellen-> Neu -> Hinzufügen	<i>Mein_SixXS_Account</i>

Feld	Menü	Wert
Upstream-Präfixe	LAN-> IP-Konfiguration-> Schnittstellen-> Neu -> Hinzufügen	<i>2001:4dd0:f829::/48</i>
Automatische Subnetzerstellung	LAN-> IP-Konfiguration-> Schnittstellen-> Neu -> Hinzufügen	<i>Aktiviert</i>
Standardrouter	LAN-> IP-Konfiguration-> Schnittstellen-> Neu	<i>Aktiviert</i>

Kapitel 9 IP - Tunnel Broker SixXS mit ::/48-Präfix und Verteilung durch einen IPSec-Tunnel

9.1 Einleitung

In diesem Beispiel wird die Vernetzung zwischen der Zentrale und einer Außenstelle beschrieben.

Ziel der Konfiguration ist die Vernetzung von Standorten mit IPv4 im WAN und IPv4/IPv6 im LAN mit einem ::/48-Präfix von SixXS und einem ::/56-Präfix von der Zentrale.

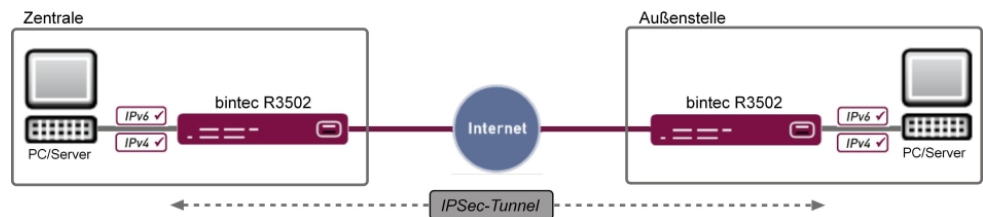


Abb. 66: Beispielszenario

Zentrale

WAN	LAN
WAN-Schnittstelle: Internet Service Provider über DSL	LAN-Schnittstelle: en1-0
IP-Adresse : Dynamische IP-Adresse	IP-Adresse : 192.168.0.254/24
	DHCP-Range: 192.168.0.10 - 192.168.0.39

Außenstelle

WAN	LAN
WAN-Schnittstelle: Internet Service Provider über DSL	LAN-Schnittstelle: en1-0
IP-Adresse : Dynamische IP-Adresse	IP-Adresse : 192.168.80.254/24
	DHCP-Range: 192.168.80.10 - 192.168.80.39

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

Das GUI ist eine web-basierte grafische Benutzeroberfläche, die Sie von jedem PC aus mit

einem aktuellen Web-Browser über eine HTTP- oder HTTPS-Verbindung bedienen können.

Um Ihr Gateway mit dem GUI konfigurieren zu können, müssen Sie über die serielle Schnittstelle, über LAN oder über eine ISDN-Verbindung auf das Gerät zugreifen. Sie müssen einen Web-Browser aufrufen, die IP-Adresse Ihres Geräts in die Adresszeile des Browsers eingeben und sich mit Benutzername sowie Passwort einloggen.

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein bintec Gateway der RS-, der Rxxx2- oder der RXL-Serie z. B. **bintec R3502** mit Systemsoftware 8.2.1
- Eine funktionierende Verbindung zum Internet
- Internet Protocol Version 6 (IPv6) aktiv auf den entsprechenden Rechnern (bei Windows 7 ist IPv6 Standardmäßig aktiviert)
- Grundkonfiguration aller benötigten Schnittstellen
- Zugang sowie einen Netzwerk-Präfix bei einem Tunnel Broker, z. B. bei SixXS
- Ein bestehender IPSec-Tunnel zwischen den beiden Standorten mit virtueller Schnittstelle

9.2 Konfiguration

Konfiguration in der Zentrale

- (1) Gehen Sie zu **WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu**.

Abb. 67: WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu

Gehen Sie folgendermaßen vor, um die Schnittstelle für IPv6 mit SixXS zu konfigurieren und den Präfix einzutragen:

- (1) Geben Sie eine **Beschreibung** für die Schnittstelle ein, z. B. *Mein_SIXXS_Account*.
- (2) Bei **Tunnelmodus** wählen Sie *SixXS* aus. Ein SixXS-Tunnel (SixXS-Konfigurationsprofil für eine 6in4-Tunnel-Konfiguration) wird verwendet.
- (3) Bei **Sicherheitsrichtlinie** belassen Sie die Einstellung *Unsicher*. Es werden nur IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert wurde. Verwenden Sie diese Einstellung, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.
- (4) Bei **Über Schnittstelle** wählen Sie die LAN-Schnittstelle aus, z. B. *LAN_EN1-0*.
- (5) Bei **Benutzername** geben Sie den SixXS-Benutzernamen ein, den Sie von SixXS erhalten haben, z. B. *PCP4-SIXXS*.
- (6) Bei **Passwort** geben Sie das Tunnelpasswort ein, das Sie für Ihren Tunnel bei SixXS konfiguriert haben.
- (7) Bei **Tunnel-ID** geben Sie die Tunnel-ID Ihres SixXS-Tunnels ein, die Ihnen SixXS zugeteilt hat.
- (8) Klicken Sie unter **Zugewiesener IPv6-Präfix/Länge** auf **Hinzufügen**.
- (9) Bei **IPv6-Präfix** und **Länge** geben Sie die Werte ein, die Sie von Ihrem Service Provider erhalten haben, z. B. *2001:4dd0:f829::* und *48*.
- (10) Bestätigen Sie Ihre Angaben mit **OK**.

Im nächsten Schritt wird die LAN-Schnittstelle konfiguriert und das Subnetz automatisch erzeugt.

