Benutzerhandbuch Workshops (Auszug)

Sicherheits- und Administrations-Workshops

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.

Inhaltsverzeichnis

Kapitel 1 Sicherheit - IPSec VPN mit Callback

1.1 Einleitung

Im Folgenden wird die Konfiguration eines IPSec VPN mit Callback (IP-Adresse im B-/D-Kanal) mit einem **bintec RS232bw** beschrieben.

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

Die Filiale eines Unternehmens soll über einen IPSec-Tunnel mit der Zentrale verbunden werden. Für die Internetverbindung steht sowohl in der Filiale als auch in der Zentrale ein xDSL-Anschluss zur Verfügung. Beide Geräte erhalten ihre IP-Adresse dynamisch vom Internet Service Provider (ISP). Um den IPSec-Tunnel in beide Richtungen aufbauen zu können, soll die dynamische IP-Adresse über ISDN zum Partner übertragen werden.

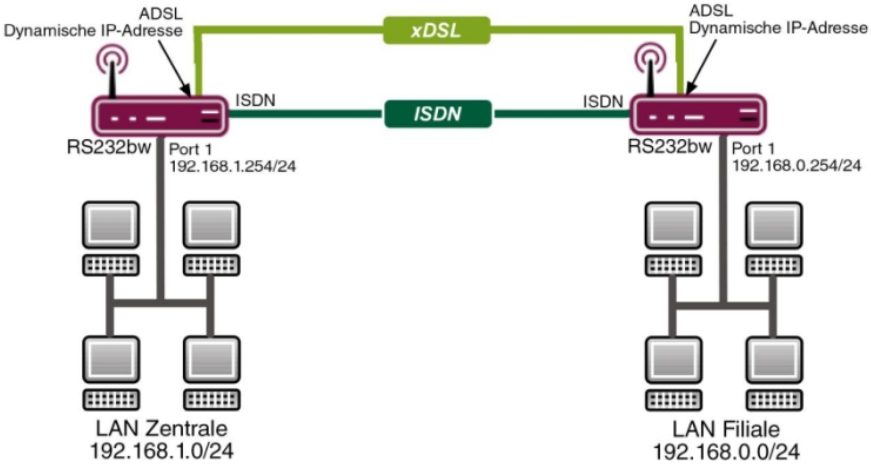


Abb. 1: Beispielszenario IPSec mit Callback

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Zwei **bintec RS232bw** Gateways
- Ein Bootimage der Version 7.10.1

- Ein xDSL-Internetzugang sowohl in der Zentrale als auch in der Filiale
- Ein ISDN-Anschluss sowohl in der Zentrale als auch in der Filiale
- Das LAN muss jeweils mit einem der Ports **1** bis **4** des Gateways verbunden sein

1.2 Konfiguration der Lizenz

Für die Übermittlung der IP-Adresse im B-/D-Kanal benötigen Sie eine zusätzliche Lizenz. Diese können Sie kostenlos unter *www.bintec-elmeg.com* (Bereich **Services** -> **Online Services**) anfordern.

Nachdem Sie die Lizenzdaten erhalten haben, gehen Sie folgendermaßen vor:

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

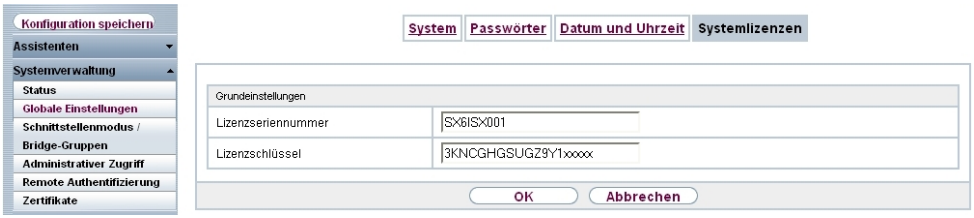


Abb. 2: **Systemverwaltung** -> **Globale Einstellungen** -> **Systemlizenzen** -> **Neu**

Relevante Felder im Menü Systemlizenzen

Feld	Bedeutung
Lizenzseriennummer	Dies ist die Seriennummer der Lizenz.
Lizenzschlüssel	Dies ist der Lizenzschlüssel.

Gehen Sie folgendermaßen vor, um die neue Lizenz einzutragen:

(1) Klicken Sie auf **Neu**, um eine Lizenz hinzuzufügen.

(2) Tragen Sie bei **Lizenzseriennummer** die Seriennummer Ihrer Lizenz ein.

(3) Tragen Sie bei **Lizenzschlüssel** Ihren Lizenzschlüssel ein.

(4) Bestätigen Sie mit **OK**.

Prüfen Sie, ob die Lizenz wie folgt korrekt aktiviert wurde:

Abb. 3: **Systemverwaltung** -> **Globale Einstellungen** -> **Systemlizenzen**

1.3 Konfiguration der ISDN-Schnittstellen

Sie müssen eine Ihrer Multiplen Subscriber Numbers (MSN) so konfigurieren, dass sie bei eingehenden Anrufen für IPSec-Callback verwendet wird.

Gehen Sie in folgendes Menü, um in der Zentrale eine MSN für IPSec-Callback zu konfigurieren:

(1) Gehen Sie zu **Physikalische Schnittstellen** -> **ISDN-Ports** -> **MSN-Konfiguration** -> **Neu**.

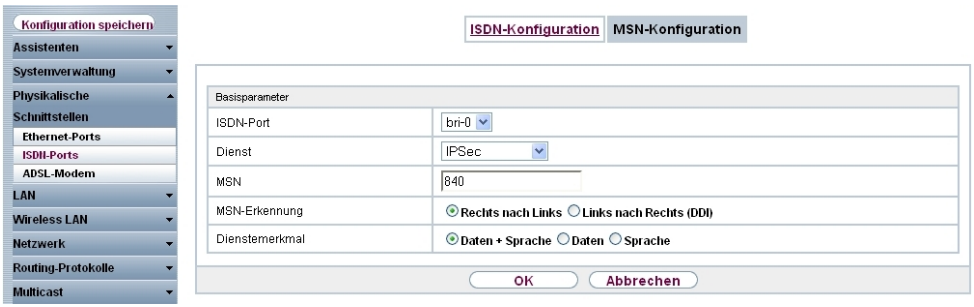


Abb. 4: **Physikalische Schnittstellen** -> **ISDN-Ports** -> **MSN-Konfiguration** -> **Neu**

Relevante Felder im Menü MSN-Konfiguration

Feld	Bedeutung
ISDN-Port	Gibt den Port an, an dem die ISDN-Verbindung angeschlossen ist.
Dienst	Definiert den Dienst, mit dem auf die MSN reagiert wird.
MSN	Dies ist die Rufnummer des Dienstes.
MSN-Erkennung	Definiert die Art der Rufnummernüberprüfung.
Dienstemerkmal	Definiert, ob auf einen Sprachanruf, einen Datenanruf oder auf

Feld	Bedeutung
	beide reagiert wird.

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **ISDN-Port** *bri-0*.

(2) Wählen Sie bei **Dienst** *IPSec*.

(3) Tragen Sie bei **MSN** die MSN ein, auf die das Gateway mit einem IPSec-Callback reagieren soll, hier *840*.

(4) Belassen Sie bei **MSN-Erkennung** *Rechts nach Links*.

(5) Belassen Sie bei **Dienstemerkmal** *Daten + Sprache*.

(6) Bestätigen Sie mit **OK**.

Konfigurieren Sie analog dazu eine MSN auf dem Gateway in der Filiale.

Hinweis

Sollte sich Ihr Gateway an einem Punkt-zu-Punkt ISDN-Anschluss befinden, ist es eventuell erforderlich, bei **MSN-Erkennung** *Links nach Rechts (DDI)* zu wählen.

1.4 Konfiguration der Internetzugänge

Für die beiden Internetverbindungen über xDSL wird auf jedem Gateway jeweils ein Eintrag angelegt. Die anschließende Konfiguration bezieht sich auf den Eintrag für die Internetverbindung in der Zentrale.

Gehen Sie in folgendes Menü, um einen Internetzugang über xDSL in der Zentrale einzurichten:

(1) Gehen Sie zu **WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**.

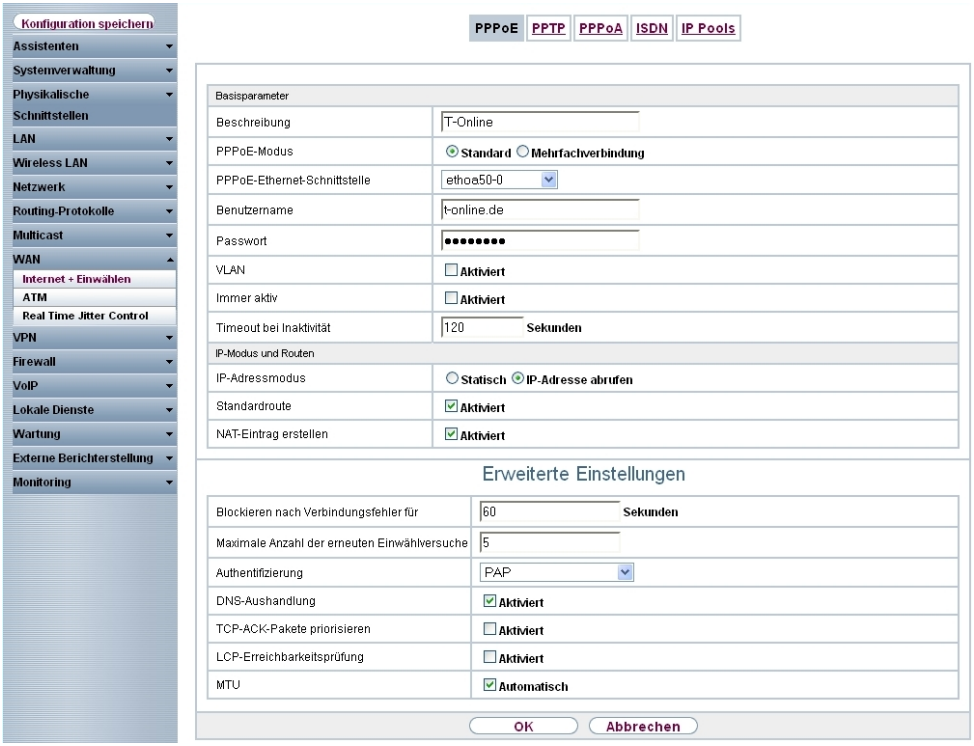


Abb. 5: **WAN -> Internet + Einwählen -> PPPoE -> Neu**

Relevante Felder im Menü PPPoE

Feld	Bedeutung
Beschreibung	Hier definieren Sie einen Namen für die xDSL-Internetverbindung.
PPPoE-Ethernet-Schnittstelle	Legen Sie die Schnittstelle Ihres Gateways fest, über die die xDSLVerbindung aufgebaut werden soll.
Benutzername	Geben Sie Ihren Benutzername ein, den Sie vom Provider erhalten haben.
Passwort	Geben Sie Ihr Passwort ein, das Sie vom Provider erhalten haben.
Immer aktiv (Flatrate-Modus)	Hier wird festgelegt, dass das Gateway die Verbindung nicht automatisch abbaut.
Timeout bei Inaktivität	Definieren Sie die Zeit in Sekunden, nach der das Gateway die Verbindung abbaut, wenn keine Daten mehr fließen.
IP-Adressmodus	Definiert den Modus, nach dem das Gateway die IP-Adresse erhält.

Feld	Bedeutung
Standardroute	Für diese Verbindung wird automatisch eine Standardroute angelegt.
NAT-Eintrag erstellen	NAT wird für diese Verbindung aktiviert.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Beschreibung** die Bezeichnung für die Verbindung ein, z. B. *T-Online*.

(2) Wählen Sie bei **PPPoE-Ethernet-Schnittstelle** *ethoa50-0* aus.

(3) Tragen Sie bei **Benutzername** Ihren in den Zugangsdaten Ihres Providers definierten Benutzernamen ein.

(4) Tragen Sie bei **Passwort** das Passwort für Ihren Internetzugang ein.

(5) Belassen Sie die Standard-Einstellung *Nicht aktiviert* bei **Immer aktiv (Flatrate-Modus)**, falls Sie keinen DSL-Anschluss mit Flatrate haben. Bei einem Internetzugang ohne Flatrate tragen Sie bei **Timeout bei Inaktivität** die Zeit in Sekunden ein, nach der das Gateway die Internetverbindung trennen soll, falls keine Daten mehr fließen, z. B. *120*.

Sollten Sie einen Internetzugang mit Flatrate haben, setzen Sie einen Haken bei **Immer aktiv (Flatrate-Modus)**. Dadurch baut das Gateway die Internetverbindung niemals von sich aus ab.

(6) Belassen Sie bei **IP-Adressmodus** *IP-Adresse abrufen* aus.

(7) Belassen Sie den Haken bei **Standardroute**.

(8) Setzen Sie einen Haken bei **NAT-Eintrag erstellen** .

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

Konfigurieren Sie analog dazu eine Internetverbindung auf dem Gateway in der Filiale.

1.5 Konfiguration von IPSec

Im Folgenden wir die Konfiguration eines IPSec-Peers mit Callback und die Anpassung der Standardprofile für die Phase-1 und die Phase-2 erklärt.

1.5.1 Konfiguration des IPSec-Peers und des Callbacks

Ein IPSec-Peer bezeichnet immer eine Gegenstelle, also hier die Filiale.

Gehen Sie folgendermaßen vor, um einen IPSec-Peer anzulegen.

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

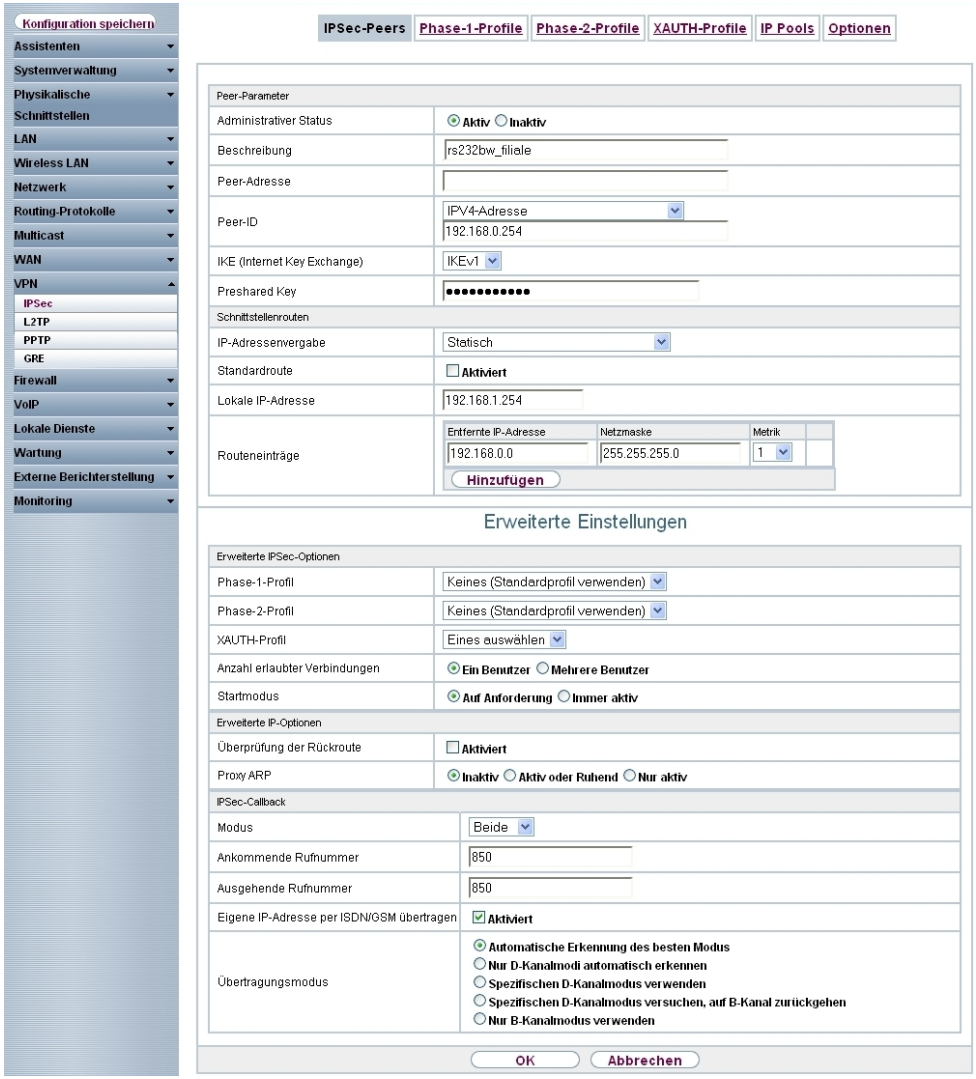


Abb. 6: **VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**

Relevante Felder im Menü IPSec-Peers

Feld	Bedeutung
Beschreibung	Hier definieren Sie einen Namen für den IPSec-Peer.
Peer-ID	Wählen Sie die Art der Identität und geben Sie die Identität des Peers ein.
Preshared Key	Dies ist der geheime Schlüssel für die IPSec-Aushandlung.
Standardroute	Wählen Sie aus, ob die Route zu diesem IPSec Peer als Standard- Route festgelegt wird.

Feld	Bedeutung
Lokale IP-Adresse	Geben Sie die WAN IP-Adresse Ihres Geräts ein.
Routeneinträge: Entfernte IP-Adresse/Netzmaske	Hier geben sie die Netzwerke an, die über diesen IPSec-Tunnel erreicht werden sollen.

Gehen Sie folgendermaßen vor, um einen IPSec-Peer anzulegen:

(1) Tragen Sie bei **Beschreibung** eine Beschreibung des Peers ein, z. B. *rs232bw_filiale*.

(2) Lassen Sie **Peer-Adresse** leer, da die IP-Adresse des Peer dynamisch vom Provider zugewiesen wird.

(3) Wählen Sie bei **Peer-ID** *IPV4-Adresse* und tragen Sie die ID der Gegenstelle ein, hier *192.168.0.254*.

(4) Tragen Sie bei **Preshared Key** den Preshared Key ein, z. B. *geheim123*.

(5) Deaktivieren Sie den Haken bei **Standardroute**.

(6) Geben Sie bei **Lokale IP-Adresse** die IP-Adresse Ihres Geräts ein, z. B. *192.168.1.254*.

(7) Tragen Sie bei **Routeneinträge** für **IP-Adresse** und **Netzmaske** die IP-Adresse und die zugehörige Subnetzmaske des Netzwerks ein, dass Sie über den Tunnel erreichen möchten, hier *192.168.0.0* und *255.255.255.0*.

Für die Peer-Konfiguration sind weitere Einstellungen nötig. Gehen Sie dazu in folgendes Menü:

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

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Bedeutung
Modus	Wählen Sie hier die Art des IPSec Callbacks.
Eingehende ISDN-Nummer	Gibt die Rufnummer an, die ankommt, wenn der Peer den Callback initiiert.
Ausgehende ISDN-Nummer	Gibt die Rufnummer an, die gewählt wird, wenn das Gateway einen Callback initiiert.
Eigene IP-Adresse per ISDN übertragen	Bestimmt, ob die IP-Adresse des Gateways über ISDN übertragen werden soll oder nicht.
Übertragungsmodus	Wählen Sie die Art der Übertragung der IP-Adresse.

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Modus** *Beide*.

(2) Tragen Sie bei **Eingehende ISDN-Nummer** die MSN ein, von der aus ein Callback

angefordert wird, hier *850*.

(3) Tragen Sie bei **Ausgehende ISDN-Nummer** die MSN ein, die für einen Callback angerufen werden soll, hier *850*.

(4) Setzen Sie einen Haken bei **Eigene IP-Adresse per ISDN übertragen**.

(5) Belassen Sie bei **Übertragungsmodus** *Automatische Erkennung des besten Modus*.

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

Klicken Sie auf **Konfiguration speichern** und bestätigen Sie anschließend mit **OK**.

Konfigurieren Sie analog zu dieser Beschreibung IPSec für das Gateway in der Filiale. Beachten Sie dabei, dass IDs, IP-Adressen und MSN richtig konfiguriert sind.

Hinweis

Der Preshared Key ist hier bewusst sehr einfach gehalten und nur für einen Testaufbau gedacht. Im Produktivbetrieb sollten Sie einen Key verwenden, der mindestens 30 Zeichen, keine zusammenhängenden Wörter und am besten Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen enthält.

Durch das anlegen eines IPSec-Peers werden automatisch Standardprofile für Phase 1 und Phase 2 erstellt, die im Folgenden auf die Anforderungen dieses Szenarios angepasst werden.

1.5.2 Anpassen des Phase-1-Profils

Gehen Sie in folgendes Menü, um das Profil für die Phase 1 anzupassen:

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

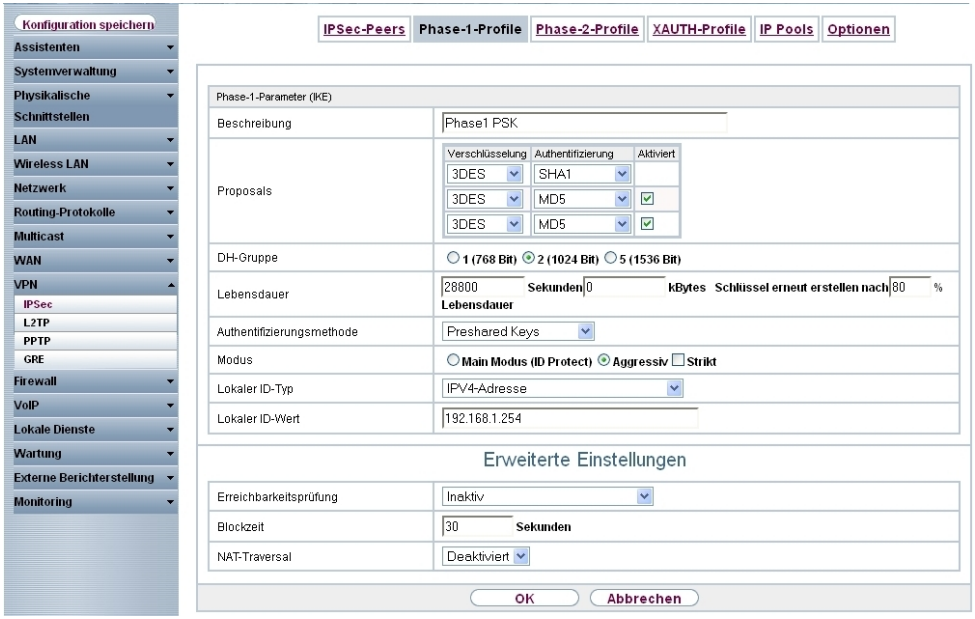


Abb. 7: **VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->

Relevante Felder im Menü Phase-1-Profile

Feld	Bedeutung
Beschreibung	Hier definieren Sie einen Namen für das Profil.
Proposal	Legt die zu verwendenden Verschlüsselungs- und Authentifizierungsalgorithmus fest.
DH-Gruppe	Legt die zu verwendende Diffie-Hellman Gruppe.
Lebensdauer	Bestimmt die Zeit bzw. das Datenvolumen, nach der eine Reauthentifizierung erfolgt.
Authentifizierungsmethode	Wählen Sie die Authentifizierungsmethode.
Modus	Bestimmt die Art der Tunnelaushandlung.
Lokaler ID-Typ	Definiert die Art der lokalen ID des Gateways.
Lokaler ID-Wert	Dies ist die lokale ID des Gateways.

Gehen Sie folgendermaßen vor, um das Profil für die Phase 1 anzupassen:

(1) Tragen Sie bei **Beschreibung** den Namen des Profils ein, z. B. `Phase1 PSK`.

(2) Wählen Sie bei **Proposals Verschlüsselung** `3DES`, bei **Authentifizierung** `SHA1` im ersten Eintrag. Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.

(3) Belassen Sie bei **DH-Gruppe** *2(1024 Bit)*.

(4) Tragen Sie bei **Lebensdauer Sekunden** eine Zeit in Sekunden ein, hier *28800*, und belassen Sie KBytes bei *0*.

(5) Belassen Sie bei **Authentifizierungsmethode** *Preshared Keys*.

(6) Belassen Sie bei **Modus** *Aggressiv*.

(7) Wählen Sie bei **Lokaler ID-Typ** *IPV4-Adresse*.

(8) Tragen Sie bei **Lokaler ID-Wert** die ID ein, hier *192.168.1.254*.

Für die Phase-1-Konfiguration sind erweiterte Einstellungen nötig. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Phase-1-Profile** -> **<Multi-Proposal>** ->  -> **Erweiterte Einstellungen**.

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Bedeutung
Erreichbarkeitsprüfung	Definiert die Art der Phasenüberwachung.
NAT-Traversal	Bestimmt, ob NAT-Traversal verwendet wird oder nicht.

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Erreichbarkeitsprüfung** *Inaktiv*.

(2) Entfernen Sie den Haken bei **NAT-Traversal** .

(3) Bestätigen Sie mit **OK**.

Konfigurieren Sie analog zu dieser Beschreibung die Phase 1 für das Gateway in der Filiale.

1.5.3 Anpassen des Phase-2-Profils

Gehen Sie in folgendes Menü, um das Profil für die Phase 2 anzupassen:

(1) Gehen Sie zu **VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** ->  .

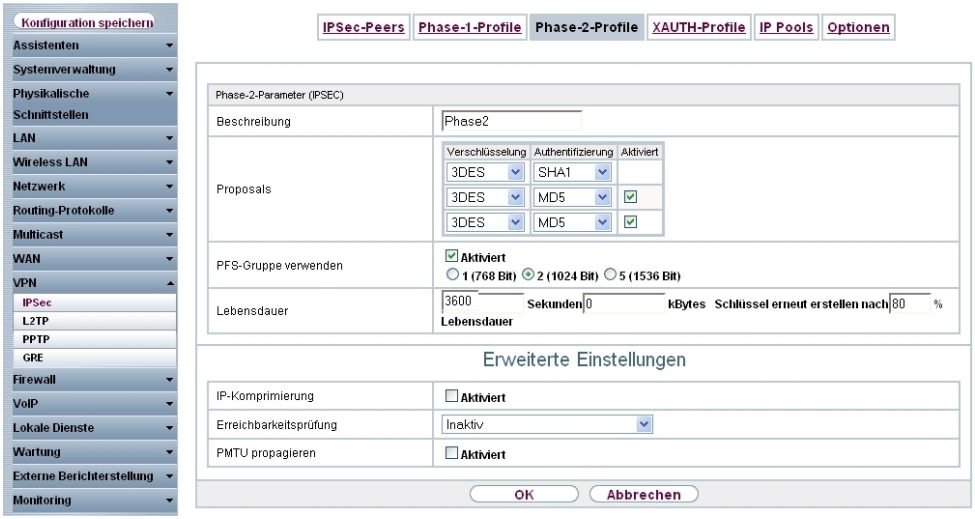


Abb. 8: **VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** ->

Relevante Felder im Menü Phase-2-Profile

Feld	Bedeutung
Beschreibung	Hier definieren Sie einen Namen für das Profil.
Proposal	Legt die zu verwendenden Verschlüsselungs- und Authentifizierungsalgorithmus fest.
PFS-Gruppe verwenden	Bestimmt, ob PFS (Perfect Forwarding Secrecy) verwendet wird.
Lebensdauer	Bestimmt die Zeit bzw. das Datenvolumen, nach der eine Reauthentifizierung erfolgt.

Gehen Sie folgendermaßen vor, um das Profil für die Phase 2 anzupassen:

(1) Tragen Sie bei **Beschreibung** den Namen des Profils ein, z. B. `Phase2`.

(2) Wählen Sie bei **Proposals Verschlüsselung** `3DES`, bei **Authentifizierung** `SHA1` im ersten Eintrag. Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.

(3) Setzen Sie einen Haken bei **PFS-Gruppe verwenden**.

(4) Tragen Sie bei **Lebensdauer Sekunden** die Zeit in Sekunden ein, hier `3600`, und belassen Sie KBytes bei `0`.

Für die Phase-2-Konfiguration sind erweiterte Einstellungen nötig. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Phase-2-Profile** -> **<Multi-Proposal>** -> -> **Erweiterte Einstellungen**.

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Bedeutung
Erreichbarkeitsprüfung	Definiert die Art der Phasenüberwachung.
PMTU propagieren	Bestimmt, ob die PMTU (Path Maximum Transfer Unit) weitergeleitet wird.

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Erreichbarkeitsprüfung** *Inaktiv*.

(2) Entfernen Sie den Haken bei **PMTU propagieren**.

(3) Bestätigen Sie mit **OK**.

Konfigurieren Sie analog zu dieser Beschreibung die Phase 2 für das Gateway in der Filiale.

1.6 Ergebnis

Sie haben eine Lizenz für die Übertragung der IP-Adresse im B-/D-Kanal eingetragen. Die ISDN-Schnittstelle wurde für die Nutzung der Funktion IPSec Callback konfiguriert. In der Zentrale und der Filiale wurden xDSL-Internetzugänge eingerichtet. Die IPSec-Verbindung wurde auf dem Gateway der Zentrale konfiguriert.

1.7 Überprüfen der Konfiguration

Sie haben nun eine IPSec-Verbindung zwischen zwei Gateways konfiguriert, wobei die IP-Adressen der Gateways über ISDN zur Gegenseite übermittelt werden.

1.7.1 Test der Verbindung und des ISDN-Callback

Die Verbindung wird von der Zentrale aus aufgebaut, z. B. durch einen Ping. Indem Sie auf der Kommandozeile den Befehl `debug ipsec` eingeben, können Sie den Aufbau der Verbindung und den ISDN-Callback mitverfolgen.

```
r232bw:> debug ipsec
00:01:04 INFO/IPSEC: IPSEC CB - need callback from Peer "r232bw_filiale"
00:01:04 INFO/IPSEC: IPSEC CB - trigger callback at Peer "r232bw_filiale" (do call "*"->"850")
00:01:05 INFO/IPSEC: IPSEC CB - Peer "r232bw_filiale", trigger call "*" -> "850" is ALERTING
00:01:11 INFO/IPSEC: IPSEC CB - Peer "r232bw_filiale", CB Mode LLC failed (next B) - clear trigger call ("*" -> "850") now
00:01:11 INFO/IPSEC: P1: peer 1 (r232bw_filiale) sa 0 (-): Callback retry
00:01:11 INFO/IPSEC: IPSEC CB - need callback from Peer "r232bw_filiale"
00:01:11 INFO/IPSEC: IPSEC CB - trigger callback at Peer "r232bw_filiale" (do call "*"->"850")
00:01:11 INFO/IPSEC: IPSEC CB - Peer "r232bw_filiale", trigger call requested while peer triggeres ("*" -> "850");
                     clearing trigger call from peer first
00:01:11 INFO/IPSEC: IPSEC CB - Peer "r232bw_filiale", trigger call "*" -> "850" is ALERTING
00:01:21 INFO/IPSEC: IPSEC CB - Trigger Call by Peer "r232bw_filiale" successfully transmitted IP 84.146.201.132 /
                     Token 59766 via B channel
00:01:21 DEBUG/IPSEC: P1: peer 0 () sa 1 (R): new ip 84.146.201.132 <- ip 84.146.228.145
00:01:21 INFO/IPSEC:  P1: peer 0 () sa 1 (R): Vendor ID: 84.146.228.145:1023(No Id) is 'BINTEC'
00:01:21 INFO/IPSEC:  P1: peer 0 () sa 1 (R): Vendor ID: 84.146.228.145:1023(No Id) is 'BINTEC Heartbeats Version 1'
00:01:21 INFO/IPSEC:  P1: peer 0 () sa 1 (R): Vendor ID: 84.146.228.145:1023(No Id) is 'Dead Peer Detection (DPD, RFC 3706)'
00:01:21 DEBUG/IPSEC: P1: peer 1 (r232bw_filiale) sa 1 (R): identified ip 84.146.201.132 <- ip 84.146.228.145
00:01:21 DEBUG/IPSEC: P1: peer 1 (r232bw_filiale) sa 1 (R):token payload: received token 59766
00:01:22 DEBUG/IPSEC: P1: peer 1 (r232bw_filiale) sa 1 (R):notify id ipv4(any:0,[0..3]=192.168.1.254) <- id
                        ipv4(any:0,[0..3]=192.168.0.254) (unencrypted): Initial contact notification proto 1 spi(16) =
                        [c838dcd0 28dfec79 : 6511d733 cf7dd976]
00:01:22 INFO/IPSEC:  Trigger Bundle -1 (Peer 1 Traffic -1) prot 1 192.168.1.2:0->192.168.0.2:0
00:01:22 INFO/IPSEC:  P1: peer 1 (r232bw_filiale) sa 1 (R): done id ipv4(any:0,[0..3]=192.168.1.254)
                        <- id ipv4(any:0,[0..3]=192.168.0.254) AG[c838dcd0 28dfec79 : 6511d733 cf7dd976]
00:01:22 INFO/IPSEC:  P2: peer 1 (r232bw_filiale) traf 0 bundle -1 (I): created 192.168.1.0/24:0 < any >
                        192.168.0.0/24:0 rekeyed 0
00:01:23 DEBUG/IPSEC: P2: peer 1 (r232bw_filiale) traf 0 bundle -1 (I): SA 1 established ESP[20893821] in[0]
                        Mode tunnel enc 3des-cbc (192 bit) auth sha (160 bit)
00:01:23 DEBUG/IPSEC: P2: peer 1 (r232bw_filiale) traf 0 bundle -1 (I): SA 2 established ESP[34fffbf5] out[0]
                        Mode tunnel enc 3des-cbc (192 bit) auth sha (160 bit)
00:01:23 INFO/IPSEC:  Activate Bundle -1 (Peer 1 Traffic -1)
00:01:23 INFO/IPSEC:  P2: peer 1 (r232bw_filiale) traf 0 bundle -1 (I): established  (84.146.201.132<->84.146.228.145)
                        with 2 SAs life 3600 Sec/0 Kb rekey 2880 Sec/0 Kb Hb none
r232bw:>
```

In diesem Debug Auszug ist zu sehen, wie von der Zentrale aus der IPSec-Tunnel initiiert wird. Zuerst wird versucht, die IP-Adresse über den D-Kanal zu übertragen. Dies scheitert jedoch, z. B. weil dies von der Telefonanlage oder dem Provider nicht unterstützt wird. Anschließend wird die IP-Adresse im B-Kanal übertragen und der Tunnel aufgebaut.

1.8 Konfigurationsschritte im Überblick

Lizenz für IP-Adressübertragung über ISDN

Feld	Menü	Wert
Lizenzseriennummer	**Systemverwaltung** -> **Globale Einstellungen** -> **Systemlizenzen** -> **Neu**	Seriennummer
Lizenzschlüssel	**Systemverwaltung** -> **Globale Einstellungen** -> **Systemlizenzen** -> **Neu**	Lizenzschlüssel

ISDN-Schnittstellen

Feld	Menü	Wert
ISDN-Port	**Physikalische Schnittstellen** -> **ISDN-Ports** -> **MSN-Konfiguration** -> **Neu**	z. B. *bri-0*
Dienst	**Physikalische Schnittstellen** -> **ISDN-Ports** -> **MSN-Konfiguration** -> **Neu**	*IPSec*
MSN	**Physikalische Schnittstellen** -> **ISDN-**	z. B. *840*

Feld	Menü	Wert
	Ports -> **MSN-Konfiguration** -> **Neu**	
MSN-Erkennung	**Physikalische Schnittstellen** -> **ISDN-Ports** -> **MSN-Konfiguration** -> **Neu**	*Rechts nach Links*
Dienstemerkmal	**Physikalische Schnittstellen** -> **ISDN-Ports** -> **MSN-Konfiguration** -> **Neu**	*Daten + Sprache*

Internetzugänge

Feld	Menü	Wert
Beschreibung	**WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**	z. B. *T-Online*
PPPoE-Ethernet-Schnittstelle	**WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**	*ethoa50-0*
Benutzername	**WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**	Ihr Benutzername z. B. *t-online.de*
Passwort	**WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**	Ihr Passwort
Immer aktiv (Flatrate-Modus)	**WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**	*Deaktiviert*
IP-Adressmodus	**WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**	*IP-Adresse abrufen*
Standardroute	**WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**	*Aktiviert*
NAT-Eintrag erstellen	**WAN** -> **Internet + Einwählen** -> **PPPoE** -> **Neu**	*Aktiviert*

IPSec-Konfiguration

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *rs232bw_filiale*
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *IPV4-Adresse* und *192.168.0.254*
Preshared Key	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *geheim123*
Standardroute	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*Deaktiviert*
Lokale IP-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *192.168.1.254*
Routeneinträge	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. für *192.168.0.* **IP-Adresse** *0* und für *255.255.25*

Feld	Menü	Wert
		5.0
Modus	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu** -> **Erweiterte Einstellungen**	*Beide*
Eingehende ISDN-Nummer	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu** -> **Erweiterte Einstellungen**	z. B. *850*
Ausgehende ISDN-Nummer	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu** -> **Erweiterte Einstellungen**	z. B. *850*
Eigene IP-Adresse per ISDN übertragen	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu** -> **Erweiterte Einstellungen**	Aktiviert
Übertragungsmodus	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu** -> **Erweiterte Einstellungen**	z. B. *Automatische Erkennung des besten Modus*
Beschreibung	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->	z. B. *Phase1 PSK*
Proposal	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->	z. B. *3DES* und *SHA1*
DH-Gruppe	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->	z. B. *2(1024 Bit)*
Lebensdauer	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->	z. B. *28800* und *0*
Authentifizierungsmethode	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->	*Preshared Keys*
Modus	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->	*Aggressiv*
Lokaler ID-Typ	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->	z. B. *IPV4-Adresse*
Lokaler ID-Wert	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->	z. B. *192.168.1.254*
Erreichbarkeitsprüfung	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** -> -> **Erweiterte Einstellungen**	*Inaktiv*
NAT-Traversal	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** -> -> **Erweiterte Einstellungen**	*Deaktiviert*
Beschreibung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** ->	z. B. *Phase2*

Feld	Menü	Wert
Proposal	**VPN** -> **IPSec** -> **Phase-2-Profile**-> **<Multi-Proposal>** ->	z. B. *3DES* und *SHA1*
PFS-Gruppe verwenden	**VPN** -> **IPSec** -> **Phase-2-Profile**-> **<Multi-Proposal>** ->	*Aktiviert*
Lebensdauer	**VPN** -> **IPSec** -> **Phase-2-Profile**-> **<Multi-Proposal>** ->	z. B. *3600* und *0*
Erreichbarkeitsprüfung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** -> -> **Erweiterte Einstellungen**	*Deaktiviert*
PMTU propagieren	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** -> -> **Erweiterte Einstellungen**	*Deaktiviert*

Kapitel 2 Sicherheit - IPSec-Client-Authentifizierung über XAuth am Microsoft RADIUS Server (IAS)

2.1 Einleitung

Dieses Kapitel beschreibt die VPN IPSec-Anbindung des **bintec Secure IPSec Clients** an ein **bintec R3000** VPN-Gateway mit erweiterter Authentifizierung (XAuth) am Microsoft Windows 2003 RADIUS Server. Beim Aufbau des VPN-Tunnels wird eine doppelte Authentifizierung durchgeführt. Der VPN IPSec-Client Authentifiziert sich per Preshared Key am VPN-Gateway und zusätzlich wird über den Windows 2003 Server eine Benutzeranmeldung durchgeführt. Anschließend wird dem VPN IPSec-Client (per IKE Config Mode) eine dynamische private IP-Adresse aus dem Lokalen Netzwerk zugewiesen.

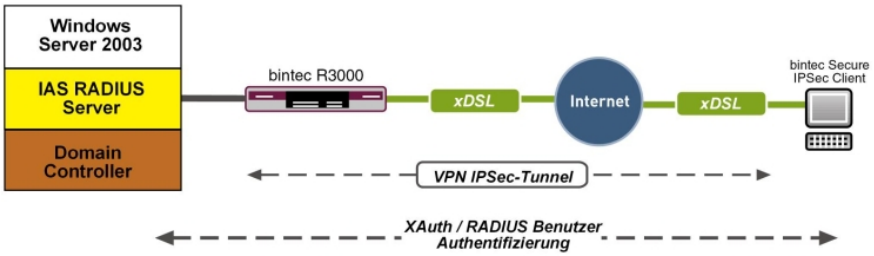


Abb. 9: Beispielszenario

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein VPN-Gateway z. B. **bintec R3000** mit Systemsoftware 7.8.7 (XAuth-Unterstützung)
- Ein **bintec Secure IPSec Client**
- Ein Microsoft Windows 2003 Server mit installiertem Internet Authentication Service (IAS)
- VPN-Gateway und VPN-Client benötigen jeweils eine unabhängige Verbindung zum Internet

2.2 Konfiguration

2.2.1 Konfiguration des VPN-Gateways

Lokale IP-Adresse konfigurieren

Das VPN-Gateway wird hier mit der IP-Adresse 192.168.10.254 betrieben. Um dem VPN-Client eine IP-Adresse aus diesem Netzwerkbereich zuweisen zu können muss die Option **Proxy ARP** aktiviert werden.

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

Abb. 10: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Bearbeiten**

Relevante Felder im Menü Schnittstellen

Feld	Bedeutung
Adressmodus	Hier wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird.
IP-Adresse / Netzmaske	Tragen Sie hier die **IP-Adresse** und die entsprechende **Netzmaske** der Schnittstelle ein.
Schnittstellenmodus	Hier wählen Sie den Konfigurationsmodus der Schnittstelle aus.
Proxy ARP	Aktivieren Sie die Option **Proxy ARP**.

VPN-Konfiguration

Im Menü **IP Pools** wird ein IP-Adress-Pool spezifiziert, aus dem dem VPN-Client beim Aufbau des Tunnels eine Adresse zugewiesen wird. In unserem Beispiel wird ein Bereich aus dem lokalen Netzwerk gewählt z. B. 192.168.10.150 bis 192.168.10.180.

(1) Gehen Sie zu **VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**.

Abb. 11: **VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**

Relevante Felder im Menü IP Pools

Feld	Bedeutung
IP-Poolname	Geben Sie die Bezeichnung des IP Pools ein.
IP-Poolbereich	Geben Sie im ersten Feld die erste IP-Adresse aus dem lokalen Netzwerk ein. Geben Sie im zweiten Feld die letzte IP-Adresse aus dem lokalen Netzwerk ein.

XAUTH-Konfiguration

Für die Erweiterte IPSec-Authentifizierung (XAuth) soll ein RADIUS Server verwendet werden. Die hierfür notwendigen Einstellungen werden im Menü **XAuth-Profile** vorgenommen.

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

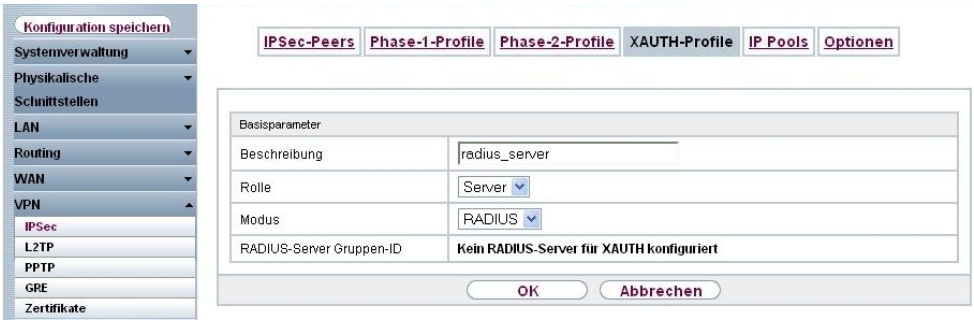


Abb. 12: **VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**

Relevante Felder im Menü XAUTH-Profile

Feld	Bedeutung
Beschreibung	Geben Sie eine Beschreibung für die IPSec-Authentifizierung ein.
Rolle	Wählen Sie hier `Server` aus.
Modus	Bei **Modus** wählen Sie `RADIUS` aus.

IPSec-Peers-Konfiguration

Sie können nun die **IPSec-Peers** konfigurieren. Pro VPN Client-Verbindung wird ein Eintrag angelegt. Der **Preshared Key** sowie die **Lokale ID** müssen für jeden Benutzer bzw. für jeden Tunnel unterschiedlich hinterlegt werden.

Wählen Sie die Schaltfläche **Neu**, um weitere IPSec-Peers einzurichten.