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

Konfiguration speichern

Assistenten

Systemverwaltung

Physikalische

Schnittstellen

LAN

IP-Konfiguration

VLAN

Wireless LAN Controller

Netzwerk

Routing-Protokolle

Multicast

WAN

VPN

Firewall

VoIP

Lokale Dienste

Wartung

Externe Berichterstattung

Monitoring

Schnittstellen

(VLAN-ID1)

Basisparameter

Basierend auf Ethernet-Schnittstelle: en1-0

Schnittstellenmodus: Untagged Tagged (VLAN)

VLAN-ID: 1

MAC-Adresse: 00:00:00 Voreingestellte verwenden

Grundlegende IPv4-Parameter

Adressmodus: Statisch DHCP

IP-Adresse / Netzmaske:

Grundlegende IPv6-Parameter

IPv6: Aktiviert

Sicherheitsrichtlinie: Unsicher Sicher

Zusätzliche IPv6-Adresskonfiguration: Aktiviert

IPv6-Modus: Client Router

Rolle bei der Präfixdelegation: Upstream Downstream

Router Advertisement übertragen: Aktiviert

IPv6-Präfix/Länge:

Standardrouter: Aktiviert

Erweiterte Einstellungen

Abb. 68: LAN -> IP-Konfiguration -> Schnittstellen -> Neu

- (2) Wählen Sie bei **Basierend auf Ethernet-Schnittstelle** die Schnittstelle aus, hier z. B. *en1-0*.
- (3) Bei **IPv6** wählen Sie *Aktiviert* aus.
- (4) Bei **Sicherheitsrichtlinie** belassen Sie die Einstellung *Sicher*. Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.
- (5) Bei **IPv6-Modus** belassen Sie die Einstellung *Router*.
- (6) Bei **Rolle bei der Präfixdelegation** belassen Sie die Einstellung *Downstream*.
- (7) Für **Router Advertisement übertragen** belassen Sie *Aktiviert*. Router Advertisements werden über die gewählte Schnittstelle gesendet.
- (8) Klicken Sie unter **IPv6-Präfix/Länge** auf **Hinzufügen**, um ein Subnetz automatisch erstellen zu lassen.

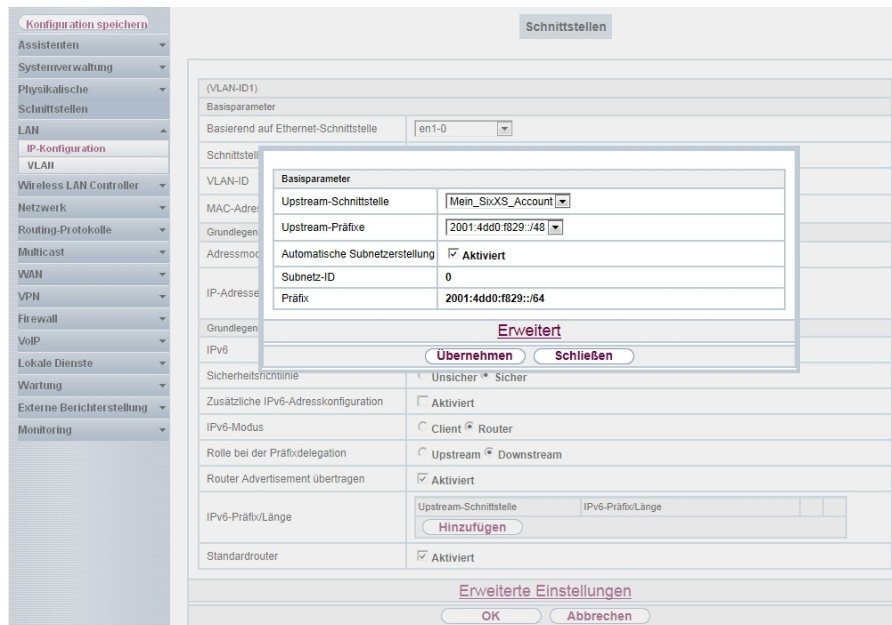


Abb. 69: LAN -> IP-Konfiguration -> Schnittstellen -> Neu -> Hinzufügen

- (9) Bei **Upstream-Schnittstelle** wählen Sie die bereits konfigurierte Schnittstelle aus, hier *Mein_SixXS_Account*.
- (10) Bei **Upstream-Präfixe** wählen Sie den angelegten Präfix *2001:4dd0:f829::/48* aus.
- (11) Belassen Sie die Einstellung **Automatische Subnetzerstellung** *Aktiviert*.
Die automatisch erzeugte **Subnetz-ID** *0* und der automatisch erzeugte **Präfix** *2001:4dd0:f829::/64* für das Subnetz werden angezeigt.
- (12) Bestätigen Sie Ihre Angaben mit **Übernehmen**.
- (13) Belassen Sie die Einstellung **Standardrouter** *Aktiviert*.
- (14) Bestätigen Sie Ihre Angaben mit **OK**.

Im nächsten Schritt wird die Tunnel-Schnittstelle definiert.

- (1) Gehen Sie zu **WAN ->IPv6-Tunnel ->IPv6-Tunnel ->Neu**.

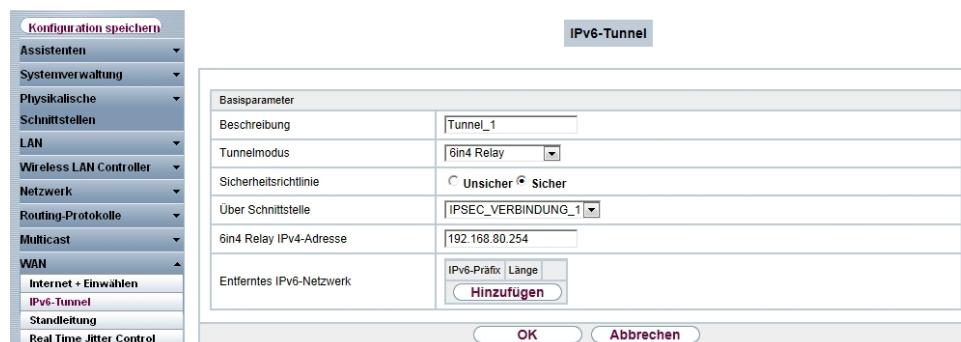


Abb. 70: WAN ->IPv6-Tunnel -> IPv6-Tunnel -> Neu

Gehen Sie folgendermaßen vor, um die Tunnelschnittstelle zu konfigurieren und den Präfix einzutragen:

- (1) Geben Sie eine **Beschreibung** für die Schnittstelle ein, z. B. *Tunnel_1*.
- (2) Bei **Tunnelmodus** wählen Sie *6in4 Relay* aus. Eine 6in4-Tunnel-Konfiguration wird verwendet.
- (3) Bei **Sicherheitsrichtlinie** wählen Sie *Sicher*. Alle IP-Pakete werden durchgelassen.
- (4) Bei **Über Schnittstelle** wählen Sie die IPsec-Schnittstelle aus, z. B. *IP-SEC_VERBINDUNG_1*.
- (5) Bei **6in4Relay IPv4-Adresse** geben Sie die IP-Adresse des Routers in der Außenstelle ein, z. B. *192.168.80.254*.
- (6) Bestätigen Sie Ihre Angaben mit **OK**.

Im letzten Schritt wird eine statische Route für den Präfix in der Außenstelle konfiguriert. Diese Route ist notwendig, damit die Zentrale "weiß", über welche Schnittstelle die IPv6-Pakete der Außenstelle geroutet werden müssen.

Gehen Sie folgendermaßen vor:

- (1) Gehen Sie zu **Netzwerk ->Routen -> IPv6-Routen -> Neu**.