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

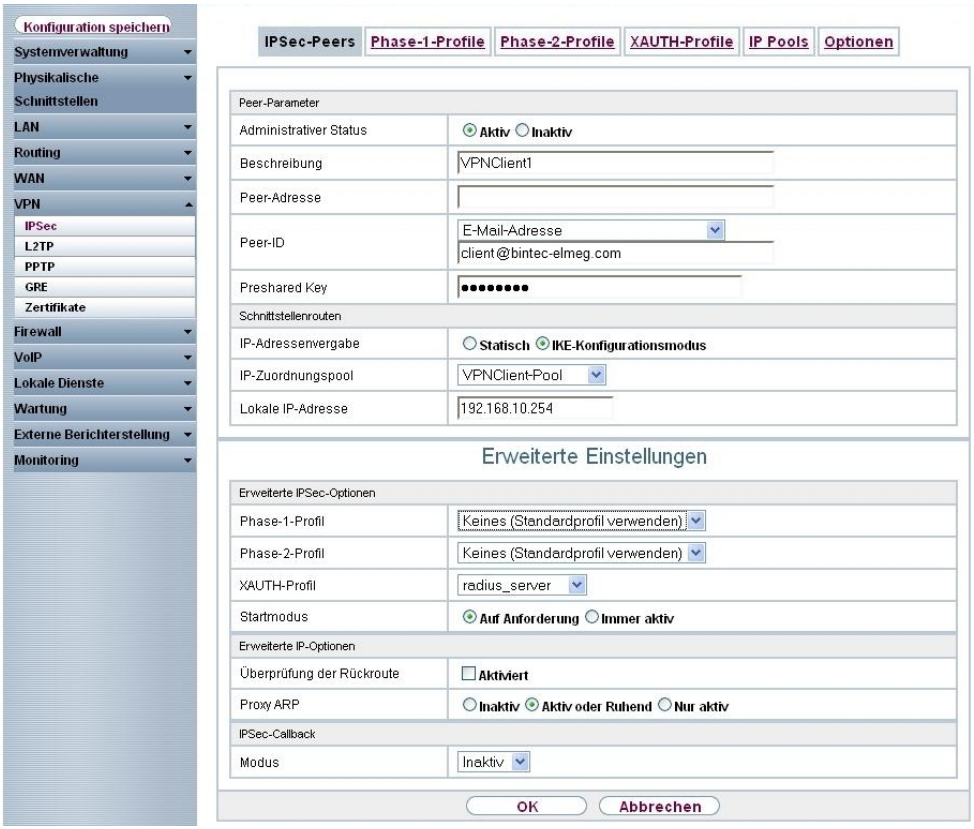


Abb. 13: **VPN** -> **IPSec** -> **IPSec-Peers** ->

Relevante Felder im Menü Peer-Parameter

Feld	Bedeutung
Administrativer Status	Stellen Sie den Administrativer Status auf **Aktiv**. Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung.
Beschreibung	Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert.
Peer-ID	Wählen Sie den ID-Typ aus und geben Sie die ID des Peers ein. Auf dem Peer-Gerät entspricht diese ID dem Parameter **Lokaler ID-Wert**. Mögliche ID-Typen: • Full Qualified Domain Name (FQDN) • E-Mail-Adresse • IVP4-Adresse • ASN.1-DN (Distinguished Name)
Preshared Key	Bei **Preshared Key** geben Sie das mit dem Peer vereinbarte Passwort ein.
IP-Adressenvergabe	Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Bei Auswahl der Option *IKE-Konfigurationsmodus* wählen Sie eine IP-Adresse aus dem konfigurierten IP-Pool aus.
IP-Zuordnungspool	Wählen Sie einen im Menü **VPN** -> **IP Pools** konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung *Noch nicht definiert*.
Lokale IP-Adresse	Geben Sie die WAN IP-Adresse Ihrer IPSec-Verbindung an. Es kann die gleiche IP-Adresse sein, die als LAN IP-Adresse an Ihrem Router konfiguriert ist.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Bedeutung
Phase-1-Profil	Mit Auswahl von *Keines (Standardprofil verwenden)* wird das in **Phase-1-Profile** als Standard markiertes Profil verwendet.
Phase-2-Profil	Mit Auswahl von *Keines (Standardprofil verwenden)* wird das in **Phase-2-Profile** als Standard markiertes Profil verwendet.

Feld	Bedeutung
XAUTH-Profil	Wählen Sie hier ein konfiguriertes XAUTH-Profil (z. B. *radius_server*) aus.
Startmodus	Hier können Sie auswählen, wie der Peer in den aktiven Zustand versetzt werden soll. Mit Auswahl von *Auf Anforderung* wird der Peer durch einen Trigger in den aktiven Zustand versetzt.
Überprüfung der Rückroute	Hier wird festgelegt, ob für die Schnittstelle zum Verbindungspartner eine Überprüfung der Rückroute aktiviert werden soll.
Proxy ARP	Stellen Sie **Proxy ARP** auf *Aktiv oder Ruhend*. Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer aktiv oder ruhend ist.
Modus	Stellen Sie den **Modus** des **IPSec-Callback** auf *Inaktiv*. Das lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gerät.

Phase-1-Profile

Im Menü **Phase-1-Profile** können Sie die Phase 1 (IKE) Einstellungen festlegen. Klicken Sie auf das -Symbol, um vorhanden Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Profile hinzuzufügen.

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

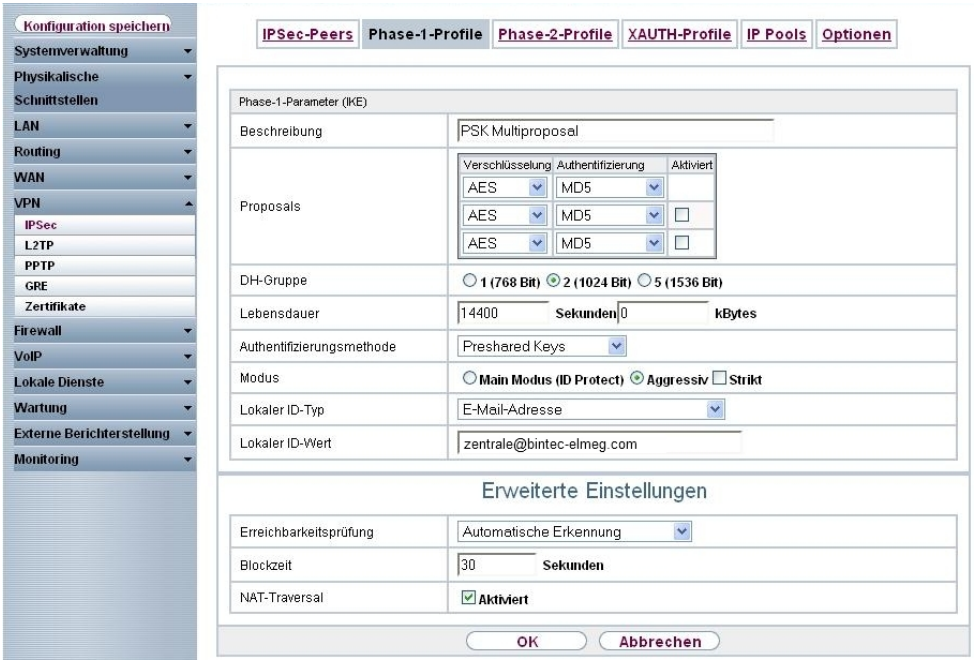


Abb. 14: **VPN** -> **IPSec** -> **Phase-1-Profile** ->

Relevante Felder im Menü Phase-1-Parameter (IKE)

Feld	Bedeutung
Modus	Wählen Sie den Phase-1-Modus `Aggressiv` aus. Der Aggressive Modus ist erforderlich, falls einer der Peers keine statische IP-Adresse hat und Preshared Keys für die Authentifizierung genutzt werden; er erfordert nur drei Meldungen für die Einrichtung eines sicheren Kanals.
Lokaler ID-Typ	Wählen Sie den Typ der Lokalen ID aus. Mögliche Werte: • Full Qualified Domain Name (FQDN) • E-Mail-Adresse • IVP4-Adresse • ASN.1-DN (Distinguished Name)
Lokaler ID-Wert	Geben Sie die ID des VPN Gateways ein, z. B. `zentrale@bintec-elmeg.com`

Phase-2-Profile

Die Einstellungen im Menü **VPN** -> **IPSec** -> **Phase-2-Profile** können unverändert übernommen werden.

RADIUS-Einstellungen

Durch die Einstellungen im Menü **RADIUS** wird die erweiterte IPSec-Authentifizierung (XAuth) mit dem Windows 2003 RADIUS Server (IAS) aktiviert. Es ist notwendig den **Authentifizierungstyp** auf den Wert `XAuth` zu setzen sowie die **Server-IP-Adresse** des Microsft Windows 2003 RADIUS Server (IAS) zu hinterlegen. Die Kommunikation mit dem RADIUS Server wird mit einem Passwort geschützt.

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**.

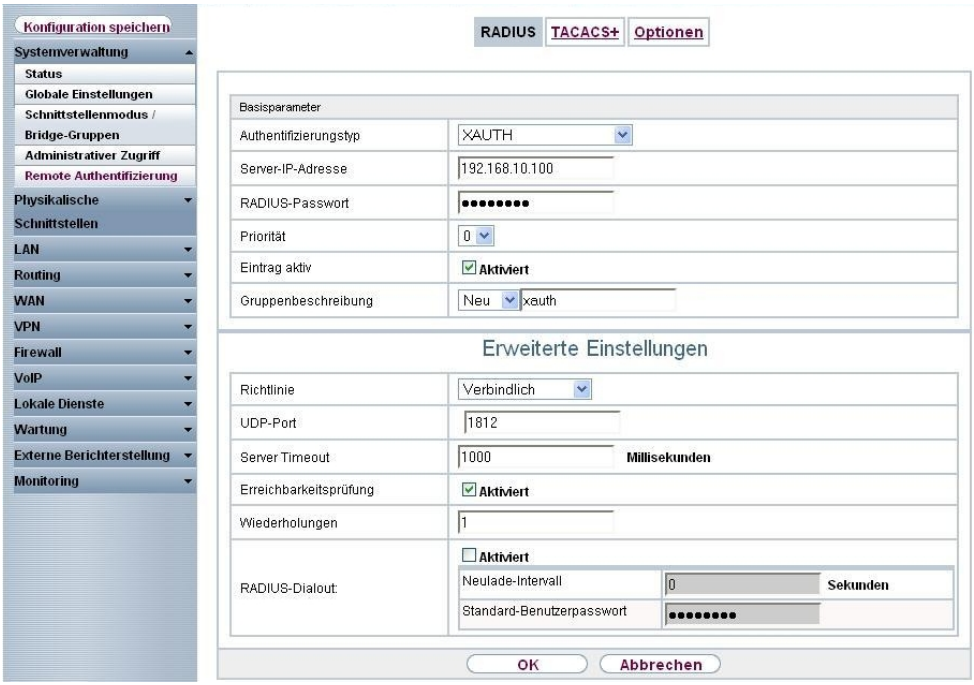


Abb. 15: **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**

Relevante Felder im Menü RADIUS

Feld	Bedeutung
Authentifizierungstyp	Wählen Sie den **Authentifizierungstyp** `XAUTH` aus.
Server-IP-Adresse	Geben Sie die **Server-IP-Adresse** des Microsft Windows 2003 RADIUS Server (IAS) ein.

Feld	Bedeutung
RADIUS-Passwort	Geben Sie das für die Kommunikation zwischen RADIUS Server und Ihrem Gerät gemeinsam genutzte Passwort (z. B. *bintec elmeg*) ein.
Gruppenbeschreibung	Definieren Sie eine neue RADIUS-Gruppenbeschreibung bzw. weisen Sie den neuen RADIUS-Eintrag einer schon definierten Gruppe zu. Die konfigurierten RADIUS-Server einer Gruppe werden gemäß der **Priorität** und der **Richtlinie** abgefragt. Mögliche Werte: • *Neu* (Standardwert): Tragen Sie in das Textfeld eine neue Gruppenbeschreibung ein, z. B. xauth • <Gruppenname>: Wählen Sie aus der Liste eine schon definierte Gruppe aus.

2.2.2 Konfiguration des Windows 2003 RADIUS Servers

In diesem Beispiel wird ein Windows 2003 RADIUS Server für die erweiterte IPSec-Authentifizierung (XAuth) verwendet. An diesem Server muss der **Internet Authentication Service** (IAS) installiert sein. Der RADIUS Server greift auf den Microsoft Active Directory Service zu und verwendet für die erweiterte IPSec-Authentifizierung (XAuth) die Windows Logon Daten.

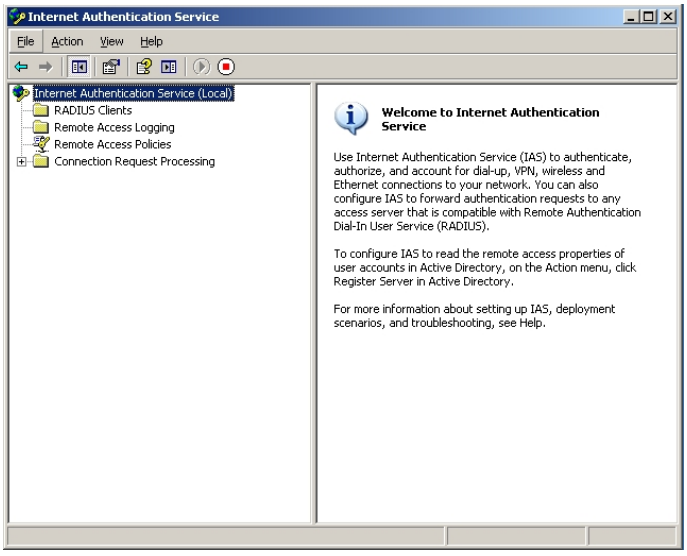


Abb. 16: Internet Authentication Service

In der Microsoft Management Console **Internet Authentication Service** muss im Untermenü **New RADIUS Client** der `R3000` als RADIUS Client angelegt werden. Geben Sie die Bezeichnung und die IP-Adresse des VPN Gateways ein.

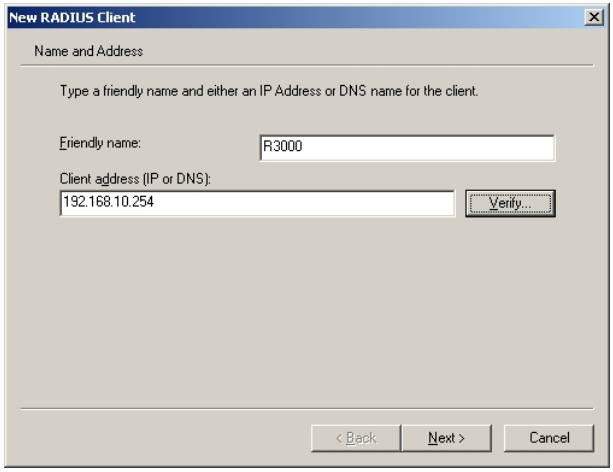


Abb. 17: New RADIUS Client

Hier wird das Passwort für die RADIUS-Kommunikation (z. B. `bintec elmeg`) hinterlegt.

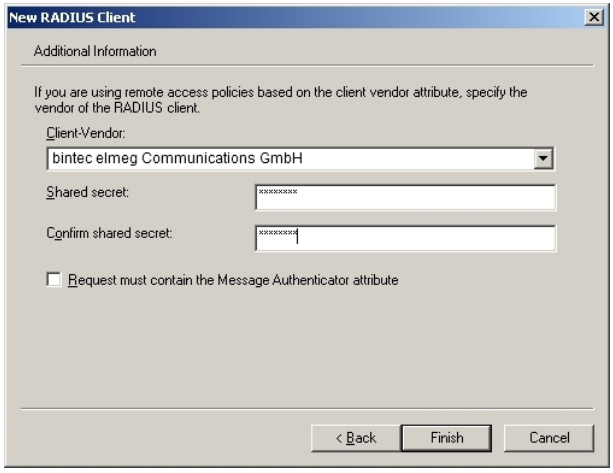


Abb. 18: Password

Anschließend wird im Untermenü **New Remote Access Policy Wizard** eine neue Richtlinie angelegt.

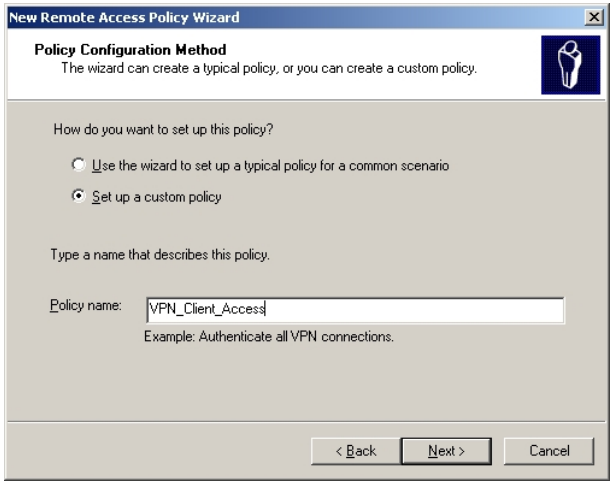


Abb. 19: Policy Name

Beim Anlegen der **Remote Access Policy** müssen Bedingungen hinterlegt werden für die diese Einwahl-Richtlinie greifen soll. In diesem Beispiel wird der entsprechende Client-Anbieter hinterlegt. Beispielsweise wäre es auch möglich eine bestimmte Zeitspanne, während diese Einwahl-Richtlinie verwendet werden soll, zu hinterlegen.

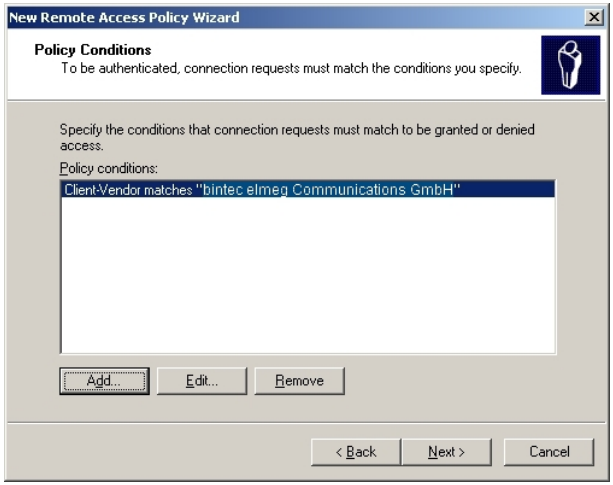


Abb. 20: Policy Conditions

Die Einwahl-Richtlinie soll den VPN-Zugriff bzw. den Zugriff auf das Netzwerk erlauben. Aktivieren Sie dazu `Grant remote access permission`.

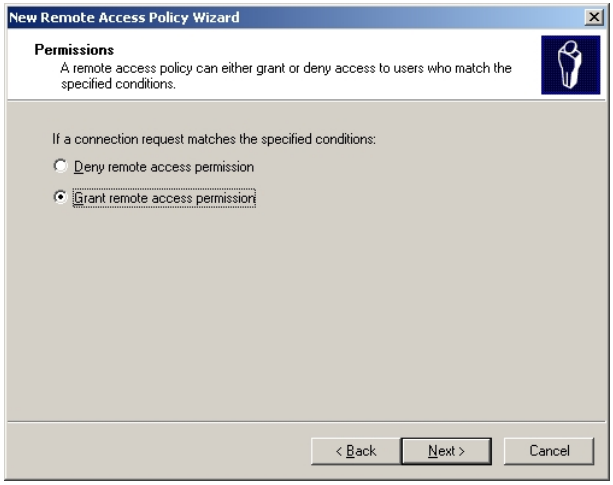


Abb. 21: Permissions

Die weiteren Schritten zum Anlegen einer neuen Einwahl-Richtlinie können, wie in den folgenden Schritten gezeigt, übernommen werden.

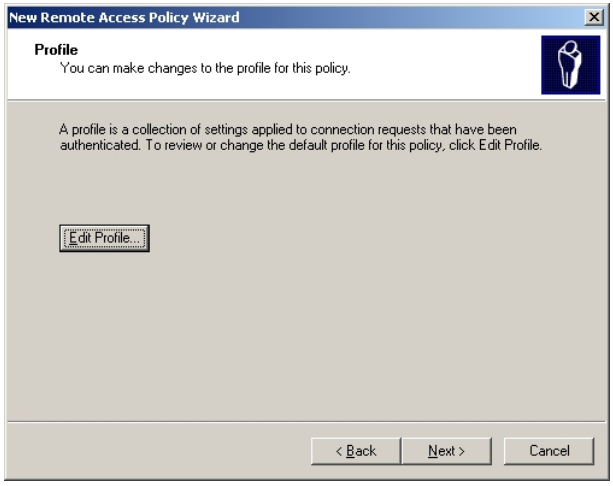


Abb. 22: Profile

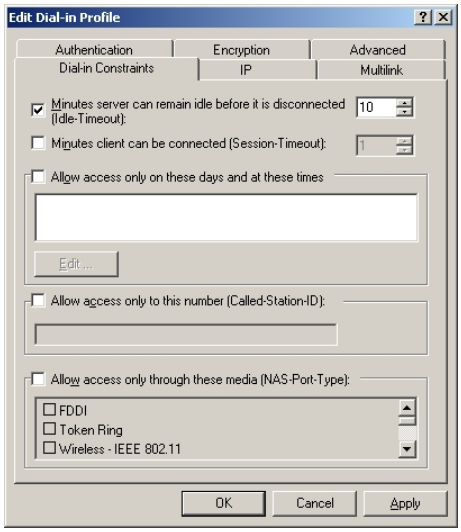


Abb. 23: Dial-in Constraints

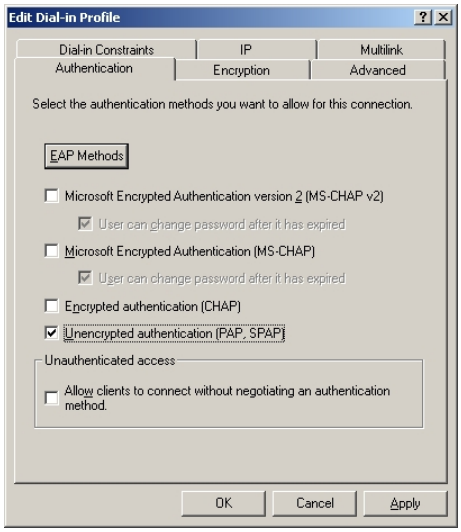


Abb. 24: Authentication

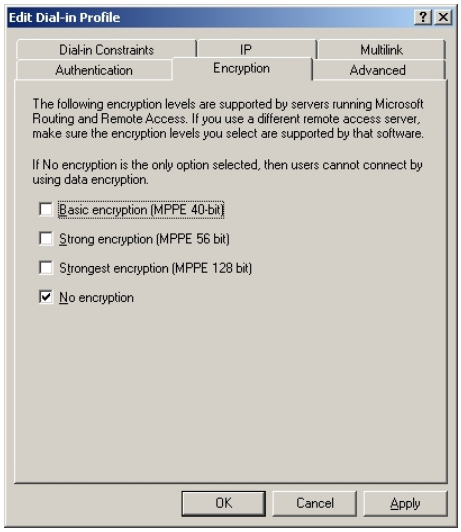


Abb. 25: Encryption

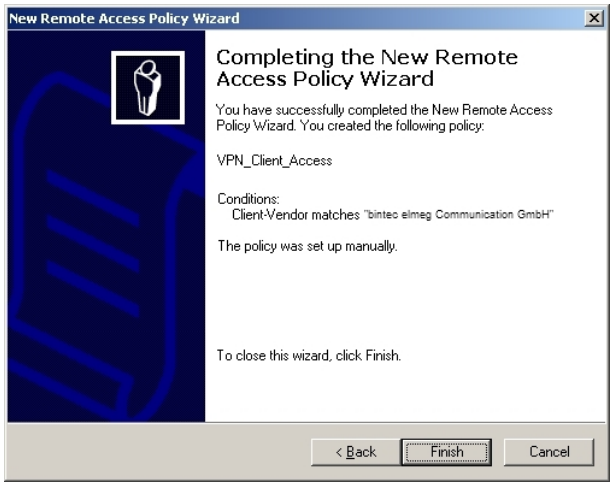


Abb. 26: New Remote Access policy Wizard

Über die Benutzerverwaltung des **Active Directory Services** besteht die Möglichkeit pro Anwender die VPN-Einwahl zu erlauben bzw. zu unterbinden.