Konfiguration speichern

Assistenten Systemverwaltung Physikalische Schnittstellen LAN Wireless LAN Controller Netzwerk Routen IPv6 Prefixes NAT Lastverteilung QoS Zugriffsregeln Drop-In

IPv4-Routen IPv6-Routen Optionen

Routenparameter

Beschreibung	Route Außenstelle	
Route aktiv	<input checked="" type="checkbox"/> Aktiviert	
Routentyp	Direkt	
Zielschnittstelle	Tunnel_1	
Quelladresse/Länge		/64
Zieladresse/Länge	2001:4dd0:f829:1000::	/56

OK Abbrechen

Abb. 71: Netzwerk -> Routen -> IPv6-Routen -> Neu

- (1) Geben Sie eine **Beschreibung** ein, z. B. *Route Außenstelle*.
- (2) Belassen Sie die Einstellung **Route aktiv** *Aktiviert*.
- (3) Bei **Routentyp** wählen Sie *Direkt*.
- (4) Bei **Zielschnittstelle** wählen Sie die Tunnelschnittstelle aus, hier *Tunnel_1*.
- (5) Bei **Zieladresse/Länge** geben Sie *2001:4dd0:f829:1000::/56* ein.
Durch den Wert *:1000::* in obiger Adresse wird das *::/48* Präfix weiter unterteilt.
Somit "weiß" die Zentrale, dass alle Anfragen aus dem Netz
2001:4dd9:f829:1000::/56 von der Außenstelle kommen.
- (6) Bestätigen Sie Ihre Angaben mit **OK**.

Konfiguration in der Außenstelle

Sie müssen zuerst die Tunnel-Schnittstelle definieren.

- (1) Gehen Sie zu **WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu**.

Konfiguration speichern

Assistenten Systemverwaltung Physikalische Schnittstellen LAN Wireless LAN Controller Netzwerk Routing-Protokolle Multicast WAN Internet + Einwählen IPv6-Tunnel Standleitung Real Time Jitter Control VPN

IPv6-Tunnel

Basisparameter

Beschreibung	Tunnel_1	
Tunnelmodus	6in4 Relay	
Sicherheitsrichtlinie	<input type="radio"/> Unsicher <input checked="" type="radio"/> Sicher	
Über Schnittstelle	IPSEC_VERBINDUNG_1	
6in4 Relay IPv4-Adresse	192.168.0.254	
Entferntes IPv6-Netzwerk	IPv6-Präfix	Länge
	2001:4dd0:f829:1000::	56

Hinzufügen

OK Abbrechen

Abb. 72: WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu

Gehen Sie folgendermaßen vor, um die Tunnel-Schnittstelle zu definieren:

- (1) Bei **Beschreibung** geben Sie z. B. *Tunnel_1* ein.
- (2) Bei **Tunnelmodus** wählen Sie. *6in4 Relay*. Eine Standard-6in4-Tunnel-Schnittstelle wird verwendet.
- (3) Bei **Sicherheitsrichtlinie** wählen Sie *Sicher* aus.
- (4) Wählen Sie bei **Über Schnittstelle** den Namen der Schnittstelle der IPSec-Verbindung, hier z. B. *IPSEC_VERBINDUNG_1*.
- (5) Bei **6in4 Relay IPv4-Adresse** geben Sie die IP-Adresse des Routers in der Zentrale ein, z. B. *192.168.0.254*.
- (6) Klicken Sie bei **Entferntes IPv6-Netzwerk** auf **Hinzufügen** und tragen Sie den Präfix ein, den die Außenstelle von der Zentrale bekommt, z. B. *2001:4dd0:f829:1000::/56*.
- (7) Bestätigen Sie Ihre Angaben mit **OK**.

Im nächsten Schritt wird die LAN-Schnittstelle konfiguriert.

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

The screenshot displays the 'Schnittstellen' configuration window. On the left is a navigation menu with 'IP-Konfiguration' and 'VLAN' selected. The main area shows the configuration for '(VLAN-ID1)'. Under 'Basisparameter', 'Basierend auf Ethernet-Schnittstelle' is set to 'en1-0'. 'Schnittstellenmodus' is 'Tagged (VLAN)'. 'VLAN-ID' is '1'. 'MAC-Adresse' is '00:80:19' with a checkbox for 'Voreingestellte verwenden'. Under 'Grundlegende IPv4-Parameter', 'Adressmodus' is 'Statisch'. 'IP-Adresse / Netzmaske' is '192.168.0.19'. Under 'Grundlegende IPv6-Parameter', 'IPv6' is checked. 'Sicherheitsrichtlinie' is 'Sicher'. 'Zusätzliche IPv6-Adresskonfiguration' is unchecked. 'IPv6-Modus' is 'Router'. 'Rolle bei der Präfixdelegation' is 'Upstream'. 'Router Advertisement übertragen' is checked. 'IPv6-Präfix/Länge' is 'Upstream-Schnittstelle'. At the bottom are 'Erweiterte Einstellungen', 'OK', and 'Abbrechen' buttons.

Abb. 73: LAN -> IP-Konfiguration ->Schnittstellen -> Neu

Gehen Sie folgendermaßen vor, um die LAN-Schnittstelle zu konfigurieren:

- (1) Wählen Sie bei **Basierend auf Ethernet-Schnittstelle** die Schnittstelle aus, hier z. B. *en1-0*.

- (2) Bei **IPv6** wählen Sie *Aktiviert* aus.
- (3) Bei **Sicherheitsrichtlinie** belassen Sie die Einstellung *Sicher*. Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.
- (4) Bei **IPv6-Modus** belassen Sie die Einstellung *Router*.
- (5) Bei **Rolle bei der Präfixdelegation** belassen Sie die Einstellung *Downstream*.
- (6) Für **Router Advertisement übertragen** belassen Sie *Aktiviert*. Router Advertisements werden über die gewählte Schnittstelle gesendet.
- (7) Klicken Sie bei **IPv6-Präfix/Länge** auf **Hinzufügen**.

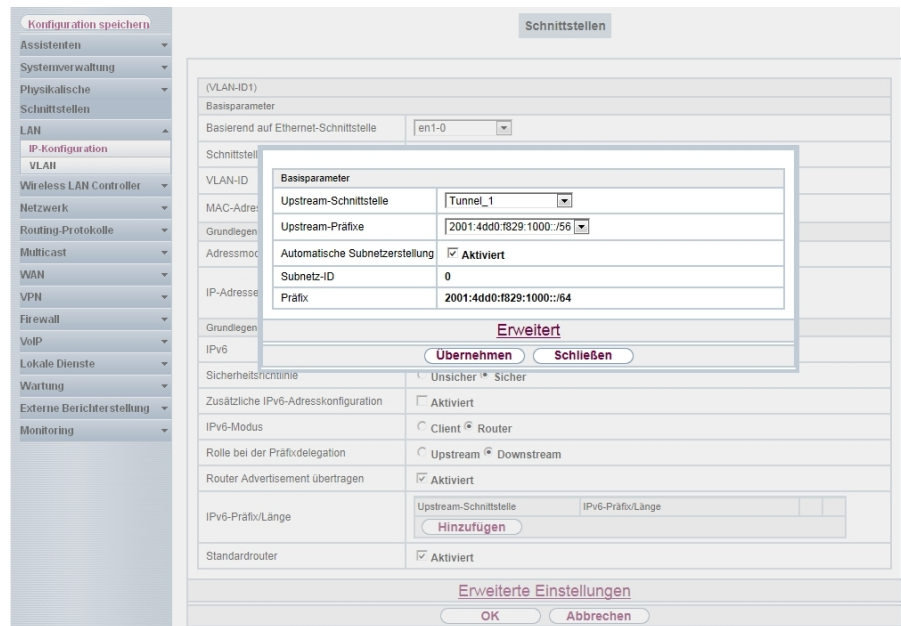


Abb. 74: LAN -> IP-Konfiguration ->Schnittstellen -> Neu -> Hinzufügen

- (8) Bei **Upstream-Schnittstelle** wählen Sie den bereits konfigurierten 6in4 Relay-Tunnel aus, hier *Tunnel_1*.
- (9) Bei **Upstream-Präfixe** wählen Sie den Präfix *2001:4dd0:f829:1000::/56* aus.
- (10) Belassen Sie die Einstellung **Automatische Subnetzerstellung** *Aktiviert*.
Die automatisch erzeugte **Subnetz-ID** *0* und der automatisch erzeugte **Präfix** *2001:4dd0:f829:1000::/64* für das Subnetz werden angezeigt.
- (11) Bestätigen Sie Ihre Angaben mit **Übernehmen**.
- (12) Belassen Sie die Einstellung **Standardrouter** *Aktiviert*.
- (13) Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern.

9.3 Konfigurationsschritte im Überblick

9.3.1 Konfiguration in der Zentrale

Schnittstelle konfigurieren und Adressraum zuweisen

Feld	Menü	Wert
Beschreibung	WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu	z. B. <i>Mein_SIXXS_Account</i>
Tunnelmodus	WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu	<i>SixXS</i>
Sicherheitsrichtlinie	WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu	<i>Unsicher</i>
Über Schnittstelle	WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu	z. B. <i>LAN_EN1-0</i>
Benutzername	WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu	z. B. <i>PCP4-SIXXS</i>
Passwort	WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu	wird bei SixXS vergeben
Tunnel-ID	WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu	wird von SixXS vergeben
Zugewiesener IPv6-Präfix/Länge	WAN ->IPv6-Tunnel ->IPv6-Tunnel -> Neu -> Hinzufügen	z. B. <i>2001:4dd0:f829::/48</i>

LAN konfigurieren und Subnetz erzeugen lassen

Feld	Menü	Wert
Basierend auf Ethernet-Schnittstelle	LAN-> IP-Konfiguration-> Schnittstellen-> Neu	z. B. <i>en1-0</i>
IPv6	LAN-> IP-Konfiguration-> Schnittstellen-> Neu	<i>Aktiviert</i>
Sicherheitsrichtlinie	LAN-> IP-Konfiguration-> Schnittstellen-> Neu	<i>Sicher</i>
IPv6-Modus	LAN-> IP-Konfiguration-> Schnittstellen-> Neu	<i>Router</i>
Rolle bei der Präfixdelegation	LAN-> IP-Konfiguration-> Schnittstellen-> Neu	<i>Downstream</i>
Router Advertisement übertragen	LAN-> IP-Konfiguration-> Schnittstellen-> Neu	<i>Aktiviert</i>

Feld	Menü	Wert
Upstream-Schnittstelle	LAN-> IP-Konfiguration-> Schnittstellen-> Neu -> Hinzufügen	<i>Mein_SixXS_Account</i>
Upstream-Präfixe	LAN-> IP-Konfiguration-> Schnittstellen-> Neu -> Hinzufügen	<i>2001:4dd0:f829::/48</i>
Automatische Subnetzzerstellung	LAN-> IP-Konfiguration-> Schnittstellen-> Neu -> Hinzufügen	<i>Aktiviert</i>

Tunnel-Schnittstelle definieren

Feld	Menü	Wert
Beschreibung	WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>z. B. Tunnel_1</i>
Tunnelmodus	WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>6in4 Relay</i>
Sicherheitsrichtlinie	WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>Sicher</i>
Über Schnittstelle	WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>z. B. IP-SEC_VERBINDUNG_1</i>
6in4Relay IPv4-Adresse	WAN -> IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>z. B. 192.168.80.254</i>

Statische Route anlegen

Feld	Menü	Wert
Beschreibung	Netzwerk-> Routen-> IPv6-Routen-> Neu	<i>Route Außenstelle</i>
Route aktiv	Netzwerk-> Routen-> IPv6-Routen-> Neu	<i>Aktiviert</i>
Routentyp	Netzwerk-> Routen-> IPv6-Routen-> Neu	<i>Direkt</i>
Zielschnittstelle	Netzwerk-> Routen-> IPv6-Routen-> Neu	<i>z. B. Tunnel_1</i>
Zieladresse/Länge	Netzwerk-> Routen-> IPv6-Routen-> Neu	<i>2001:4dd0:f829:1000::/56</i>

9.3.2 Konfiguration in der Außenstelle

Tunnel-Schnittstelle definieren

Feld	Menü	Wert
Beschreibung	WAN-> IPv6-Tunnel -> IPv6-Tunnel -> Neu	z. B. <i>Tunnel_1</i>
Tunnelmodus	WAN-> IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>6in4 Relay</i>
Sicherheitsrichtlinie	WAN-> IPv6-Tunnel -> IPv6-Tunnel -> Neu	<i>Sicher</i>
Über Schnittstelle	WAN-> IPv6-Tunnel -> IPv6-Tunnel -> Neu	z. B. <i>IP-SEC_VERBINDUNG_1</i>
6in4 Relay IPv4-Adresse	WAN-> IPv6-Tunnel -> IPv6-Tunnel -> Neu	z. B. <i>192.168.0.254</i>
Entferntes IPv6-Netzwerk	WAN-> IPv6-Tunnel -> IPv6-Tunnel -> Neu -> Hinzufügen	<i>2001:4dd0:f829:1000::/56</i>