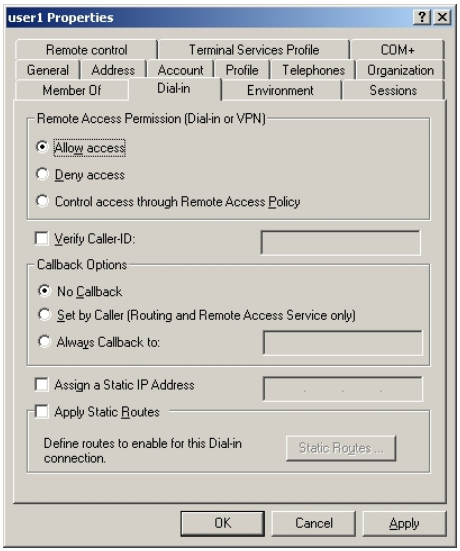


Abb. 27: Dial-in

2.2.3 Konfiguration des bintec Secure IPSec Clients

Der **bintec Secure IPSec Clients** wird über **Start** -> **Programme** -> **FEC Secure IPSec Client** -> **Secure Client Modus** aufgerufen. Die Konfiguration des **bintec Secure IPSec Clients** wird über den Assistenten durchgeführt. Beim ersten Start des **bintec Secure IPSec Clients** wird der **Assistent für neues Profil** automatisch gestartet. Wählen Sie die Auswahl **Verbindung zum Firmennetz über IPSec** aus.

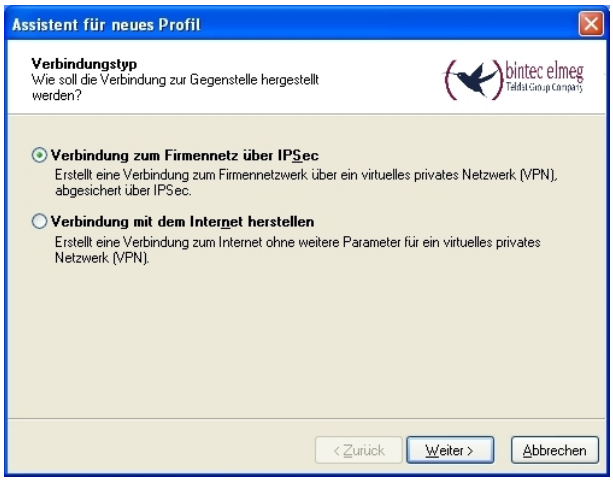


Abb. 28: Verbindungstyp

Geben Sie einen Namen für das Profil ein z. B. *Zentrale*.

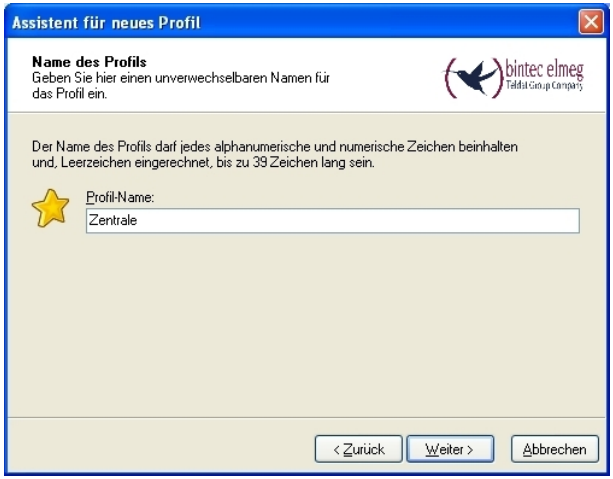


Abb. 29: Profil-Name

Im nächsten Schritt des Assistenten muss ein **Verbindungsmedium** ausgewählt werden über welches eine Verbindung zum Internet aufgebaut wird. In unserem Beispiel wird die Auswahl *LAN (over IP)* verwendet da der VPN-Client keinen direkten Zugang zum Internet herstellt sondern einen Internetzugangsrouter verwendet.

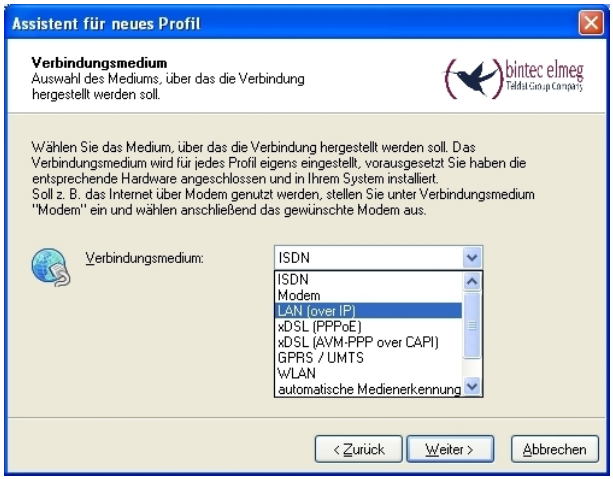


Abb. 30: Verbindungsmedium

Bei der Option **Gateway (Tunnel-Endpunkt)** wird die Adresse hinterlegt über die das VPN-Gateway aus dem Internet erreichbar ist. Aktivieren Sie die Option *Erweiterte Authentifizierung (XAUTH)*.

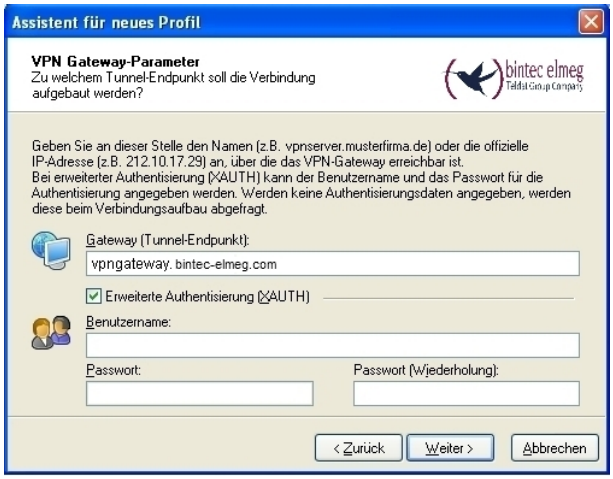


Abb. 31: VPN Gateway-Parameter

Anschließend wird als **Austausch-Modus** der `Aggressive Mode` verwendet, da dem **bintec R3000** Router und dem **bintec Secure IPSec Client** dynamische IP-Adresse vom Provider zugewiesen werden. Die **PFS-Gruppe** setzen Sie z. B. auf `DH-Gruppe 2 (1024 Bit)`. Die Option `Benutze IP-Kompression` wird in dieser Konfiguration nicht eingesetzt.

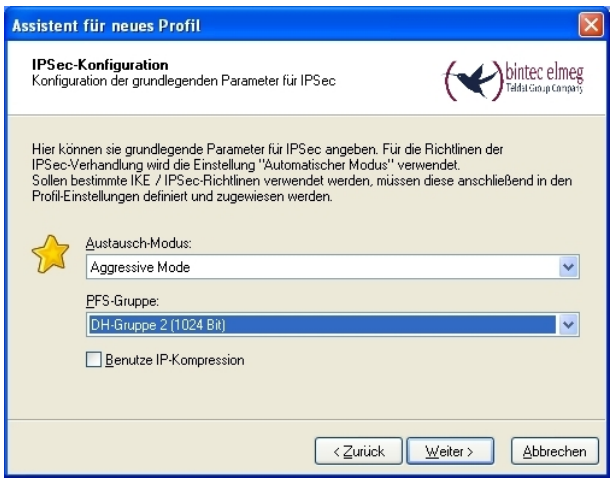


Abb. 32: IPSec-Konfiguration

Im nächsten Schritt des Assistenten wird der am VPN-Gateway hinterlegte **Preshared Key** sowie dessen **Peer-ID** hinterlegt. Im Feld **Type** wird die Benutzung der Option `Fully Qualified Username` empfohlen.

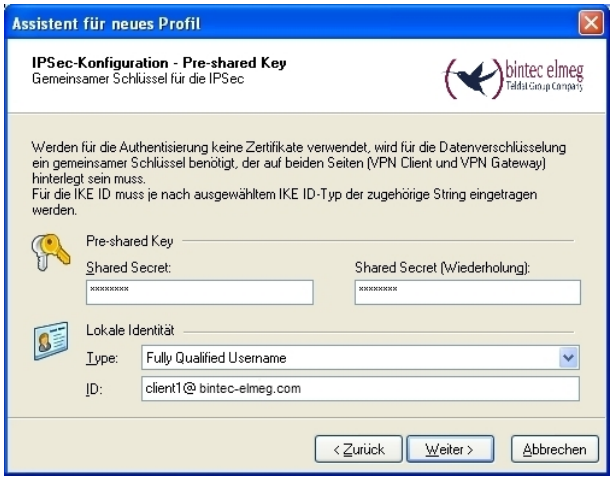


Abb. 33: Pre-shared Key

In diesem Beispiel wird dem VPN IPSec-Client eine dynamische VPN IP-Adresse zugewiesen. Dazu muss die Option *IKE Config Mode verwenden* ausgewählt werden.

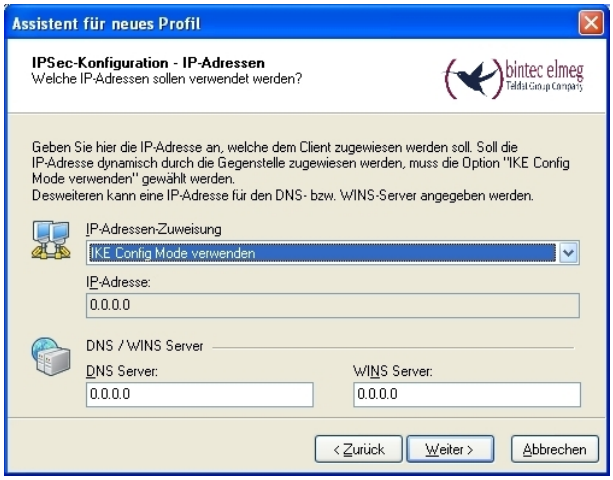


Abb. 34: IKE Config Mode

Im letzten Schritt wird die **Firewall** des **bintec Secure IPSec Clients** konfiguriert. Wenn der Client direkt mit dem Internet verbunden ist, sollte die Firewall aktiviert sein.

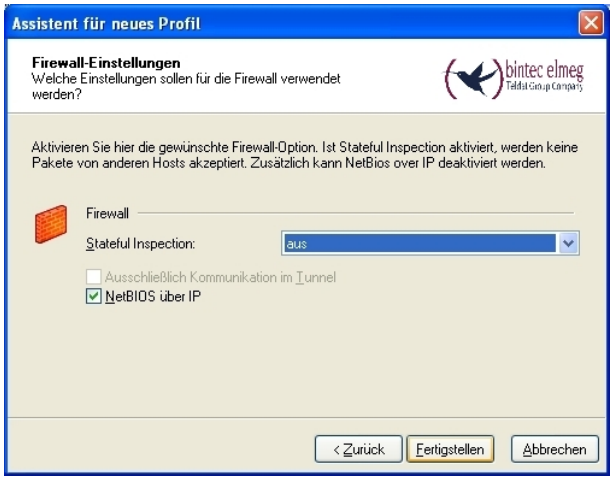


Abb. 35: Firewall

2.3 Kontrolle

Beim Aufbau des VPN IPsec-Tunnels erscheint am **bintec Secure IPSec Client** eine Benutzer-Passwortabfrage. Dort müssen die Windows-Logon Daten eingetragen werden. Neben der IPSec-Authentifizierung erfolgt eine zusätzliche Authentifizierung am RADIUS Server. Anschließend wird dem **bintec Secure IPSec Client** eine IP-Adresse zugewiesen.

Systemmeldungen des VPN-Gateways

```
13:38:37 DEBUG/IPSEC: P1: peer 0 () sa 78 (R): new ip 10.1.1.2 <- ip 10.1.1.3
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'da8e937880010000'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'draft-ietf-ipsra-isakmp-xauth-06'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'draft-ietf-ipsec-nat-t-ike-03'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'draft-ietf-ipsec-nat-t-ike-02'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'draft-ietf-ipsec-nat-t-ike-00'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is '4a131c81070358455c5728f20e95452f'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'Dead Peer Detection (DPD, RFC 3706)'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'cb1ed48b6d68269bb411b61a07bce24a'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'c61baca1f1a60cc10800000000000000'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is '4048b7d56ebce88525e7de7f00d6c2d3c0000000'
13:38:37 INFO/IPSEC:  P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is '12f5f28c457168a9702d9fe274cc0100'
13:38:37 DEBUG/IPSEC: P1: peer 1 (VPNClient) sa 78 (R): identified ip 10.1.1.2 <- ip 10.1.1.3
13:38:38 DEBUG/IPSEC: P1: peer 1 (VPNClient) sa 78 (R): notify id usr@fqdn(any:0,[0..23]=zentrale@funkwerk-ec.com) <- id
                      usr@fqdn(any:0,[0..22]=client1@funkwerk-ec.com): Initial contact notification proto 1 spi(16) =
                      [f8c1c782 5235a083 : aa54a587 ea60d83d]
13:38:38 DEBUG/IPSEC: P1: peer 1 (VPNClient) sa 78 (R): [Aggr] NAT-T: port change: local: 10.1.1.2:500->10.1.1.2:4500,
                      remote: 10.1.1.3:669->10.1.1.3:56542
13:38:38 INFO/IPSEC:  XAUTH: peer 1 (VPNClient) sa 78 (I): request extended authentication
13:38:38 INFO/IPSEC:  P2: peer 1 (VPNClient) traf 0 bundle 48 (R): deleted (Initial contact), Pkts: 123/98 Kb: 0/1 Bytes:
                      40856(48984)/18600(25840) rekeyed by 0
13:38:38 DEBUG/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 48 (R): SA 106 deleted errors 0/0/0
13:38:38 DEBUG/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 48 (R): SA 105 deleted errors 0/0/0
13:38:38 INFO/IPSEC:  Destroy Bundle 48 (Peer 1 Traffic -1)
13:38:38 INFO/IPSEC:  P1: peer 1 (VPNClient) sa 78 (R): done id usr@fqdn(any:0,[0..23]=zentrale@funkwerk-ec.com) <- id
                      usr@fqdn(any:0,[0..22]=client1@funkwerk-ec.com) AG[f8c1c782 5235a083 : aa54a587 ea60d83d]
13:38:38 DEBUG/IPSEC: RADIUS: requested user user1
13:38:38 INFO/IPSEC:  XAUTH: peer 1 (VPNClient) sa 78 (I): extended authentication for user 'user1' succeeded
13:38:40 INFO/IPSEC:  CFG: peer 1 (VPNClient) sa 78 (R): request for ip address received
13:38:40 INFO/IPSEC:  CFG: peer 1 (VPNClient) sa 78 (R): ip address 192.168.10.166 assigned
13:38:40 INFO/IPSEC:  P2: peer 1 (VPNClient) traf 0 bundle 49 (R): created 0.0.0.0/0:0 < any > 192.168.10.166/32:0 rekeyed 0
13:38:40 DEBUG/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 49 (R): SA 107 established ESP[490750e9] in[0] Mode tunnel enc
                      aes-cbc (128 bit) auth md5 (128 bit)
13:38:40 DEBUG/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 49 (R): SA 108 established ESP[56954d49] out[0] Mode tunnel enc
                      aes-cbc (128 bit) auth md5 (128 bit)
13:38:40 INFO/IPSEC:  Activate Bundle 49 (Peer 1 Traffic -1)
13:38:40 INFO/IPSEC:  P2: peer 1 (VPNClient) traf 0 bundle 49 (R): established  (10.1.1.2<->10.1.1.3) with 2 SAs life 28800
                      Sec/0 Kb rekey 25920 Sec/0 KbHb none PMTU
```

Logbuch des bintec Secure IPSec Clients

Zusätzlich erfolgt ein Eintrag im Systemprotokoll des Windows 2003 Servers.

```
User user1 was granted access.
 Fully-Qualified-User-Name = virtualnet.funkwerk-ec.com/FEC_QA_users/user1
 NAS-IP-Address = <not present>
 NAS-Identifier = r3000
 Client-Friendly-Name = R3000
 Client-IP-Address = 192.168.10.254
 Calling-Station-Identifier = <not present>
 NAS-Port-Type = <not present>
 NAS-Port = <not present>
 Proxy-Policy-Name = Use Windows authentication for all users
 Authentication-Provider = Windows
 Authentication-Server = <undetermined>
 Policy-Name = VPN_Client_Access
 Authentication-Type = PAP
 EAP-Type = <undetermined>
```

2.4 Windows-Anmeldung per VPN (optional)

Der **bintec Secure IPSec Client** bietet optional die Möglichkeit die Windows-Anmeldung durchzuführen. Dazu wird bereits beim Starten des Betriebssystems bzw. bei der Windows-Anmeldung die VPN-Verbindung hergestellt. Anschließend wird über diese VPN-Verbindung die Windows-Anmeldung durchgeführt.

Die Windows-Anmeldung (per VPN-Verbindung) wird im **bintec Secure IPSec Client** im Menü **Konfiguration** -> **Logon-Optionen** aktiviert.

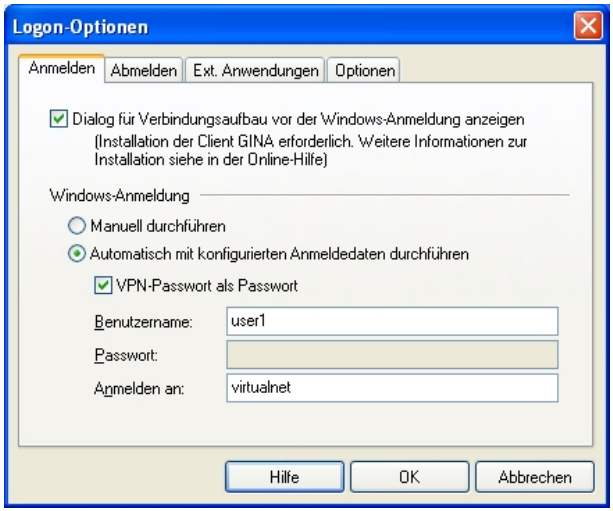


Abb. 36: Logon-Optionen

Beim Starten des Betriebssystems erscheint anschließend die **bintec Secure IPSec Client - Windows-Anmeldung**.

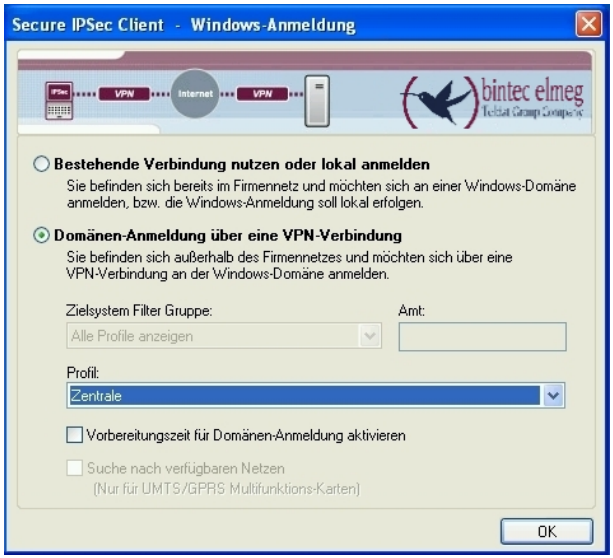


Abb. 37: Windows-Anwendung

2.5 Konfigurationsschritte im Überblick

Lokale IP-Adresse konfigurieren

Feld	Menü	Wert
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Bearbeiten**	*Statisch*
IP-Adresse / Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Bearbeiten**	z. B. *192.168.10.254* / *255.255.255.0*
Schnittstellenmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Bearbeiten**	Manuell
Proxy ARP	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Bearbeiten**	Aktiviert

VPN Konfiguration

Feld	Menü	Wert
IP-Poolname	**VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**	z. B. *VPNClient-Pool*
IP-Poolbereich	**VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**	z. B. *192.168.10.150* - *192.168.10.180*

XAUTH Konfiguration

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	z. B. *radius_server*
Rolle	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	*Server*
Modus	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	*RADIUS*

IPSec-Peers Konfiguration

Feld	Menü	Wert
Administrativer Status	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*Aktiv*
Beschreibung	**VPN** -> **IPSec** -> **IPSec-Peers** ->	z. B. *VPNClient1*
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*E-Mail-Adresse / client1@bintec-elmeg.com*
Preshared Key	**VPN** -> **IPSec** -> **IPSec-Peers** ->	z. B. *bintec elmeg*
IP-Adressenvergabe	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*IKE-Konfigurationsmodus*
IP-Zuordnungspool	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*VPNClient-Pool*
Lokale IP-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** ->	z. B. *192.168.10.254*
Phase-1-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Keines (Standardprofil verwenden)*
Phase-2-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Keines (Standardprofil verwenden)*
XAUTH-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*radius_server*
Startmodus	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Auf Anforderung*
Überprüfung der Rückroute	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	Deaktiviert
Proxy ARP	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Aktiv oder Ruhend*
Modus	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Inaktiv*

Phase-1-Profile Konfiguration

Feld	Menü	Wert
Modus	**VPN** -> **IPSec** -> **Phase-1-Profile** -> 	*Aggressiv*
Lokaler ID-Typ	**VPN** -> **IPSec** -> **Phase-1-Profile** -> 	*E-Mail-Adresse*
Lokaler ID-Wert	**VPN** -> **IPSec** -> **Phase-1-Profile** -> 	z. B. *zentrale@bintec-elmeg.com*

RADIUS-Einstellungen

Feld	Menü	Wert
Authentifizierungstyp	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	*XAuth*
Server-IP-Adresse	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *192.168.10.100*
RADIUS-Passwort	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *bintec elmeg*
Gruppenbeschreibung	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *xauth*

Konfiguration des Windows 2003 RADIUS Servers

Feld	Menü	Wert
Friendly name	**New RADIUS Client**	*R3000*
Client address (IP or DNS)	**New RADIUS Client**	*192.168.10.254*
Client-Vendor	**New RADIUS Client**	z. B. *BinTec Comunications GmbH*
Shared secret	**New RADIUS Client**	z. B. *bintec elmeg*
Confirm shared secret	**New RADIUS Client**	z. B. *bintec elmeg*
Policy name	**New Remote Access Policy Wizard**	z. B. *VPN_Client_Access*
Policy conditions	**New Remote Access Policy Wizard**	z. B. *Client-Vendor matches "BinTec Communications GmbH"*
Grant remote acces permission	**New Remote Access Policy Wizard**	Aktiviert
Edit Profile	**New Remote Access Policy Wizard**	Aktiviert

Feld	Menü	Wert
Idle Timeout	**Edit Dial-in Profile**	*10 Minuten*
Authentication	**Edit Dial-in Profile**	*Unencrypted authentication (PAP, SPAP)*
Encryption	**Edit Dial-in Profile**	*No encryption*
Dial-in	**user 1 Properties**	*Allowed acces*

Konfiguration des bintec Secure IPSec Clients

Feld	Menü	Wert
Verbindungstyp	**Assistent für neues Profil**	*Verbindung zum Firmennetz über IPSec*
Profil-Name	**Assistent für neues Profil**	*Zentrale*
Verbindungsmedium	**Assistent für neues Profil**	*LAN (over IP)*
Gateway (Tunnel-Endpunkt)	**Assistent für neues Profil**	z. B. *vpngateway.bintec-elmeg.com*
Erweiterte Authentifizierung (XAUTH)	**Assistent für neues Profil**	Aktiviert
Austausch-Modus	**Assistent für neues Profil**	Aggressive Mode
PFS-Gruppe	**Assistent für neues Profil**	DH-Gruppe 2 (1024 Bit)
Shared Secret	**Assistent für neues Profil**	z. B. *bintec elmeg*
Shared Secret (Wiederholung)	**Assistent für neues Profil**	z. B. *bintec elmeg*
Typ	**Assistent für neues Profil**	z. B. *Fully Qualified Username*
ID	**Assistent für neues Profil**	z. B. *client1@bintec-elmeg.com*
IP-Adressen-Zuweisung	**Assistent für neues Profil**	*IKE Config Mode verwenden*
Stateful Inspection	**Assistent für neues Profil**	*aus*
NetBIOS über IP	**Assistent für neues Profil**	Aktiviert

Kapitel 3 Sicherheit - VPN IPSec Authentifizierung mit KOBIL SecOVID One-Time-Passwort Abfrage

3.1 Einleitung

Dieses Kapitel beschreibt die VPN IPSec-Anbindung des **bintec Secure IPsec Clients** an ein **bintec R3000** VPN-Gateway mit erweiterter Authentifizierung (XAuth) über ein One-Time-Passwort am **KOBIL SecOVID** Server. Beim Aufbau des VPN-Tunnels wird eine doppelte Authentifizierung per One-Time-Passwort durchgeführt, welches über einen **KOBIL SecOVID** Token generiert wird. Beim Aufbau der VPN-Verbindung wird dem **bintec Secure IPSec Client** (per IKE-Config-Mode) eine dynamische IP-Adresse aus dem Lokalen Netzwerk zugewiesen. Das **bintec R3000** VPN-Gateway wird mit einem Multiuser VPN-Peer konfiguriert der Verbindungen mehrerer VPN-Clients zulässt.