LAN konfigurieren und Subnetz erzeugen lassen

Feld	Menü	Wert
Basierend auf Ethernet-Schnittstelle	LAN -> IP-Konfiguration ->Schnittstellen-> Neu	z. B. <i>en1-0</i>
IPv6	LAN -> IP-Konfiguration ->Schnittstellen-> Neu	<i>Aktiviert</i>
Sicherheitsrichtlinie	LAN -> IP-Konfiguration ->Schnittstellen-> Neu	<i>Sicher</i>
IPv6-Modus	LAN -> IP-Konfiguration ->Schnittstellen-> Neu	<i>Router</i>
Rolle bei der Präfixdelegation	LAN -> IP-Konfiguration ->Schnittstellen-> Neu	<i>Downstream</i>
Router Advertisement übertragen	LAN -> IP-Konfiguration ->Schnittstellen-> Neu	<i>Aktiviert</i>
Upstream-Schnittstelle	LAN -> IP-Konfiguration ->Schnittstellen-> Neu -> Hinzufügen	z. B. <i>Tunnel_1</i>
Upstream-Präfixe	LAN -> IP-Konfiguration ->Schnittstellen-> Neu -> Hinzufügen	<i>2001:4dd0:f829:1000::/56</i>
Automatische Subnet-	LAN -> IP-Konfiguration	<i>Aktiviert</i>

Feld	Menü	Wert
erstellung	Schnittstellen-> Neu -> Hinzufügen	
Standardrouter	LAN -> IP-Konfiguration ->Schnittstellen-> Neu	<i>Aktiviert</i>

Kapitel 10 IP - Lastverteilung von zwei parallel genutzten Internetzugängen

10.1 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.

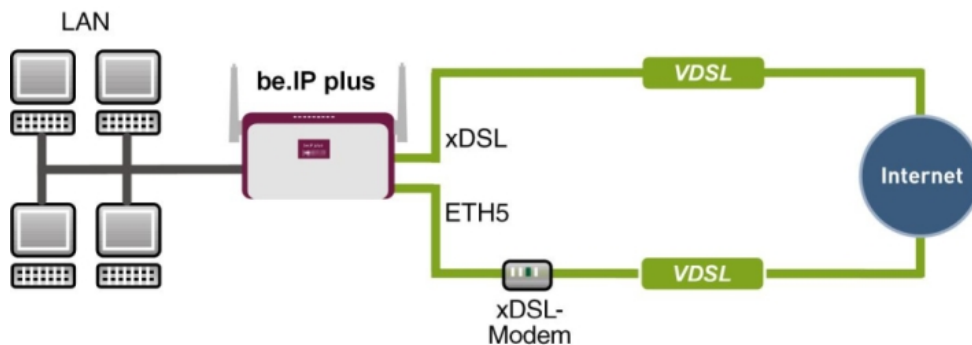


Abb. 75: Beispielszenario

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

10.2 Konfiguration

10.2.1 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.

Abb. 76: **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 ETH5 ▾</p>	<p>Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:</p> <p>Typ Benutzerdefiniert ▾</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 #001@t-online.de</p> <p>Persönliches Kennwort *****</p>

Abb. 77: **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. 78: **Assistenten -> Internet -> Internetverbindungen**

10.2.2 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. 79: **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:

- The first row has "Gruppenbeschreibung" on the left and "Internetzugang" on the right.
- The second row has "Verteilungsrichtlinie" on the left and "Sitzungs-Round-Robin" on the right.

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

- The first row has "Schnittstelle" on the left and a dropdown menu showing "WAN_ADSL-1" on the right.
- The second row has "Verteilungsverhältnis" on the left and a percentage input field showing "50" followed by a "%" symbol on the right.

Abb. 80: 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**.

The screenshot shows two configuration panels. The top panel, titled 'Basisparameter', contains the following fields:

- Gruppenbeschreibung: Internetzugang
- Verteilungsrichtlinie: Sitzungs-Round-Robin
- Verteilungsmodus: Immer Nur aktive Schnittstellen verwenden

The bottom panel, titled 'Schnittstellenauswahl für Verteilung', contains a table with the following data:

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

Below the table is a button labeled 'HINZUFÜGEN'.

Abb. 81: **Netzwerk -> Lastverteilung -> Lastverteilungsgruppen**

10.2.3 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 Aktiviert

Beschreibung
HTTPS

Dienst

Ziel-IP-Adresse/Netzmaske

Quellschnittstelle

Quell-IP-Adresse/Netzmaske

Special Handling Timer
900 Sekunden

Abb. 82: 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.

10.2.4 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. 83: Lokale Dienste -> DNS -> DNS-Server

10.3 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>fes-te_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 11 IP - Lastverteilung von zwei VPN IPSec-Tunneln über separate Internetzugänge

11.1 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.

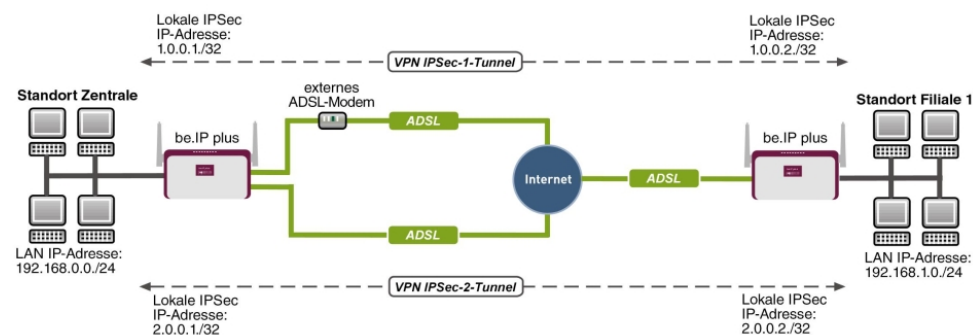


Abb. 84: Beispielszenario

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

11.2 Konfiguration

11.2.1 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.

The screenshot shows a multi-step configuration wizard. The first section, titled 'Grundeinstellungen', has a 'Beschreibung' field containing 'ADSL-1'. The second section asks to 'Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:' and shows a 'Typ' dropdown menu with 'Benutzerdefiniert' selected and a sub-menu showing '(VDSL/ADSL auto - PPPoE (PPP über Ethernet))'. The third section asks 'Wird die Konfiguration eines VLAN vom ISP angefordert (z. B. mit VDSL-Modem):' and has a 'VLAN' toggle switch turned off. The final section asks to 'Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:' and has fields for 'Benutzername' (containing 'ADSL-Benutzername') and 'Persönliches Kennwort' (with a masked password).

Abb. 85: **Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter**

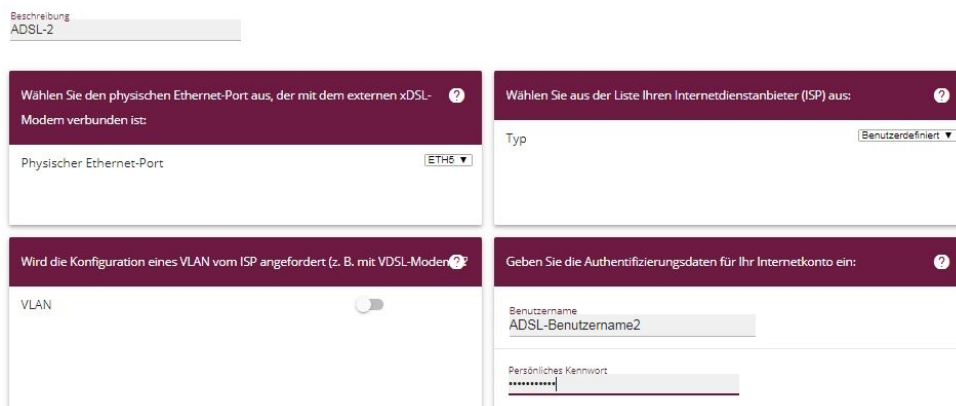
Gehen Sie folgendermaßen vor, um einen Internetzugang zu konfigurieren:

- (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 four-step configuration assistant for an internet connection. Step 1: 'Beschreibung' with the text 'ADSL-2'. Step 2: 'Wählen Sie den physischen Ethernet-Port aus, der mit dem externen xDSL-Modem verbunden ist:' with a dropdown menu showing 'ETH5'. Step 3: 'Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:' with a dropdown menu showing 'Benutzerdefiniert'. Step 4: 'Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:' with fields for 'Benutzername' (ADSL-Benutzername2) and 'Persönliches Kennwort' (test12345).

Abb. 86: **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. 87: 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. 88: 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 'WAN_ADSL-1' and 'Verteilungsverhältnis' set to '50 %'.

Basisparameter	
Gruppenbeschreibung	Internetzugang
Verteilungsrichtlinie	Sitzungs-Round-Robin

Schnittstellenauswahl für Verteilung	
Schnittstelle	WAN_ADSL-1
Verteilungsverhältnis	50 %

Abb. 89: **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. 90: 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. 92: 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 configuration panels. The left panel, titled 'Peer-Parameter', has the following settings: 'Administrativer Status' is set to 'Aktiv'; 'Beschreibung' is 'Filiale1_Peer-2'; 'Peer-Adresse' is empty; 'Peer-ID' is 'Filiale1_Peer-2@bintec-elmeg.com'; 'IKE (Internet Key Exchange)' is 'IKEv1'; 'Pre-shared Key' is masked with asterisks; and 'IP-Version des Tunnelnetzwerks' is 'IPv4'. The right panel, titled 'IPv4-Schnittstellenrouten', has 'Sicherheitsrichtlinie' set to 'Vertrauenswürdig', 'IPv4-Adressvergabe' set to 'Statisch', 'Standardroute' is 'Deaktiviert', and 'Lokale IP-Adresse' is '2.0.0.1'. The 'Routeneinträge' table contains two entries:

Entfernte IP-Adresse	Netzmaske	Metrik
2.0.0.2	255.255.255.255	1
192.168.1.0	255.255.255.0	1

A 'HINZUFÜGEN' button is located at the bottom of the routing table.

Abb. 93: 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. 94: 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. 95: 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.

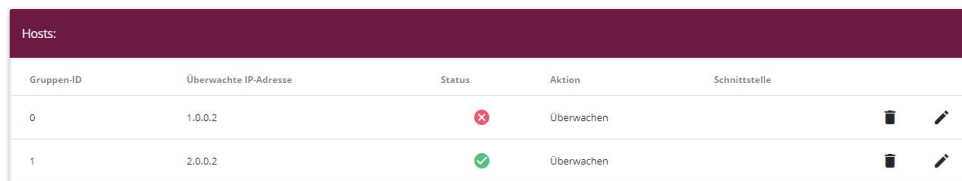
Wählen Sie *Spezifisch* und geben Sie die lokale IP-Adresse der ersten VPN IP-Sec-Schnittstelle an, z. B. *1.0.0.1*.

- (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. 96: 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', contains 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. 97: 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. 98: **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. 99: Netzwerk -> Lastverteilung -> Lastverteilungsgruppen

11.2.2 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:** A form with a 'Beschreibung' field containing the text 'PPPoE1'.
- Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:** A dropdown menu for 'Typ' with the selection 'Benutzerdefiniert' (User-defined) and a sub-option 'VDSL/ADSL auto - PPPoE (PPP über Ethernet)'.
- Wird die Konfiguration eines VLAN vom ISP angefordert (z. B. mit VDSL-Modems)?** A toggle switch for 'VLAN' is currently turned off.
- Geben Sie die Authentifizierungsdaten für Ihr Internetkonto ein:** Fields for 'Benutzername' (containing 'ADSL-Benutzername') and 'Persönliches Kennwort' (masked with dots).
- Wählen Sie den Verbindungsmodus aus:** A toggle switch for 'Immer aktiv' is currently turned on (Aktiviert).
- Geben Sie die vom Internetdiensteanbieter (ISP) definierten ATM-Einstellungen ein:** Two input fields: 'Virtual Path Identifier (VPI)' with the value '1' and 'Virtual Channel Identifier (VCI)' with the value '32'.

Abb. 100: **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. 101: 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 Sekunden 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. 102: 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. 103: **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. 105: **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**.

The screenshot shows two configuration panels. The left panel, titled "Peer-Parameter", includes fields for "Administrativer Status" (set to "Aktiv"), "Beschreibung" (Zentrale_Peer-2), "Peer-Adresse" (62.146.53.201), "Peer-ID" (central@bintec-elmeg.com), "IKE (Internet Key Exchange)" (IKEv1), "Preshared Key" (masked), and "IP-Version des Tunnelnetzwerks" (IPv4). The right panel, titled "IPv4-Schnittstellenrouten", includes "Sicherheitsrichtlinie" (set to "Vertrauenswürdig"), "IPv4-Adressvergabe" (Statisch), "Standardroute" (Deaktiviert), "Lokale IP-Adresse" (2.0.0.2), and a table of "Routeneinträge".

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

The "Erweiterte IPSec-Optionen" panel contains the following settings: "Phase-1-Profil" (Filiale1_Peer2), "Phase-2-Profil" (* Multi-Proposal), "XAUTH-Profil" (Eines auswählen), "Anzahl erlaubter Verbindungen" (Ein Benutzer), "Startmodus" (Immer aktiv), and "Backup Peer" (Keiner).