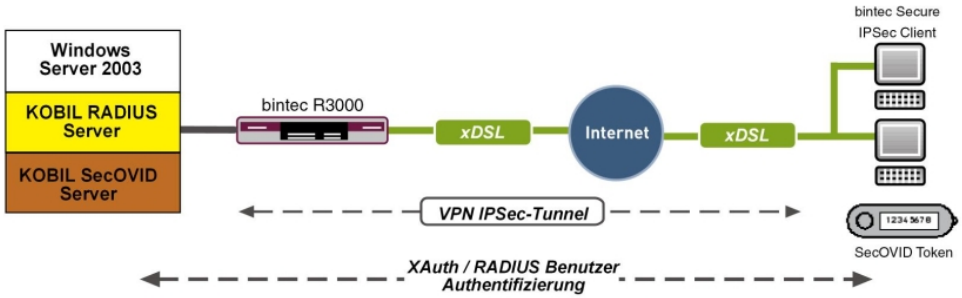


Abb. 38: Beispielszenario

Voraussetzungen

- Ein bintec VPN-Gateway z. B. **bintec R3000** mit Systemsoftware 7.8.7 (XAuth-Unterstützung)
- Ein **bintec Secure IPsec Client**
- Ein **KOBIL SecOVID** Server, der auf einem Microsoft Windows Rechner installiert wird (z. B. Server 2003 (32 Bit))
- Ein **KOBIL SecOVID** Token
- VPN-Gateway und VPN-Client benötigen jeweils eine unabhängige Verbindung zum In-

ternet

3.2 Konfiguration

3.2.1 Installation des KOBIL SecOVID Servers

Installation des KOBIL SecOVID Servers auf einem 32Bit Windows 2003 Server

Das Installationsprogramm des **KOBIL SecOVID** Servers wird auf der CD über den Aufruf der Datei `win32\server\SECOVID Server.exe` gestartet. Bitte lesen Sie die Ausgaben des Setups zu Ihrer Information und folgen Sie den Anweisungen und Empfehlungen der Installationsroutine. Nach Abschluss der Installationsroutine sollte das Logfile des **KOBIL SecOVID** Servers überprüft werden um sicher zu stellen das der Server gestartet wurde.

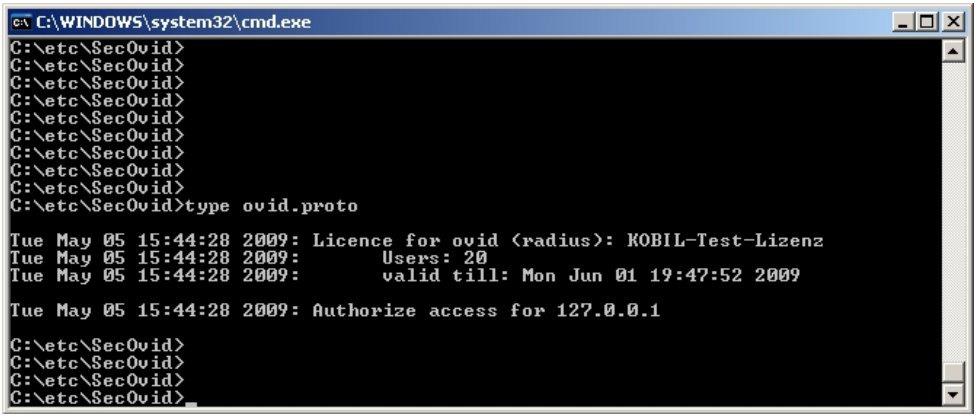


Abb. 39: Installation des **KOBIL SecOVID**

Installation des KOBIL SecOVID Administrationstools

Zur Installation des **KOBIL SecOVID** Administrationstools unter Win32-Systemen gehen Sie wie folgt vor:

- Starten Sie das Setup-Programm für die Treiber Ihres KOBIL-Chipkartenterminals über `/Treiber-Setup/KOBILTreiberSetup.exe`
- Folgen Sie den Anweisungen des Setup-Programms und schließen Sie das Chipkartenterminal an wenn Sie dazu aufgefordert werden. Das Chipkartenterminal wird benötigt um den **KOBIL SecOVID** Server per Remoteconsole zu administrieren. Für die lokale Administration des **KOBIL SecOVID** Server wird das KOBIL-Chipkartenterminal nicht be-

nötigt.

Zur Installation des **KOBIL SecOVID** Administrationstools muss das Setup-Programm `/win32/admin/Setup_admintools.exe`, der Installations-CD, gestartet werden. Bitte folgen Sie bei der Installation den weiteren Anweisungen des Setup-Programms.

Starten des KOBIL SecOVID Administrationstools

Das **KOBIL SecOVID** Administrationstool wird über das Menü **Start** -> **Programme** -> **SecOVID Admintools** -> **WxOvid** gestartet. Nach dem ersten Start des **SecOVID Admintools** können die geheimen Tokendaten importiert und zur SecOVID-Datenbank hinzugefügt werden. Bei einer SecOVID Teststellung liegen die Tokendaten im Klartext vor. Wenn Sie die SecOVID Tokens gekauft haben, werden die Tokendaten in der Regel verschlüsselt geliefert. Der Import der Tokendaten (z. B. `tokendaten_firma.db`) erfolgt über das Menü **Sonstige Token** -> **Token importieren**.

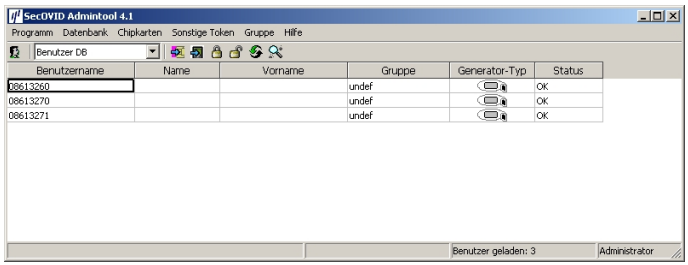


Abb. 40: Starten des **KOBIL SecOVID** *Admintools*

Personalisierung der Token

Zur Zuweisung der Token an einen Benutzer müssen die Tokendatensätze gesperrt werden. Nach dem vorübergehenden Sperren eines Tokendatensatzes können durch das Editieren des Eintrags die Benutzerinformationen hinterlegt werden. Die Information im Feld **Benutzername** wird nach erfolgter Konfiguration am **bintec Secure IPSec Client** zur Erweiterten IPSec-Authentifizierung verwendet.

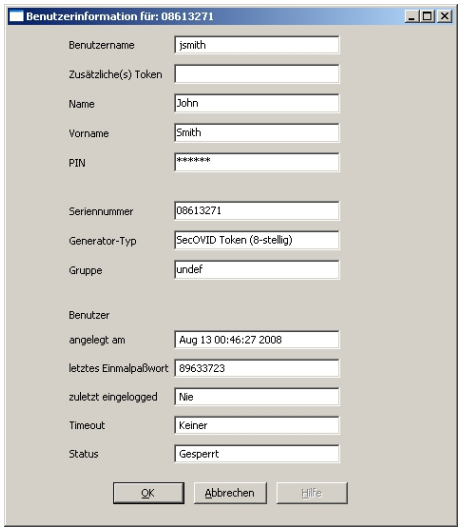


Abb. 41: Benutzerinformation

Anschließend muss die Sperrung des Datensatzes rückgängig gemacht werden.

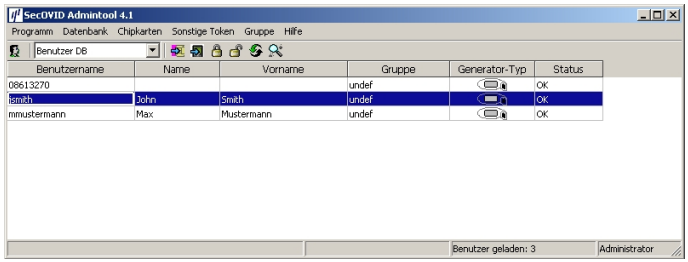


Abb. 42: Sperrung aufheben

Erster Funktionstest

Ein erster Funktionstest kann mit dem Kommandozeilen Tool `radping.exe` durchgeführt werden. `Radping` initiert mit dem Einmal-Passwort eine Authentifizierungsanfrage an den SecOVID RADIUS-Server. Das Tool wurde während der Installation im Verzeichnis \etc\SecOVID\ hinterlegt. Mit der Option `-u` wird dem SecOVID Server der Benutzername und das One-Time-Passwort übergeben. Das Einmal-Passwort muss mit dem Token des Benutzers generiert werden. Mit der Option `-S` wird der SecOVID Server angesprochen. Für den ersten Funktionstest muss `radping` direkt auf dem Server ausgeführt werden. Mit der Option `-k` wird das RADIUS-Passwort übergeben. Der default Wert ist *`geheim`*. Das SecOVID Logfile (`\etc\SecOVID\ovid.proto`) gibt bei einer erfolgreichen Authentifizierung folgende Meldung aus:

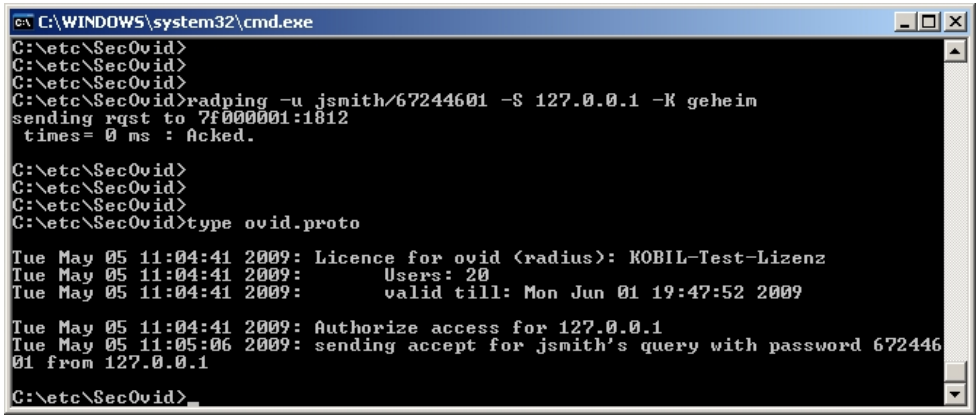


Abb. 43: Funktionstest

Konfiguration des RADIUS-Clients am SecOVID Server

Alle RADIUS-Clients (z. B. das bintec VPN-Gateway oder die Testapplikation `radping`) müssen am SecOVID Server als RADIUS-Client hinterlegt werden. Dazu wird die Konfigurationsdatei `\etc\SecOVID\clients` bearbeitet. In unserem Beispiel wird das bintec VPN-Gateway mit der IP-Adresse `192.168.0.30` und dem RADIUS-Passowort `radius_PWD` hinzugefügt. Dieses Passwort wird später auch am VPN-Gateway in den RADIUS-Einstellungen hinterlegt. Damit die Änderungen wirksam werden, muss der Dienst SecOVID Server neu gestartet werden.

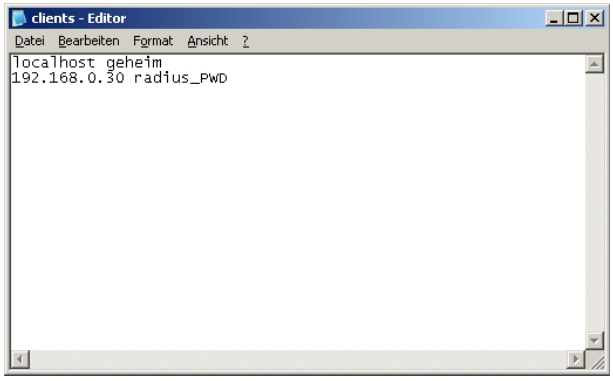


Abb. 44: Clients-Editor

3.2.2 Konfiguration des VPN-Gateways

Lokale IP-Adresse des VPN-Gateways

Das VPN-Gateway wird in unserem Beispiel mit der IP-Adresse *192.168.0.30* betrieben. Um dem **bintec Secure IPSec Client** eine IP-Adresse aus diesem Netzwerkbereich zuweisen zu können muss die Option **Proxy ARP** aktiviert werden.

Gehen Sie dazu in folgendes Menü:

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

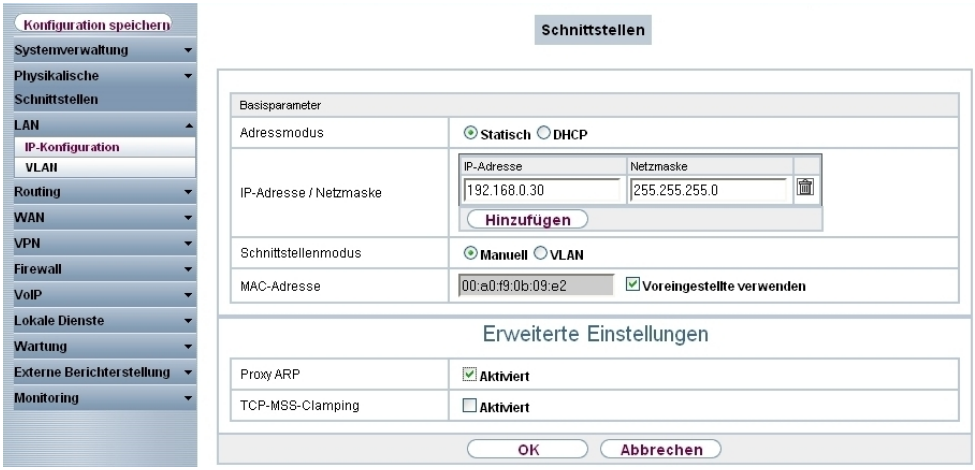


Abb. 45: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**

Relevante Felder im Menü Schnittstellen

Feld	Beschreibung
IP-Adresse / Netzmaske	Fügen Sie mit **Hinzufügen** einen neuen Adresseintrag hinzu und geben Sie die **IP-Adresse** und die entsprechende **Netzmaske** der Schnittstelle ein.
Proxy ARP	Aktivieren Sie die Option **Proxy ARP**.

RADIUS-Einstellungen

Mit den Einstellungen im Menü **RADIUS** wird die erweiterte IPSec-Authentifizierung (XAuth) mit dem RADIUS-Server des **KOBIL SecOVID** Servers aktiviert. Es ist notwendig den Authentifizierungstyp auf den Wert *XAUTH* zu setzen sowie die IP-Adresse des **KOBIL SecOVID** Servers zu hinterlegen. Die Kommunikation mit dem RADIUS-Server wird mit einem Passwort geschützt. Bitte verwenden Sie hier das am SecOVID Server hinterlegte RADIUS-Passwort (Konfigurationsdatei `\etc\SecOVID\clients`).

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS**.

Abb. 46: **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS**

Relevante Felder im Menü RADIUS

Feld	Beschreibung
Authentifizierungstyp	Wählen Sie den **Authentifizierungstyp** *XAUTH* aus.
Server-IP-Adresse	Geben Sie die **Server-IP-Adresse** des **KOBIL SecOVID** Servers ein.
RADIUS-Passwort	Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort ein, hier z. B. *radius_PWD*.
Gruppenbeschreibung	Definieren Sie eine neue RADIUS-Gruppenbeschreibung bzw. weisen Sie den neuen RADIUS-Eintrag einer schon definierten Gruppe zu. Die konfigurierten RADIUS-Server einer Gruppe werden gemäß der **Priorität** und der **Richtlinie** abgefragt. Mögliche Werte: • *Neu* (Standardwert): Tragen Sie in das Textfeld eine neue Gruppenbeschreibung ein • <Gruppenname>: Wählen Sie aus der Liste eine schon definierte Gruppe aus, z. B. *xauth*.

VPN-Konfiguration

Im Menü **IP Pools** wird ein IP-Adress-Pool spezifiziert aus dem allen VPN-Clients beim Aufbau des Tunnels eine Adresse zugewiesen wird. In unserem Beispiel wird ein Bereich aus dem lokalen Netzwerk gewählt z. B. `192.168.0.150` bis `192.168.0.180`.

(1) Gehen Sie zu **VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**.

Abb. 47: **VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**

Relevante Felder im Menü IP Pools

Feld	Bedeutung
IP-Poolname	Geben Sie die Bezeichnung des IP Pools ein.
IP-Poolbereich	Geben Sie im ersten Feld die erste IP-Adresse aus dem lokalen Netzwerk ein. Geben Sie im zweiten Feld die letzte IP-Adresse aus dem lokalen Netzwerk ein.

XAUTH-Konfiguration

Für die Erweiterte IPSec-Authentifizierung (XAuth) soll ein RADIUS-Server verwendet werden. Die hierfür notwendigen Einstellungen werden im Menü **XAUTH-Profile** vorgenommen.

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

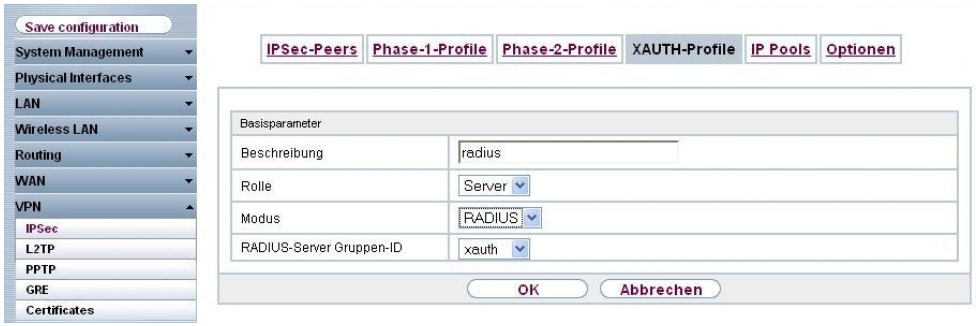


Abb. 48: **VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**

Relevante Felder im Menü XAUTH-Profile

Feld	Bedeutung
Beschreibung	Geben Sie eine Beschreibung für die IPSec-Authentifizierung ein, z. B. `radius`.
Rolle	Wählen Sie hier `Server` aus.
Modus	Bei **Modus** wählen Sie `RADIUS` aus.
RADIUS-Server Gruppen-ID	Wählen Sie den RADIUS-Server `xauth` aus.

IPSec-Peers-Konfiguration

Im Menü **IPSec-Peers** wird eine Multiuser VPN-Verbindung angelegt die den Verbindungsaufbau mehrerer **bintec Secure IPSec Clients** ermöglicht. Wenn die Multiuser VPN IPsec-Verbindung mit Preshared-Keys Authentifiziert werden soll, wird auf allen **bintec Secure IPsec Clients** der gleiche Preshared-Key verwendet. Bei den Multiuser VPN-Verbindungen wird im Feld **Peer ID** keine ID-Information hinterlegt.

Wählen Sie die Schaltfläche **Neu**, um den IPSec-Peer einzurichten.

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

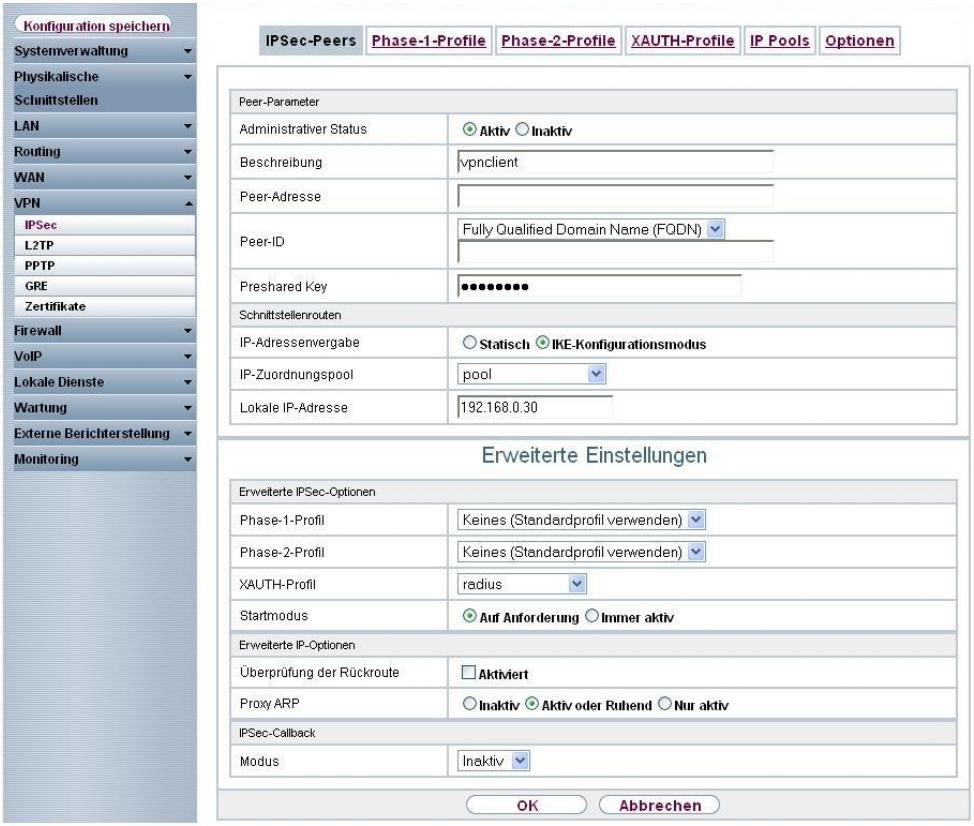


Abb. 49: **VPN** -> **IPSec** -> **IPSec-Peers** ->

Relevante Felder im Menü IPSec-Peers

Feld	Bedeutung
Administrativer Status	Stellen Sie den Administrativen Status auf **Aktiv**. Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung.
Beschreibung	Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert.
Peer-ID	Wählen Sie den ID-Typ aus. Mögliche ID-Typen: • Full Qualified Domain Name (FQDN) • E-Mail-Adresse • IVP4-Adresse • ASN.1-DN (Distinguished Name)
Preshared Key	Bei **Preshared Key** geben Sie das mit dem Peer vereinbarte

Feld	Bedeutung
	Passwort ein.
IP-Adressenvergabe	Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Bei Auswahl der Option *IKE-Konfigurationsmodus* wählen Sie eine IP-Adresse aus dem konfigurierten IP-Pool aus.
IP-Zuordnungspool	Wählen Sie einen im Menü **VPN** -> **IP Pools** konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung *Noch nicht definiert*.
Lokale IP-Adresse	Geben Sie die WAN IP-Adresse Ihrer IPSec-Verbindung an. Es kann die gleiche IP-Adresse sein, die als LAN IP-Adresse an Ihrem Router konfiguriert ist.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Bedeutung
Phase-1-Profil	Mit Auswahl von *Keines (Standardprofil verwenden)* wird das in **Phase-1-Profile** als Standard markiertes Profil verwendet.
Phase-2-Profil	Mit Auswahl von *Keines (Standardprofil verwenden)* wird das in **Phase-2-Profile** als Standard markiertes Profil verwendet.
XAUTH-Profil	Wählen Sie hier ein konfiguriertes XAUTH-Profil (z. B. *radius*) aus.
Startmodus	Hier können Sie auswählen, wie der Peer in den aktiven Zustand versetzt werden soll. Mit Auswahl von *Auf Anforderung* wird der Peer durch einen Trigger in den aktiven Zustand versetzt.
Überprüfung der Rückroute	Hier wird festgelegt, ob für die Schnittstelle zum Verbindungspartner eine Überprüfung der Rückroute aktiviert werden soll.
Proxy ARP	Stellen Sie **Proxy ARP** auf *Aktiv oder Ruhend*. Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer aktiv oder ruhend ist. Bei *ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will.
Modus	Stellen Sie den **Modus** des **IPSec-Callback** auf *Inaktiv*. Das lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch in-

Feld	Bedeutung
	itiiert es ISDN-Rufe zum entfernten Gerät.