Abb. 107: 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. 108: 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. 109: **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

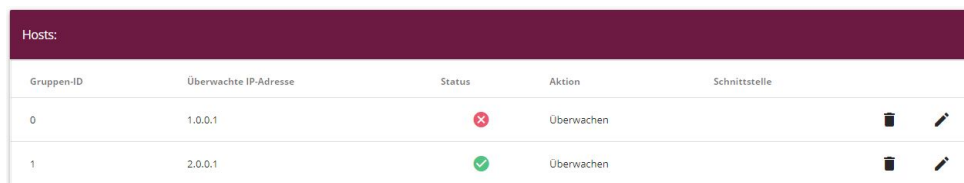
wurde so dass das Gateway der Filiale wieder über diesen Weg antworten kann.
Wählen Sie *Spezifisch* und geben Sie die lokale IP-Adresse der ersten VPN IP-Sec-Schnittstelle an, z. B. *1.0.0.2*.

- (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. 110: **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. 111: **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. 112: **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. 113: Netzwerk -> Lastverteilung -> Lastverteilungsgruppen

11.3 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>
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>2.0.0.1</i>
Routeneinträge	VPN -> IPSec -> IPSec-Peers -> Neu	<i>2.0.0.2/ 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>
Lokaler ID-Typ	VPN -> IPSec -> Phase-1-Profile -> <Multi-Proposal> 	<i>E-Mail-Adresse</i>
Lokaler ID-Wert	VPN -> IPSec -> Phase-1-Profile -> <Multi-Proposal> 	z. B. <i>cen- tral@bintec-elmeg. com</i>

Überwachungsaufgaben einzurichten

Feld	Menü	Wert
Überwachte IP-Adresse	Lokale Dienste -> Überwachung -> Hosts -> Neu	<i>Spezifisch/ z. B. 1.0.0.2</i>
Quell-IP-Adresse	Lokale Dienste -> Überwachung -> Hosts -> Neu	<i>Spezifisch/ z. B. 1.0.0.1</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>
Auszuführende Ak-	Lokale Dienste -> Überwachung ->	<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>cen- tral@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
	weiterte Einstellungen	
IP-Adresse zur Nachverfolgung	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Hinzufügen	z. B. <i>2.0.0.1</i>

Kapitel 12 IP - Mit Drop In eine Filiale durch einen VPN-Tunnel mit der Zentrale verbinden

12.1 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.

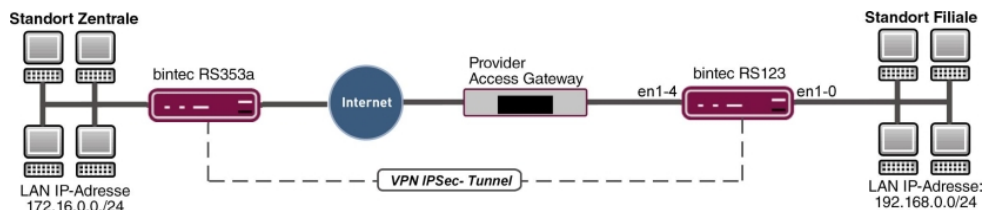


Abb. 114: Beispielszenario

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**

12.2 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	
LAN_EN1-0 ▼	
LAN_EN1-4 ▼	

Abb. 115: 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. *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. It is divided into two main sections: 'Basisparameter' (Basic parameters) and 'Routenparameter' (Route parameters). In the 'Basisparameter' section, 'Routentyp' (Route type) is set to 'Standardroute über Gateway', 'Schnittstelle' (Interface) is set to 'LAN_EN1-4', and 'Routenklasse' (Route class) has 'Standard' selected with a radio button. In the 'Routenparameter' section, 'Gateway-IP-Adresse' (Gateway IP address) is set to '192.168.0.1' and 'Metrik' (Metric) is set to '1'.

Abb. 116: **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
Entfernte IPsec ID Zentrale	255.255.255.0
Preshared Key *****	
IP-Version des Tunnelnetzwerks IPv4	
Lokale IP-Adresse 192.168.0.254	
Diese Verbindung als Standardroute definieren <input type="checkbox"/> Deaktiviert	

Abb. 117: **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. 118: **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**.

12.3 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 13 IP - Einrichtung einer DMZ mit der Funktionalität der Drop-In-Gruppe

13.1 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 plziert. 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.

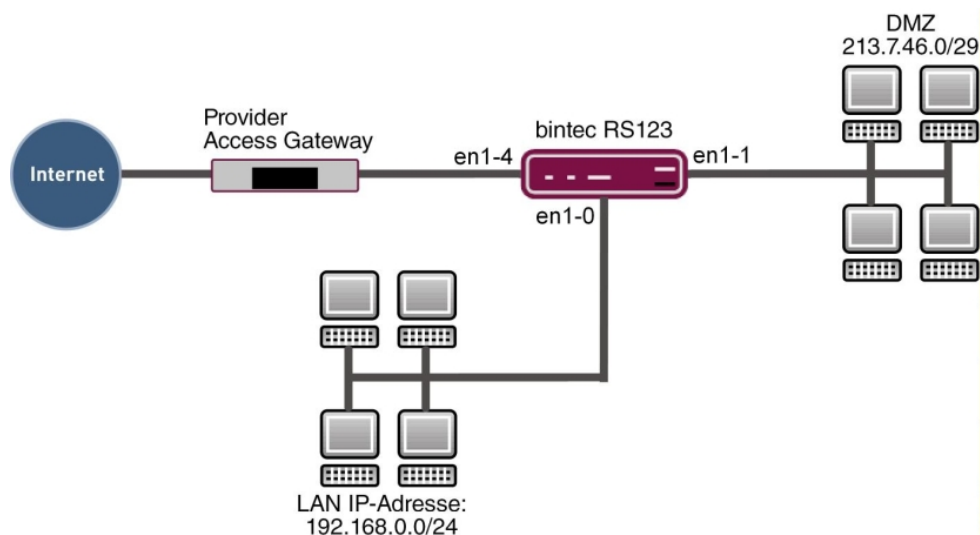


Abb. 119: Beispielszenario

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.

13.2 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.

13.2.1 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 <input type="button" value="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. 120: **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**.

13.2.2 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	
LAN_EN1-4 ▾	
LAN_EN1-1 ▾	

Abb. 121: **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**.

13.2.3 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: 'Basisparameter' (Basic parameters) and 'Routenparameter' (Route parameters).

- Basisparameter:**
 - Routentyp:** A dropdown menu set to 'Standardroute über Gateway'.
 - Schnittstelle:** A dropdown menu set to 'LAN_EN1-4'.
 - Routenklasse:** Two radio buttons: 'Standard' (selected) and 'Erweitert'.
- Routenparameter:**
 - Gateway-IP-Adresse:** A text input field containing '213.7.46.1'.
 - Metrik:** A dropdown menu set to '1'.

Abb. 122: **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**.

13.2.4 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. 123: **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**.

13.2.5 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'. It contains the following fields and controls:

- Beschreibung:** A text input field containing 'WebServer'.
- IPv4:** A toggle switch that is turned on, labeled 'Aktiviert'.
- Adresstyp:** Two radio buttons. The first is selected and labeled 'Adresse/Subnetz'. The second is unselected and labeled '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. 124: **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**.

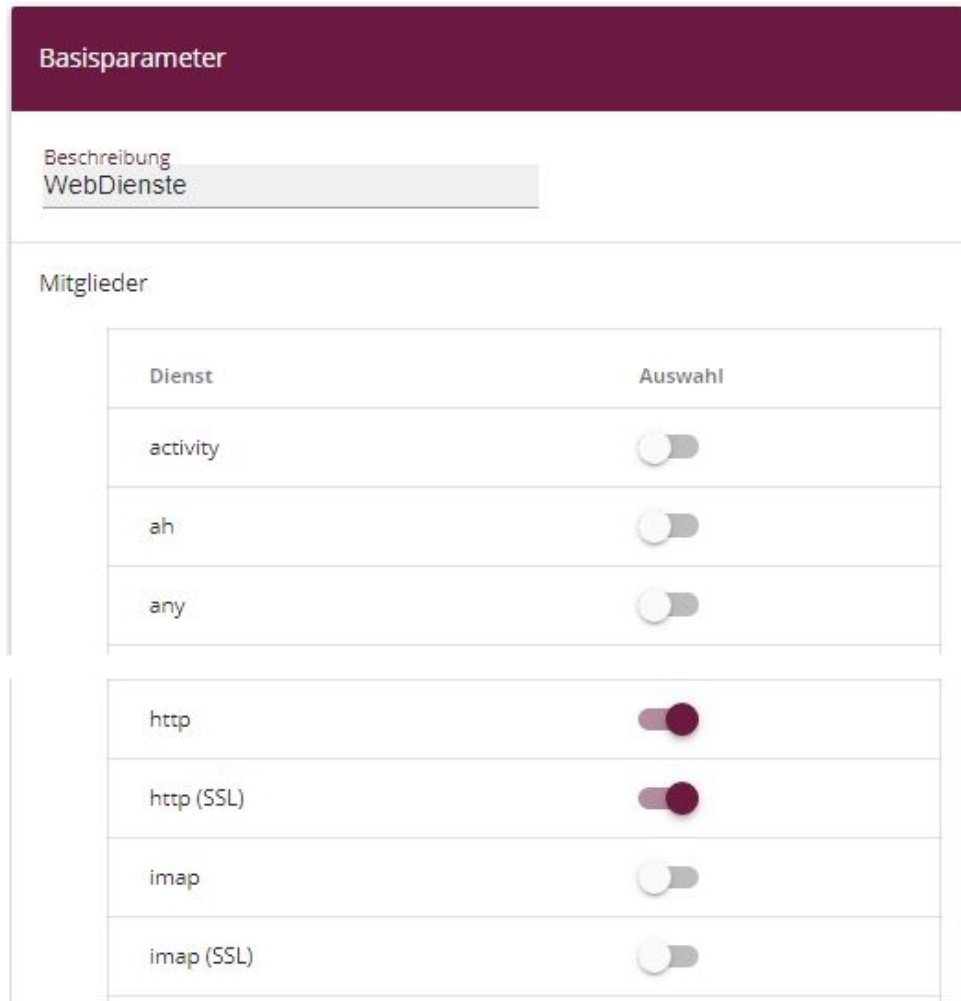


Abb. 125: Firewall -> Dienste -> Gruppen -> Neu

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. 126: **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. 127: Firewall -> Richtlinien -> IPv4- Filterregeln

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

13.3 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 14 IP - DSL-Backup über LTE (bintec 4e-LE)

14.1 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**.

14.2 Router konfigurieren

14.2.1 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"/>	🗑️

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

14.2.2 DHCP-Server für bintec 4Ge-LE einrichten

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

The screenshot shows the 'Basisparameter' section of the DHCP-Server configuration. It includes the following fields:

- IP-Poolname:** bintec 4GE-LE
- IP-Adressbereich:** 192.168.43.42 - 192.168.43.42
- DNS-Server:** Primär (empty) and Sekundär (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 the 'Basisparameter' section of the DHCP-Server configuration. It includes the following fields:

- Schnittstelle:** en1-4
- IP-Poolname:** bintec 4GE-LE
- Pool-Verwendung:** Lokal
- Beschreibung:** 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**.

14.2.3 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	-	✘	^ v	
efm35-50	Nicht konfiguriert/Nicht konfiguriert	-	✘	^ v	
ethoa35-5	Nicht konfiguriert/Nicht konfiguriert	-	✘	^ v	
br0	192.168.0.100/255.255.255.0	Präfix: Germany - Telekom Entertain:0 Host: eui64	✔	^ v	
ethoa35-5-1(VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✘	^ v	
efm35-50-1(VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✘	^ v	
en1-4-1 (VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✘	^ v	

14.2.4 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	-	✘	^	v	✎ 🔍
efm35-60	Nicht konfiguriert/Nicht konfiguriert	-	✘	^	v	✎ 🔍
ethoa35-5	Nicht konfiguriert/Nicht konfiguriert	-	✘	^	v	✎ 🔍
br0	192.168.0.100/255.255.255.0	Prefix: Germany - Telekom Enterstain0 Host: eu164	✔	^	v	✎ 🔍
ethoa35-5-1(VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✘	^	v	🗑️ ✎ 🔍
efm35-60-1(VLAN-ID8)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✘	^	v	🗑️ ✎ 🔍
en1-4-1 (VLAN-ID463)	Nicht konfiguriert/Nicht konfiguriert (DHCP)	-	✘	^	v	🗑️ ✎ 🔍

14.2.4.1 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**.

14.2.5 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**.

14.3 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**


Abb. 140: **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!

14.4 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	
Schnittstelle	VoIP ->Einstellungen ->Standorte ->Neu	z. B. <i>WAN_GERMANY - TELEKOM ENTERTAIN</i>
Standort	VoIP ->Einstellungen ->SIP-Provider  Erweiterte Einstellungen	<i>SIP-Account-Bindung-WAN-Interface</i>