Phase-1-Profile

Im Menü **Phase-1-Profile** wird der Aggressive Modus aktiviert und der **Lokaler ID-Wert** des VPN-Gateways gesetzt. Klicken Sie auf das -Symbol, um vorhanden Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Profile hinzuzufügen.

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

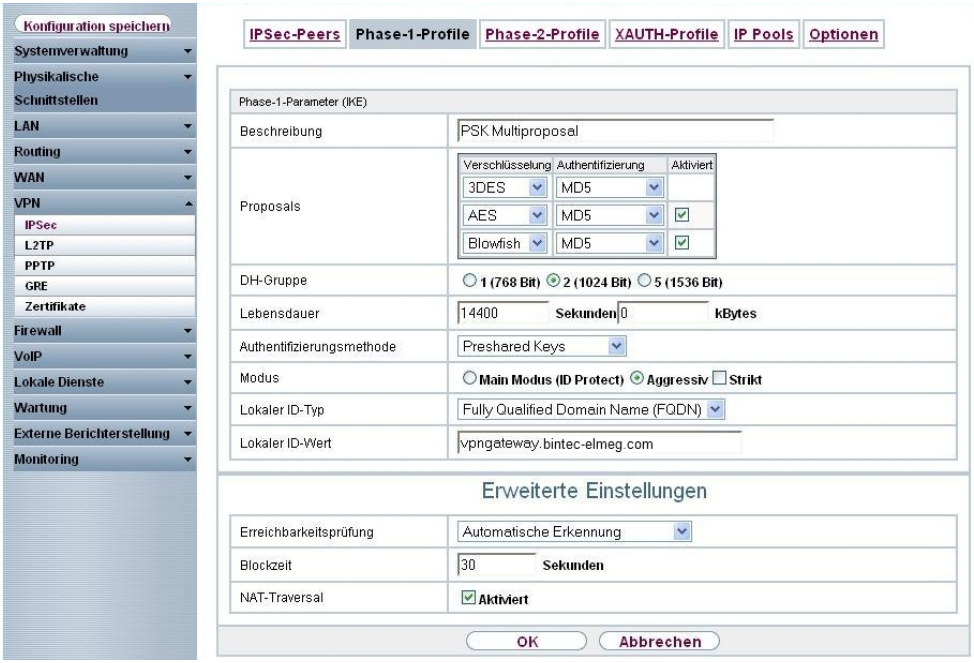


Abb. 50: **VPN** -> **IPSec** -> **Phase-1-Profile** -> **Bearbeiten**

Relevante Felder im Menü Phase-1-Profile

Feld	Bedeutung
Modus	Wählen Sie den Phase-1-Modus `Aggressiv` aus. Der Aggressive Modus ist erforderlich, falls einer der Peers keine statische IP-Adresse hat und Preshared Keys für die Authentifizierung genutzt werden; er erfordert nur drei Meldungen für die Einrichtung eines sicheren Kanals.
Lokaler ID-Wert	Geben Sie die ID des VPN-Gateways ein, z. B. `vpngate-`

Feld	Bedeutung
	way.bintec-elmeg.com

Phase-2-Profile

Die Einstellungen im Menü **VPN** -> **IPSec** -> **Phase-2-Profile** -> **Bearbeiten** können unverändert übernommen werden.

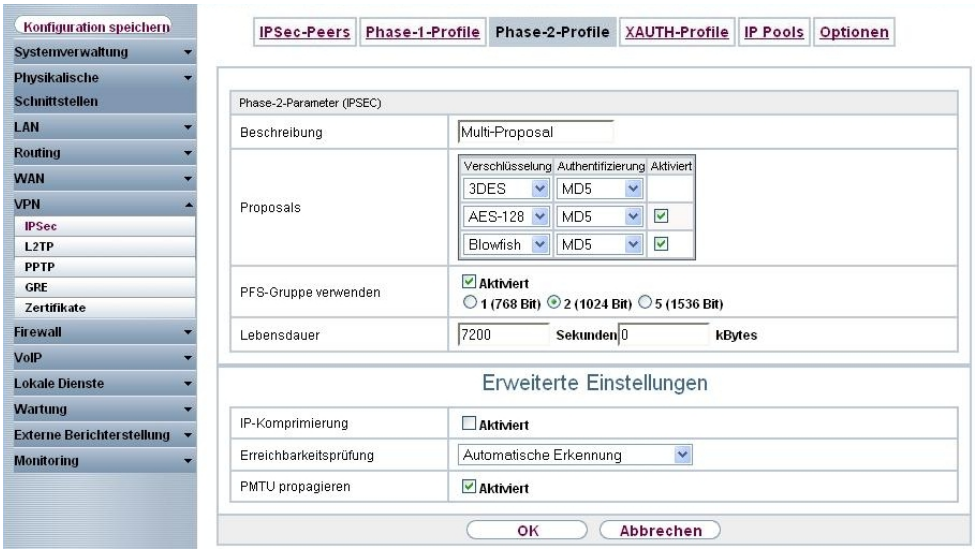


Abb. 51: **VPN** -> **IPSec** -> **Phase-2-Profile** -> **Bearbeiten**

3.2.3 Konfiguration des bintec Secure IPSec Clients

Der **bintec Secure IPSec Client** wird über **Start** -> **Programme** -> **FEC Secure IPSec Client** -> **Secure Client Modus** aufgerufen. Die Konfiguration des **bintec Secure IPSec Clients** wird über den Assistenten durchgeführt. Beim ersten Start des **bintec Secure IPSec Clients** wird der **Assistent für neues Profil** automatisch gestartet.

Wählen Sie die Auswahl **Verbindung zum Firmennetz über IPSec** aus.

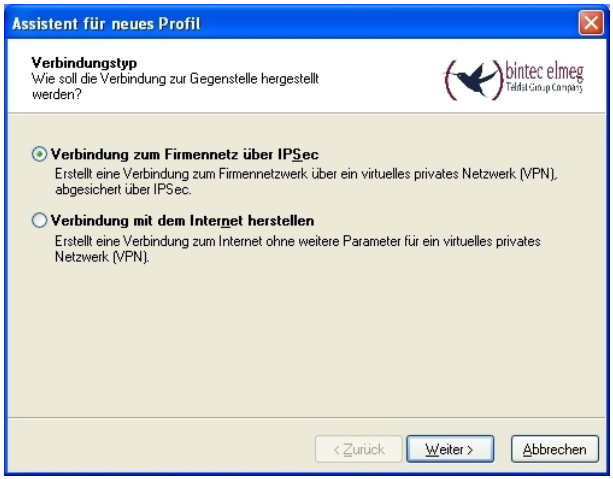


Abb. 52: Verbindungstyp

Geben Sie einen Namen für das Profil ein z. B. `Zentrale`.

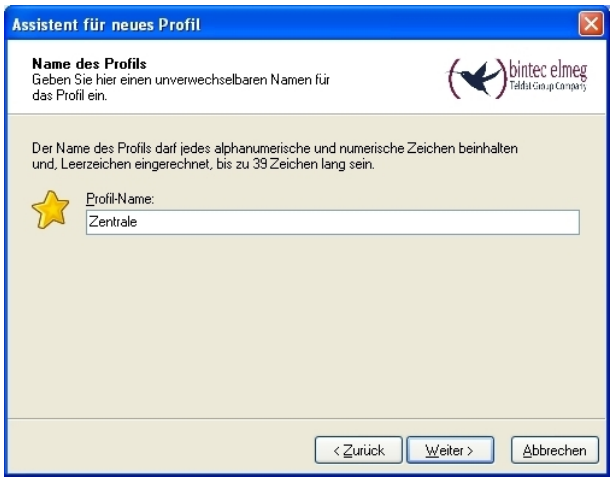


Abb. 53: Profil-Name

Im nächsten Schritt des Assistenten muss ein **Verbindungsmedium** ausgewählt werden über welches eine Verbindung zum Internet aufgebaut wird. In unserem Beispiel wird die Auswahl `LAN (over IP)` verwendet da der **bintec Secure IPSec Client** keinen direkten Zugang zum Internet herstellt sondern einen Internetzugangsrouter verwendet.

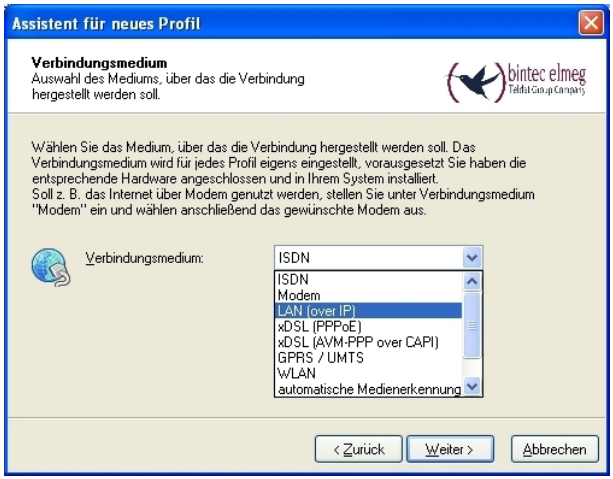


Abb. 54: Verbindungsmedium

Bei der Option **Gateway (Tunnel-Endpunkt)** wird die Adresse hinterlegt über die das VPN-Gateway aus dem Internet erreichbar ist. Aktivieren Sie die Option *Erweiterte Authentifizierung (XAUTH)* um den Benutzername und das Passwort an den **KOBIL SecOVID** Server zu übermitteln.

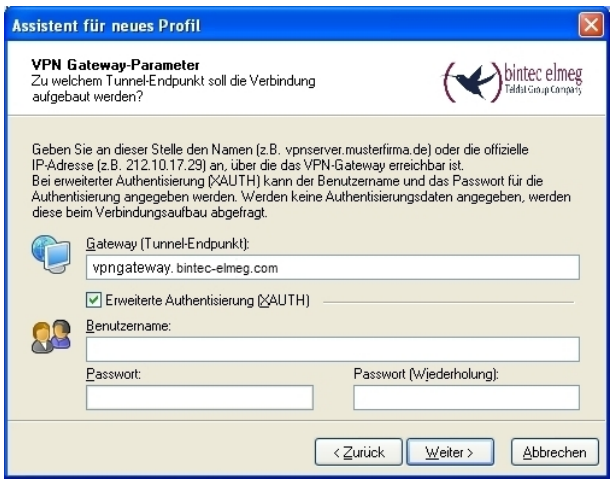


Abb. 55: VPN Gateway Parameter

Anschließend wird als **Austausch-Modus** der *Aggressive Mode* verwendet, da dem **bintec R3000** Gateway und dem **bintec Secure IPSec Client** dynamische IP-Adresse vom Provider zugewiesen werden. Die **PFS-Gruppe** setzen Sie z. B. auf *DH-Gruppe 2 (1024 Bit)*. Die Option *Benutze IP-Kompression* wird in dieser Konfiguration nicht eingesetzt.

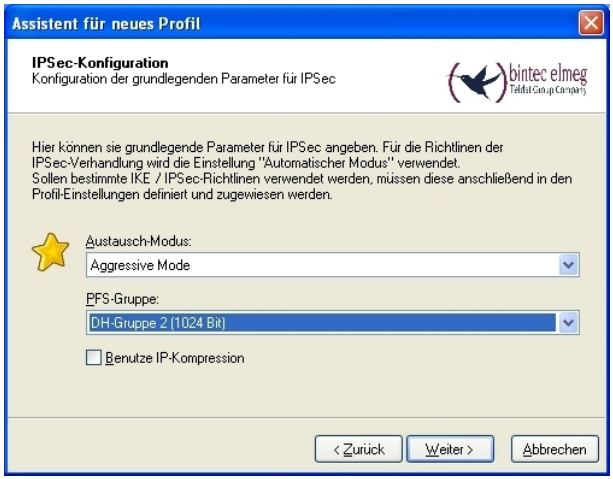


Abb. 56: IPSec-Konfiguration

Im nächsten Schritt des Assistenten wird der am VPN-Gateway konfigurierte **Preshared Key** hinterlegt. Als **Lokale Identität** soll die E-Mail-Adresse des Benutzers mit dem **Type** `Fully Qualified Username` verwendet werden.

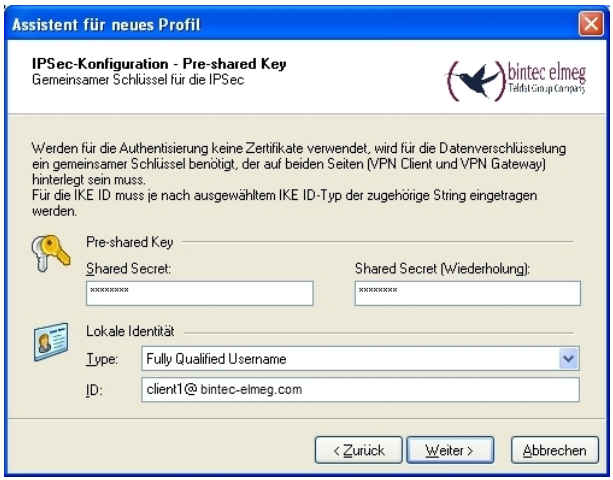


Abb. 57: Pre-shared Key

In diesem Beispiel wird dem VPN IPSec-Client eine dynamische VPN IP-Adresse zugewiesen. Dazu muss die Option `IKE Config Mode verwenden` ausgewählt werden.

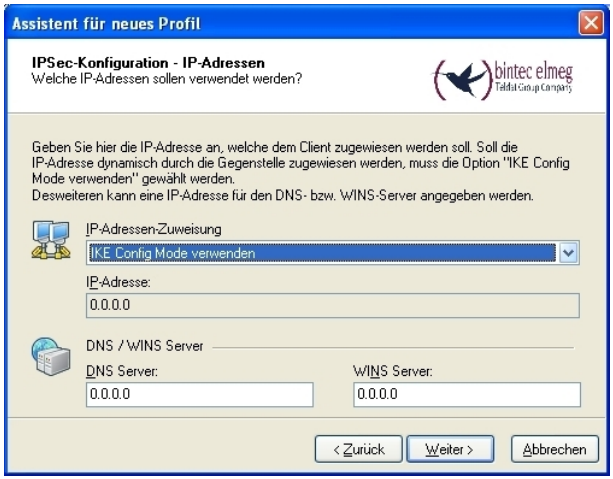


Abb. 58: IKE Config Mode

Im letzten Schritt wird die **Firewall** des **bintec Secure IPSec Clients** konfiguriert. Wenn der Client direkt mit dem Internet verbunden ist, sollte die Firewall aktiviert sein.

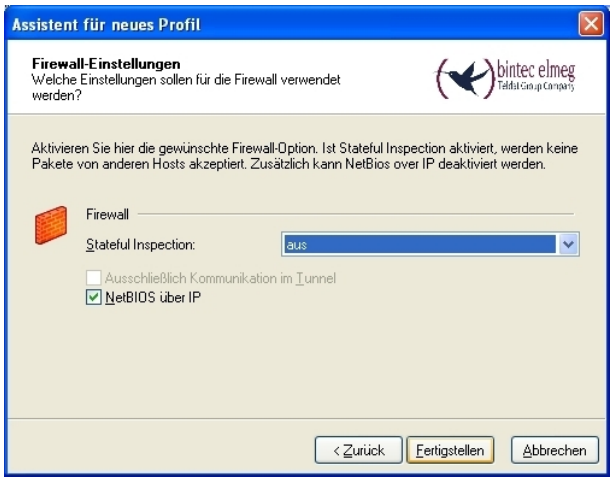


Abb. 59: Firewall

Beim Aufbau des VPN-Tunnels erscheint am **bintec Secure IPSec Client** eine **User-ID** und **Password** Abfrage. Hier wird der im SecOVID Admintool hinterlegte Benutzername und das mit dem **KOBIL SecOVID** Token generierte Einmal-Passwort abgefragt.

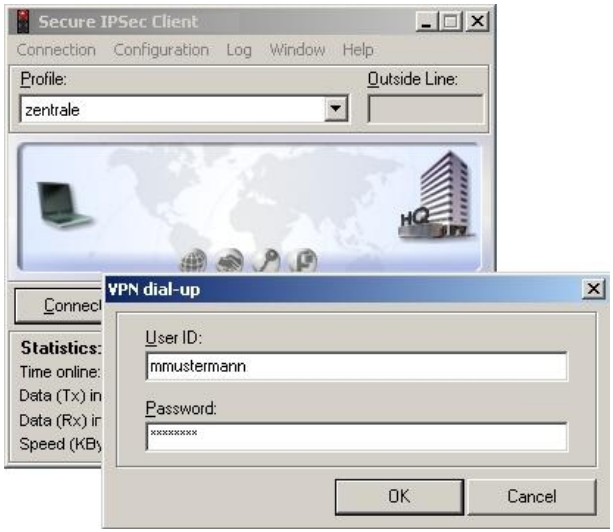


Abb. 60: User-ID / Password Abfrage

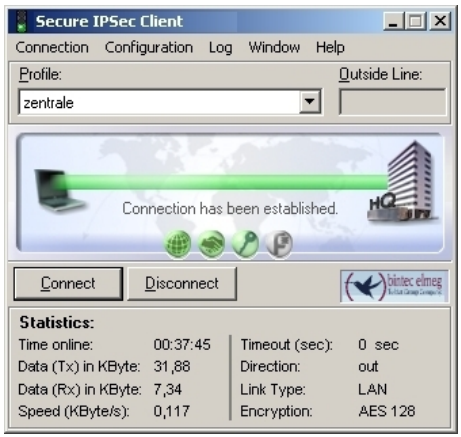


Abb. 61: FEC Secure IPSec Client

3.3 Konfigurationsschritte im Überblick

Konfiguration des VPN Gateways

Feld	Menü	Wert
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Statisch*
IP-Adresse / Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	z. B. *192.168.0.30* / *255.255.255.0*
Schnittstellenmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Manuell*
Proxy ARP	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Aktiviert*

RADIUS-Einstellungen

Feld	Menü	Wert
Authentifizierungstyp	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	*XAUTH*
Server-IP-Adresse	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *192.168.0.111*
RADIUS-Passwort	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *radius_PWD*
Gruppenbeschreibung	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	*xauth*

VPN Konfiguration

Feld	Menü	Wert
IP-Poolname	**VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**	z. B. *pool*
IP-Poolbereich	**VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**	z. B. *192.168.0.150* - *192.168.0.180*

XAUTH Konfiguration

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	z. B. *radius*
Rolle	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	*Server*
Modus	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	*RADIUS*
RADIUS-Server	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	*xauth*

Feld	Menü	Wert
Gruppen -ID		

IPSec-Peers Konfiguration

Feld	Menü	Wert
Administrativer Status	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*Aktiv*
Beschreibung	**VPN** -> **IPSec** -> **IPSec-Peers** ->	z. B. *vpnclient*
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*Fully Qualified Domain Name (FQDN)*
Preshared Key	**VPN** -> **IPSec** -> **IPSec-Peers** ->	z. B. *bintec elmeg*
IP-Adressenvergabe	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*IKE-Konfigurationsmodus*
IP-Zuordnungspool	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*pool*
Lokale IP-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** ->	z. B. *192.168.0.30*
Phase-1-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Keines (Standardprofil verwenden)*
Phase-2-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Keines (Standardprofil verwenden)*
XAUTH-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*radius*
Startmodus	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Auf Anforderung*
Überprüfung der Rückroute	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Deaktiviert*
Proxy ARP	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Aktiv oder Ruhend*
Modus	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Inaktiv*

Phase-1-Profile Konfiguration

Feld	Menü	Wert
Modus	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Bearbeiten**	*Aggressiv*

Feld	Menü	Wert
Lokaler ID-Wert	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Bearbeiten**	z. B. *vpngateway.bintec-elmeg.com*

Konfiguration des bintec Secure IPSec Clients

Feld	Menü	Wert
Verbindungstyp	**Assistent für neues Profil**	*Verbindung zum Firmennetz über IPSec*
Profil-Name	**Assistent für neues Profil**	*Zentrale*
Verbindungsmedium	**Assistent für neues Profil**	*LAN (over IP)*
Gateway (Tunnel-Endpunkt)	**Assistent für neues Profil**	z. B. *vpngateway.bintec-elmeg.com*
Erweiterte Authentifizierung (XAUTH)	**Assistent für neues Profil**	Aktiviert
Austausch-Modus	**Assistent für neues Profil**	Aggressive Mode
PFS-Gruppe	**Assistent für neues Profil**	DH-Gruppe 2 (1024 Bit)
Shared Secret	**Assistent für neues Profil**	z. B. *bintec elmeg*
Shared Secret (Wiederholung)	**Assistent für neues Profil**	z. B. *bintec elmeg*
Typ	**Assistent für neues Profil**	z. B. *Fully Qualified Username*
ID	**Assistent für neues Profil**	z. B. *client1@bintec-elmeg.com*
IP-Adressen-Zuweisung	**Assistent für neues Profil**	*IKE Config Mode verwenden*
Stateful Inspection	**Assistent für neues Profil**	*aus*
NetBIOS über IP	**Assistent für neues Profil**	Aktiviert

Kapitel 4 Sicherheit - Zertifikatsbasierte VPN IPSec mit optionaler KOBIL SecOVID One-Time-Passwort Abfrage

4.1 Einleitung

Dieses Kapitel beschreibt eine zertifikatsbasierte VPN IPSec-Anbindung des **bintec Secure IPsec Clients** an ein **bintec R3000** VPN-Gateway. Es wird eine eigene Zertifizierungsstelle (OpenSSL CA) aufgebaut welche die notwendigen Zertifikate im PKCS#12 Format erstellt. Beim Aufbau des VPN-Tunnels wird dem **bintec Secure IPSec Client** (per IKE Config Mode) eine dynamische IP-Adresse zugewiesen. Die Lösung kann optional mit einer One-Time-Passwort Abfrage erweitert werden. Dabei wird mit einem **KOBIL SecOVID** Token ein One-Time-Passwort generiert das am **KOBIL SecOVID** Server Authentifiziert wird.

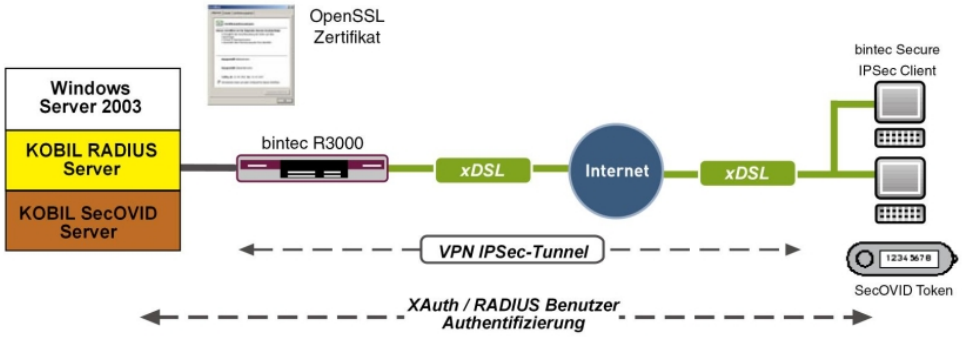


Abb. 62: Beispielszenario

Voraussetzungen

- Ein bintec VPN -Gateway z. B. **bintec R3000** mit Systemsoftware 7.8.7 (XAuth-Unterstützung)
- Ein **bintec Secure IPsec Client**
- VPN-Gateway und VPN-Client benötigen jeweils eine unabhängige Verbindung zum Internet
- Optional ein **KOBIL SecOVID** Server, der auf einem Microsoft Windows Rechner installiert wird (z. B. Server 2003 (32Bit))

4.2 Konfiguration

4.2.1 Einrichten der OpenSSL Zertifizierungsstelle

Die Zertifikate zur VPN IPSec-Authentifizierung werden in diesem Beispiel mit der in OpenSSL mitgelieferten DemoCA erstellt. Hier wird die OpenSSL Version 0.9.8g verwendet. Zur Erstellung der Zertifizierungsstelle und Generierung der Zertifikate wird das in OpenSSL mitgelieferte Script `CA.sh` genutzt (zu finden bei Debian unter `/usr/lib/ssl/misc/CA.sh`). Das Kommando zum Erstellen einer neuen Zertifizierungsstelle `CA.sh -newca` muss nur einmal ausgeführt werden. Auf Basis dieser Zertifizierungsstelle werden die Benutzerzertifikate erstellt und im PKCS#12 Format exportiert.

Wenn die OpenSSL Standardeinstellungen (`openssl.cnf`) verwendet werden, wird beim erstellen einer neuen Zertifizierungsstelle ein Verzeichnis `demoCA` erstellt das folgende Informationen enthält:

`private/cakey.pem`	privater Schlüssel der Zertifizierungsstelle (CA)
`cacert.pem`	selbstzertifziertes Zertifikat der Zertifizierungsstelle (CA
`index.txt`	Liste der bereits ausgestellten Zertifikate
`serial`	Seriennummer für das nächste Zertifikat
`newcerts`	Verzeichnis für erstellte Zertifikate

Im Folgenden wird ein Beispiel zum Erstellen einer neuen Zertifizierungsstelle mittels OpenSSL bzw. dem Script `CA.sh -newca` gezeigt:

```
root@server:/usr/lib/ssl/misc# ./CA.sh -newca
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 1024 bit RSA private key
.....................................................................++++++
.................................++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:bavaria
Locality Name (eg, city) []:nuernberg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:funkwerk-ec
Organizational Unit Name (eg, section) []:dev
Common Name (eg, YOUR name) []:demo
Email Address []:demo@funkwerk-ec.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 0 (0x0)
        Validity
            Not Before: Jun  8 07:52:39 2009 GMT
            Not After : Jun  7 07:52:39 2012 GMT
        Subject:
            countryName               = DE
            stateOrProvinceName       = bavaria
            organizationName          = funkwerk-ec
            organizationalUnitName    = dev
            commonName                = demo
            emailAddress              = demo@funkwerk-ec.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                8C:4A:25:72:E5:43:B2:B0:44:1C:F6:E8:5C:6C:FC:58:DA:90:12:13
            X509v3 Authority Key Identifier:
                keyid:8C:4A:25:72:E5:43:B2:B0:44:1C:F6:E8:5C:6C:FC:58:DA:90:12:13
                DirName:/C=DE/ST=bavaria/O=funkwerk-ec/OU=dev/CN=demo/emailAddress=demo@funkwerk-ec.com
                serial:00

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Jun  7 07:52:39 2012 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
root@server:/usr/lib/ssl/misc#
```

4.2.2 Erstellung der Benutzerzertifikate

Nach dem Erstellen der Zertifizierungsstelle (CA) können die Benutzerzertifikate des VPN-Gateways und die der VPN-Clients erstellt werden. Zum Generieren eines Benutzerzertifikats sind je drei Schritte notwendig:

(a) Erstellung eines neuen Schlüssels sowie einer Zertifikatsanforderung (`CA.sh -newreq`)

(b) Signierung der Zertifikatsanforderung mit der Zertifizierungsstelle (`CA.sh -sign`)

(c) Export der Zertifikate (CA Zertifikat und Kunden Zertifikat) incl. Schlüssel (public und private Key des Kunden) im PKCS#12 Format mittels OpenSSL.

Im ersten Schritt wird mit dem Kommando `CA.sh -newreq` ein neuer Zertifikatsschlüssel und eine Zertifikatsanforderung, erstellt:

`newkey.pem` = RSA Key Pair (public und private Key)

`newreq.pem` = Zertifikatsanforderung (enthält den public key sowie die notwendigen Daten zur Zertifikatsanforderung)

Im zweiten Schritt wird diese Zertifikatsanforderung mit dem Befehl `CA.sh -sign` von der Zertifizierungsstelle signiert. Dadurch wird die Datei `newcert.pem` erstellt. Nun sollte ein separater Ordner erstellt werden in dem der Zertifikatsschlüssel, die Zertifikatsanforderung und das signierte Zertifikat aufbewart werden:

- erstellen Sie einen neuen Ordner `mkdir ./vpn-gateway`
- kopieren Sie die temporären Dateien in den Ordner
- verschieben Sie folgende Dateien in diesen Ordner

  mv newreq.pem vpn-gateway/hinz_req.pem

  mv newkey.pem vpn-gateway/hinz_key.pem

  mv newcert.pem vpn-gateway/hinz_cert.pem

Im dritten Schritt wird das Zertifikat der Zertifizierungsstelle, das eben erstellte Benutzerzertifikat inklusive der Zertifikatsschlüssel in einer Datei im PKCS#12 Format exportiert. Diese Datei wird mit einem Passwort geschützt und ermöglicht die Übertragung der Zertifikate an das VPN-Gateway bzw. an einen VPN-Client. Folgendes Kommando wird dafür verwendet:

```
openssl pkcs12 -export -in vpn-gateway/newcert.pem -inkey vpn-
gateway/newkey.pem -certfile demoCA/cacert.pem -name vpn-gateway -
out vpn-gateway/vpn-gateway1.p12
```

Die beschriebenen Schritte zum Erstellen eines Benutzerzertifikats werden am Beispiel des Zertifikats, welches für das VPN-Gateway erstellt wird, gezeigt.

Diese drei Schritte müssen analog für jeden der **bintec Secure IPsec Clients** durchgeführt werden.

Erstellung eines neuen Schlüssels sowie einer Zertifikatsanforderung:

```
root@server:/usr/lib/ssl/misc# ./CA.sh -newreq
Generating a 1024 bit RSA private key
.++++++
.........................++++++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:bavaria
Locality Name (eg, city) []:nuernberg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:fec
Organizational Unit Name (eg, section) []:dev
Common Name (eg, YOUR name) []:vpn-gateway
Email Address []:vpn-gateway@funkwerk-ec.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request is in newreq.pem, private key is in newkey.pem
root@tp2h1:/usr/lib/ssl/misc#
```

Signierung der Zertifikatsanforderung mit der Zertifizierungsstelle:

```
root@server:/usr/lib/ssl/misc# ./CA.sh -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jun  8 08:54:05 2009 GMT
            Not After : Jun  8 08:54:05 2010 GMT
        Subject:
            countryName               = DE
            stateOrProvinceName       = bavaria
            localityName              = nuernberg
            organizationName          = fec
            organizationalUnitName    = dev
            commonName                = vpn-gateway
            emailAddress              = vpn-gateway@funkwerk-ec.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                48:65:44:7A:45:B4:68:03:8C:C9:00:67:E2:E5:54:E2:7B:7D:4A:5B
            X509v3 Authority Key Identifier:
                keyid:8C:4A:25:72:E5:43:B2:B0:44:1C:F6:E8:5C:6C:FC:58:DA:90:12:13

Certificate is to be certified until Jun  8 08:54:05 2010 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, ST=bavaria, O=funkwerk-ec, OU=dev, CN=demo/emailAddress=demo@funkwerk-ec.com
        Validity
            Not Before: Jun  8 08:54:05 2009 GMT
            Not After : Jun  8 08:54:05 2010 GMT
        Subject: C=DE, ST=bavaria, L=nuernberg, O=fec, OU=dev,
CN=vpn-gateway/emailAddress=vpn-gateway@funkwerk-ec.com
        Subject Public Key
```

```
Info:
            Public Key Algorithm:
rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):

00:dc:de:3f:5f:f8:09:08:3b:a0:4d:9d:3d:c2:70:

02:98:ac:68:1d:4f:f9:47:b4:2c:6b:68:6e:a6:b2:

4a:87:16:57:29:e7:d7:83:b5:5e:c6:ba:44:34:03:

2b:90:f3:e9:7a:b2:3b:9c:99:70:ba:f6:55:27:eb:

51:5c:f7:5d:a7:bc:46:12:9e:24:f8:ba:3c:c1:37:

87:ef:a6:ec:62:9c:fc:5b:f6:3e:4d:27:db:11:54:

8d:38:39:8a:79:eb:86:cd:3e:55:77:2d:94:ef:59:

15:4c:32:36:8a:9b:08:0d:23:36:20:0f:e8:50:7a:
                    43:5a:2f:0d:3b:77:0b:8e:59
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                48:65:44:7A:45:B4:68:03:8C:C9:00:67:E2:E5:54:E2:7B:7D:4A:5B
            X509v3 Authority Key Identifier:
                keyid:8C:4A:25:72:E5:43:B2:B0:44:1C:F6:E8:5C:6C:FC:58:DA:90:12:13

    Signature Algorithm: sha1WithRSAEncryption
        a0:2b:df:23:6b:5a:4e:ac:4d:71:b8:b7:ca:ad:3e:49:4c:55:
        72:14:e0:a0:1f:d5:21:3e:f3:98:0a:51:86:fe:c2:02:2b:81:
        88:76:cd:69:a3:88:75:ed:c2:5c:43:64:14:cc:9e:b1:c8:88:
        ee:b0:e7:f4:c5:b4:2f:a0:b5:55:e9:61:1b:9d:ec:7a:25:95:
        a7:d8:53:65:7a:04:f3:b7:b8:7a:f3:af:62:88:46:b9:a6:a3:
        48:93:a9:d4:ff:2b:4e:3c:3b:d4:74:cc:45:dd:c4:30:8e:c6:
        de:ac:e0:57:b3:ae:7b:03:f8:aa:c8:cc:34:0c:45:ef:8a:8d:
        93:66

-----BEGIN CERTIFICATE-----
MIIC+jCCAmOgAwIBAgIBATANBgkqhkiG9w0BAQUFADB3MQswCQYDVQQGEwJERTEQ
MA4GA1UECBMHYmF2YXJpYTEUMBIGA1UEChMLZnVua3dlcmstZWMxDDAKBgNVBAsT
A2RldjENMAsGA1UEAxMEZGVtbzEjMCEGCSqGSIb3DQEJARYUZGVtb0BmdW5rd2Vy
ay1lYy5jb20wHhcNMDkwNjA4MDg1NDA1WhcNMTAwNjA4MDg1NDA1WjCBkTELMAkG
A1UEBhMCREUxEDAOBgNVBAgTB2JhdmFyaWExEjAQBgNVBAcTCW51ZXJuYmVyZzEM
MAoGA1UEChMDZmVjMQwwCgYDVQQLEwNkZXYxFDASBgNVBAMTC3Zwbi1nYXRld2F5
MSowKAYJKoZIhvcNAQkBFht2cG4tZ2FOZXdheUBmdW5rd2Vyay1lYy5jb20wgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANzeP1/4CQg7oE2dPcJwApisaB1P+UeO
LGtobqaySocWVynn14O1Xsa6RDQDK5Dz6XqyO5yZcLr2VSfrUVz3Xae8RhKeJPi6
PME3h++m7GKc/Fv2PkOn2xFUjTg5innrhs0+VXctlO9ZFUwyNoqbCAOjNiAP6FB6
Q1ovDTt3C45ZAgMBAAGjezB5MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9w
ZW5TUOwgR2VuZXJhdGVkIEN1cnRpZmljYXRlMBOGA1UdDgQWBBRIZUR6RbRoA4zJ
AGfi5VTie31KWzAfBgNVHSMEGDAWgBSMSiVy5UOysEQc9uhcbPxY2pASEzANBgkq
hkiG9w0BAQUFAAOBgQCgK98ja1pOrE1xuLfKrT5JTFVyFOCgH9UhPvOYC1GG/sIC
K4GIds1po4h17cJcQ2QUzJ6xyIjusOfOxbQvoLVV6WEbnex6JZWn2FN1egTzt7h6
869iiEa5pqNIk6nU/ytOPDvUdMxF3cQwjsberOBXs657A/iqyMwODEXvio2TZg==
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
root@server:/usr/lib/ssl/misc#
```

Export der Zertifikate (CA Zertifikat und Kunden Zertifikat) incl. Schlüssel (public und private Key des Kunden) im PKCS#12 Format mittels OpenSSL:

```
root@server:/usr/lib/ssl/misc# openssl pkcs12 -export -in newcert.pem -inkey newkey.pem -certfile
demoCA/cacert.pem
-name vpn-gateway -out vpn-gateway.p12
Enter pass phrase for newkey.pem:
Enter Export Password:
Verifying - Enter Export Password:
root@server:/usr/lib/ssl/misc# ls -l vpn-gateway/
insgesamt 16
-rw-r--r-- 1 root root 3249 2009-06-08 10:58 newcert.pem
-rw-r--r-- 1 root root  963 2009-06-08 10:28 newkey.pem
-rw-r--r-- 1 root root  708 2009-06-08 10:28 newreq.pem
-rw-r--r-- 1 root root 2732 2009-06-08 11:07 vpn-gateway.p12
```

4.2.3 Konfiguration des VPN-Gateways

Lokale IP-Adresse des VPN-Gateways

Das VPN-Gateway wird in diesem Beispiel mit der IP-Adresse *192.168.0.30* betrieben. Um dem **bintec Secure IPSec Client** eine IP-Adresse aus diesem Netzwerkbereich zuweisen zu können muss die Option **Proxy ARP** aktiviert werden.

Gehen Sie dazu in folgendes Menü:

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

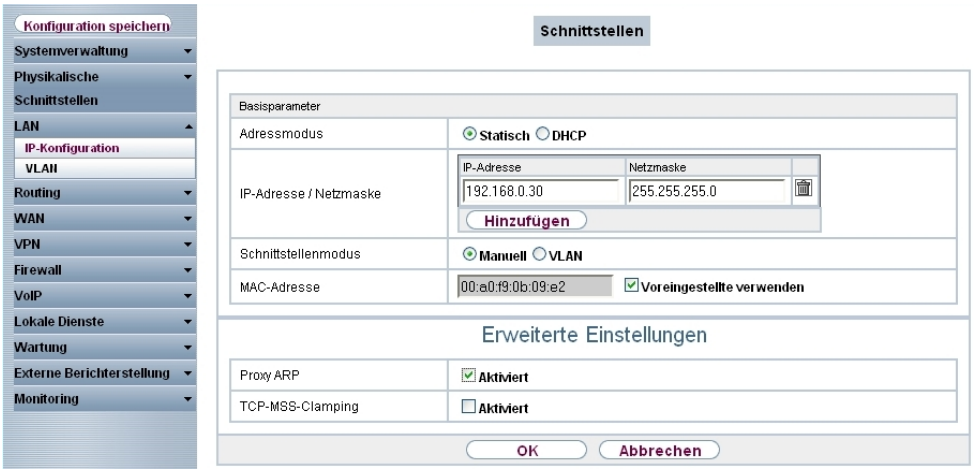


Abb. 63: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**

Relevante Felder im Menü Schnittstellen

Feld	Bedeutung
IP-Adresse / Netzmaske	Fügen Sie mit **Hinzufügen** einen neuen Adresseintrag hinzu und geben Sie die **IP-Adresse** und die entsprechende **Netzmaske** der Schnittstelle ein.
Proxy-ARP	Aktivieren Sie die Option **Proxy ARP**.

Definition eines IP-Adress-Pools

Im Menü **IP Pools** wird ein IP-Address Pool spezifiziert, aus dem allen VPN-Clients beim Aufbau des Tunnels eine Adresse zugewiesen wird. In unserem Beispiel wird ein Bereich aus dem lokalen Netzwerk gewählt z. B. *192.168.0.150* bis *192.168.0.180*.

(1) Gehen Sie zu **VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**.

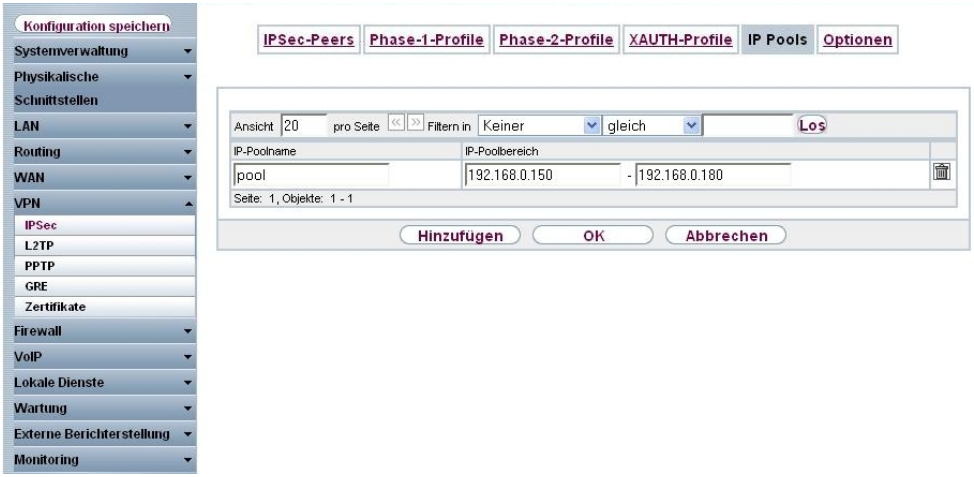


Abb. 64: **VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**

Relevante Felder im Menü IP Pools

Feld	Bedeutung
IP-Poolname	Geben Sie die Bezeichnung des IP Pools ein, z. B. *pool*.
IP-Poolbereich	Geben Sie im ersten Feld die erste IP-Adresse aus dem lokalen Netzwerk ein. Geben Sie im zweiten Feld die letzte IP-Adresse aus dem lokalen Netzwerk ein.

Import der Zertifikate

Zur VPN IPsec-Authentifizierung wurde für jeden der **bintec Secure IPSec Clients** sowie des VPN-Gateways je ein PKCS#12 Zertifikat erstellt. Das Zertifikat des VPN-Gateways wird über das Menü **Zertifikatsliste** importiert.

(1) Gehen Sie zu **VPN** -> **Zertifikate** -> **Zertifikatsliste** -> **Importieren**.

Abb. 65: **VPN** -> **Zertifikate** -> **Zertifikatsliste** -> **Importieren**

Relevante Felder im Menü Zertifikatsliste

Feld	Bedeutung
Externer Dateiname	Wählen Sie mit **Durchsuchen...** den Dateipfad bzw. Dateiname des PKCS#12 Zertifikats aus.
Lokale Zertifikatsbeschreibung	Geben Sie eine Bezeichnung unter der das Zertifikat im VPN-Gateway gespeichert wird ein, z. B. `vpn-gateway` .
Passwort	Geben Sie das Passwort ein, das beim Erstellen des PKCS#12 Zertifikats vergeben wurde.

Nach dem Importiern des PKCS#12 Kontainers sehen Sie in der **Zertifikatsliste** das eingefügte Zertifikat des VPN-Gateway und das Root Zertifiakat der Zertifizierungsstelle.

(1) Gehen Sie zu **VPN** -> **Zertifikate** -> **Zertifikatsliste**.

Abb. 66: **VPN** -> **Zertifikate** -> **Zertifikatsliste**

Konfiguration der IPSec-Phase-1 Parameter

Im Menü **Phase-1-Profile** wird anschließend das importierte Zertifikat (z. B. vpn-gateway) als **Lokales Zertifikat** ausgewählt.

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

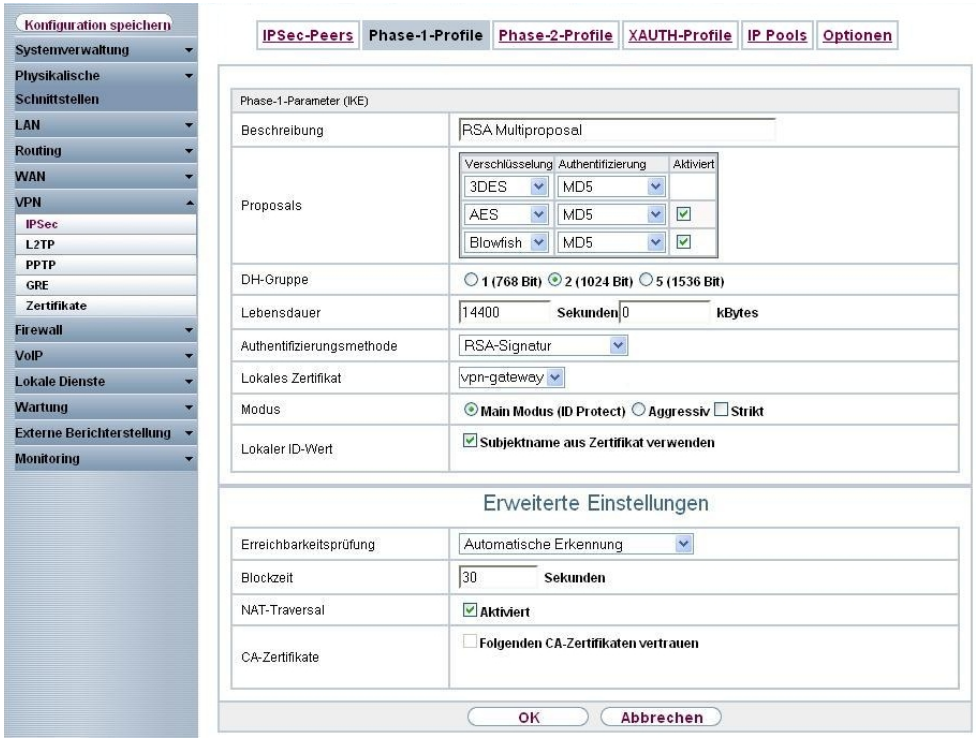


Abb. 67: **VPN** -> **IPSec** -> **Phase-1-Profile** -> **Bearbeiten**

Relevante Felder im Menü Phase-1-Profile

Feld	Bedeutung
Authentifizierungsmethode	Wählen Sie bei **Authentifizierungsmethode** *RSA-Signatur* aus. Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert.
Lokales Zertifikat	Dieses Feld ermöglicht Ihnen, das importierte Zertifikat (z. B. vpn-gateway) als Lokales Zertifikat auszuwählen.
Modus	Mit der Option **Main Modus (ID Protect)** wird sichergestellt, dass bereits die Daten zur Aushandlung der IPSec-Phase-1 verschlüsselt übertragen werden.
Lokaler ID-Wert	Wenn Sie die Option **Subjektname aus Zertifikat verwenden** aktivieren, wird der Subject Name des VPN-Gateway-Zertifikats (in unserem Beispiel: "MAIL-TO=vpn-gateway@bintec-elmeg.com, CN=vpn-gateway, OU=dev, O=fec, L=nuernberg, ST=bavaria, C=DE") als lokale IPSec-ID verwendet.

Konfiguration der IPSec-Phase-2 Parameter

Die Einstellungen im Menü **VPN** -> **IPSec** -> **Phase-2-Profile** -> **Bearbeiten** können unverändert übernommen werden.

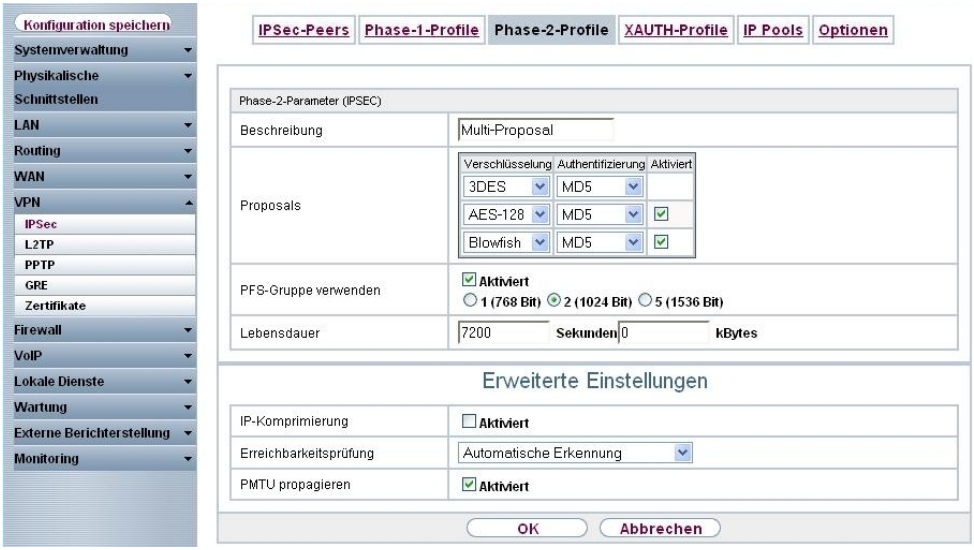


Abb. 68: **VPN** -> **IPSec** -> **Phase-2-Profile** -> **Bearbeiten**

Einrichten des VPN IPSec-Peers

Im Menü **IPSec-Peers** wird für jeden **bintec Secure IPSec Client** eine VPN-Verbindung angelegt.

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

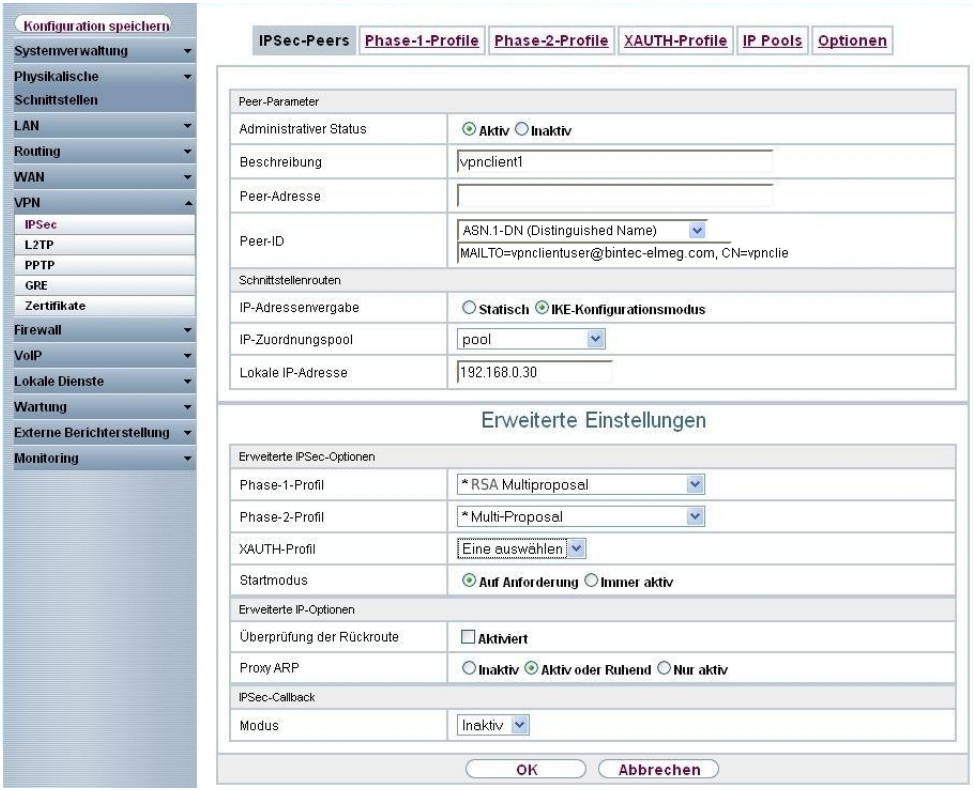


Abb. 69: **VPN** -> **IPSec** -> **IPSec-Peers** -> **Bearbeiten**

Relevante Felder im Menü IPSec-Peers

Feld	Bedeutung
Beschreibung	Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert, z. B. *vpnclient1*.
Peer-ID	Als **Peer-ID** wird der **Subjektname** des VPN-Client-Zertifiates mit dem Typ *ASN.1-DN (Distinguished Name)* hinterlegt. Dieser **Subjektname** wurde bei der Generierung der Zertifikate, welche für die **bintec Secure IPSec Clients** erstellt wurden, vergeben. Für den ersten VPN Peer wird in diesem Beispiel folgender Subjektname hinterlegt: `MAILTO=vpnclientuser@bintec-elmeg.com, CN=vpnclientuser, OU=sales, O=FEC, L=nuernberg, ST=bavaria, C=DE.`
IP-Adressenvergabe	Wählen Sie hier den Konfigurationsmodus

Feld	Bedeutung
	IKE-Konfigurationsmodus aus.
IP-Zuordnungspool	Wählen Sie einen im Menü **VPN** -> **IP Pools** konfigurierten IP-Pool aus.
Lokale IP-Adresse	Weißen Sie dem **bintec Secure IPSec Client** eine IP-Adresse zu.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Bedeutung
Phase-1-Profil	Wählen Sie ein schon im Menü **Phase-1-Profile** konfiguriertes Profil, z. B. *RSA Multiproposal* für die Phase 1 aus.
Phase-2-Profil	Wählen Sie ein schon im Menü **Phase-2-Profile** konfiguriertes Profil, z. B. *Multi-Proposal* für die Phase 1 aus.
Proxy ARP	Stellen Sie **Proxy ARP** auf *Aktiv oder Ruhend*. Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer aktiv oder ruhend ist. Bei *ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will.

4.2.4 Konfiguration des bintec Secure IPSec Clients

Der **bintec Secure IPSec Client** wird über **Start** -> **Programme** -> **FEC Secure IPSec Client** -> **Secure Client Modus** aufgerufen. Die Konfiguration des **bintec Secure IPSec Clients** wird über den Assistenten durchgeführt. Beim ersten Start des **bintec Secure IPSec Clients** wird der **Assistent für neues Profil** automatisch gestartet.

Wählen Sie bei **Verbindungstyp** die Auswahl **Verbindung zum Firmennetz über IPSec** aus.

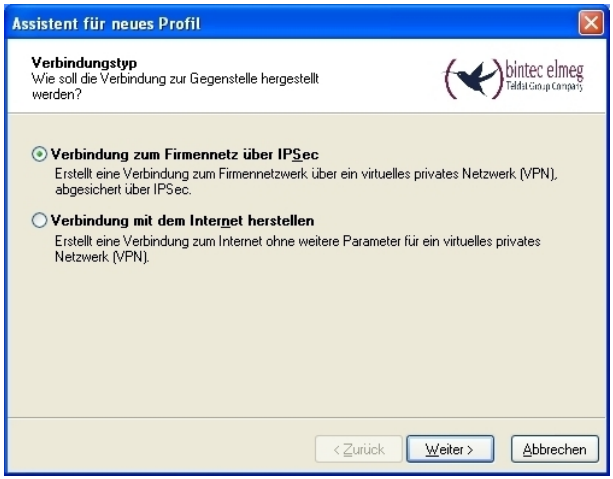


Abb. 70: Verbindungstyp

Geben Sie einen Namen für das Profil ein z. B. `Zentrale`.

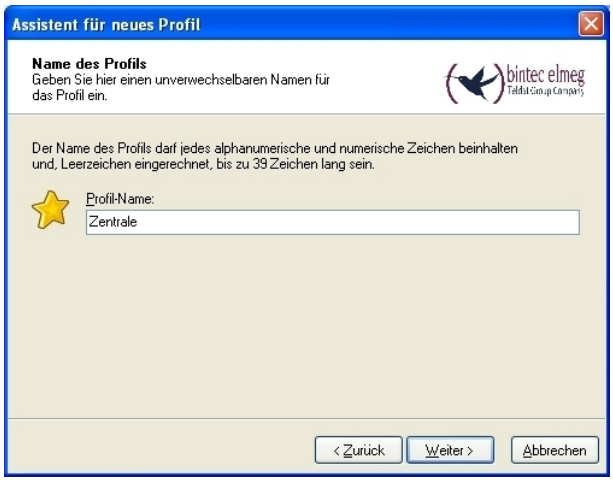


Abb. 71: Profil-Name

Im nächsten Schritt des Assistenten muss ein **Verbindungsmedium** ausgewählt werden über welches eine Verbindung zum Internet aufgebaut wird. In unserem Beispiel wird die Auswahl `LAN (over IP)` verwendet da der **bintec Secure IPSec Client** keinen direkten Zugang zum Internet herstellt sondern einen Internetzugangsrouter verwendet.

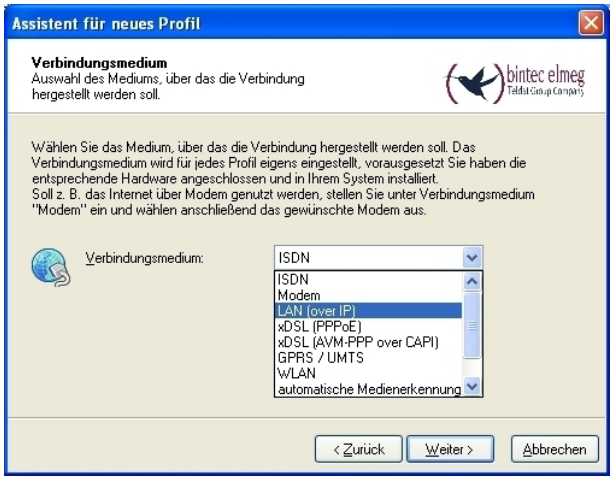


Abb. 72: Verbindungsmedium

Bei der Option **Zugangsdaten für Internetdienstanbieter** wird unter **Benutzername** die Adresse hinterlegt über die das VPN-Gateway aus dem Internet erreichbar ist, z. B. *vpn-gateway.bintec-elmeg.com*.

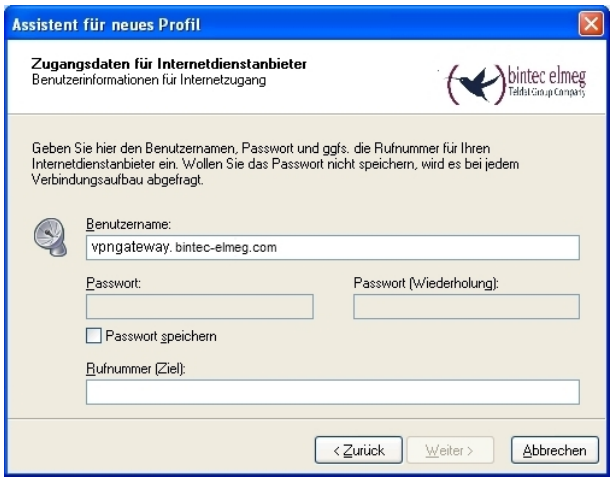


Abb. 73: Benutzername

Anschließend wird als **Austausch-Modus** der *Main Mode* verwendet. Wenn der *Main Mode* verwendet wird, werden die Informationen zum Aufbau der IPSec-Phase-1 im Gegensatz zum Aggressive Mode bereits verschlüsselt übertragen. Als **PFS-Gruppe** wird, wie bereits am VPN-Gateway, die *DH-Gruppe 2 (1024 Bit)* ausgewählt und die Option *Benutze IP-Kompression* aktiviert.

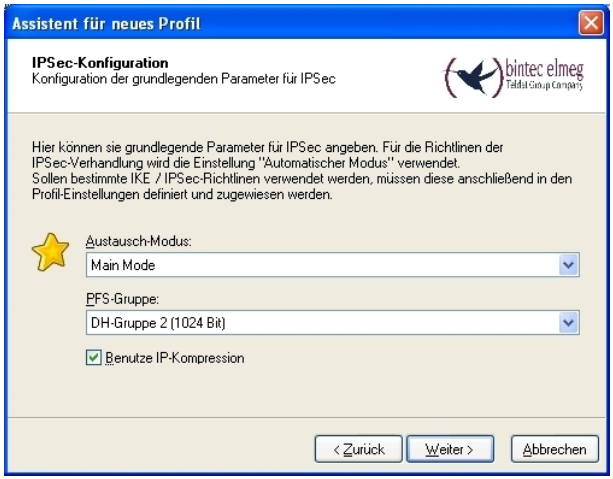


Abb. 74: IPSec-Konfiguration

Da die Authentifizierung des **bintec Secure IPSec Clients** über Zertifikate erfolgen soll wird kein **Pre-shared Key** hinterlegt. Der **Type** der **Lokalen Identität** wird auf *`ASN1 Distinguished Name`* gesetzt.

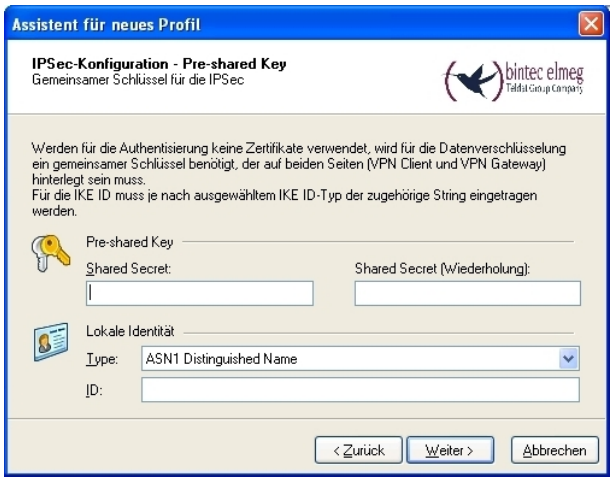


Abb. 75: Pre-shared Key

In diesem Beispiel wird dem VPN IPSec-Client eine dynamische VPN IP-Adresse zugewiesen. Dazu muss der *`IKE Conifg Mode`* aktiviert werden.

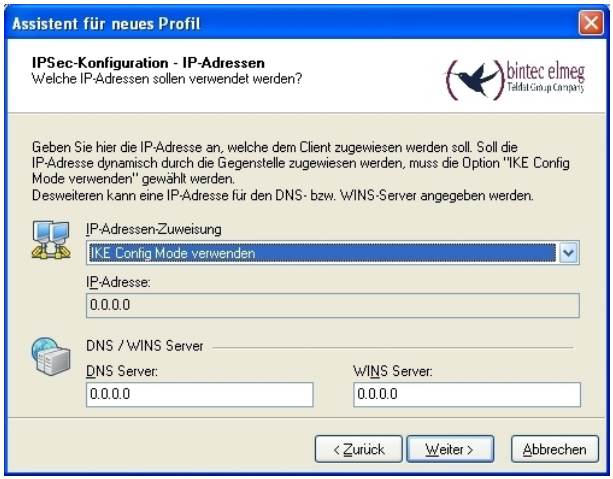


Abb. 76: IKE Config Mode

Im letzten Schritt wird die **Firewall** des **bintec Secure IPSec Clients** konfiguriert. Wenn der Client direkt mit dem Internet verbunden ist, sollte die Firewall aktiviert sein.

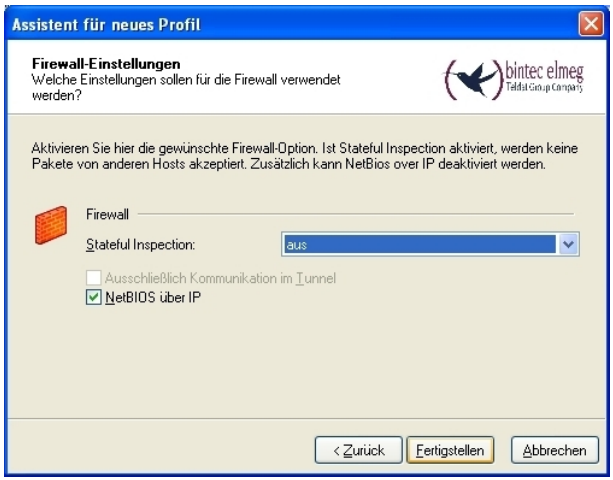


Abb. 77: Firewall

Nach dem Durchlauf des Assistenten zum Anlegen eines neuen VPN-Tunnels muss das Zerifikat (PKCS#12 Datei) des ersten VPN-Clients auf diesen Rechner kopiert werden. Anschließend wird im Menü **Konfiguration** -> **Zertifikate** -> **Hinzufügen** des **bintec Secure IPSec Clients** das Benutzer-Zertifikat ausgewählt.

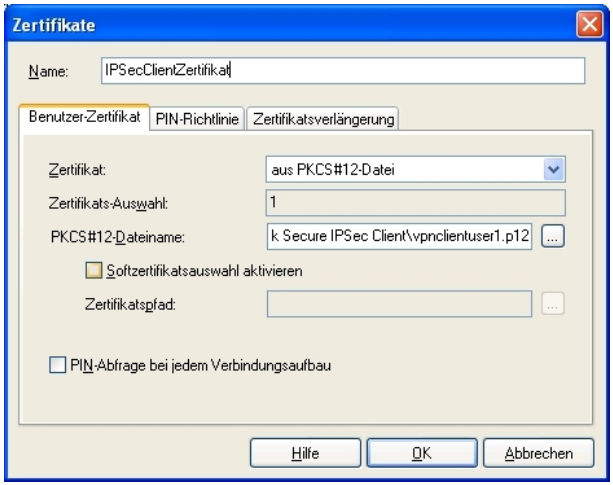


Abb. 78: Zertifikate

Danach sind noch einige Anpassungen im Profil der VPN-Verbindung notwendig.

Im Menü **Konfiguration** -> **Profile** -> **Edit** -> **IPSec-Einstellungen** wird die vordefinierte **IKE-Richtline** *RSA Signature* und die **IPSec-Richtline** *ESP - AES128 - MD5* gewählt.

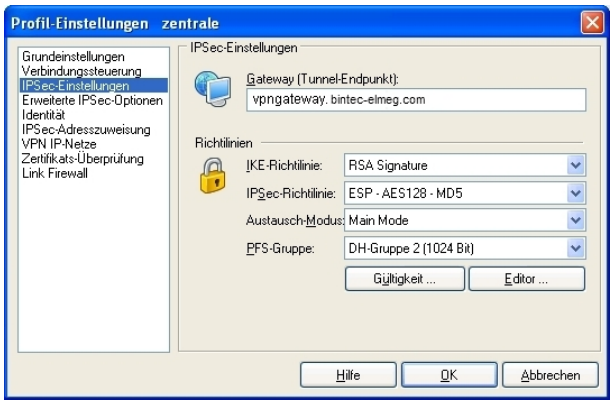


Abb. 79: IPSec-EInstellungen

Im Menü **Konfiguration** -> **Profile** -> **Edit** -> **Identität** wird die bereits angelegte Zertifikats-Richtline ausgewählt. Das hier hinterlegte Zertifikat/Zertifikatsprofil wird beim Aufbau des VPN IPSec-Tunnels zur Authentifikation verwendet.

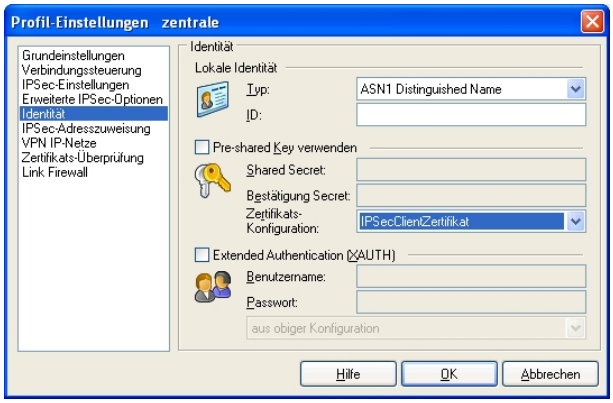


Abb. 80: Identität

4.2.5 Aufbau des VPN IPSec-Tunnels

Beim Aufbau des VPN IPSec-Tunnels erfolgt eine PIN-Abfrage. Die **PIN** wird verwendet um den Kontainer des PKCS#12 Zertifikats zu öffnen. Hier muss das Passwort verwendet werden, welches beim Erstellen des PKCS#12 Zertifikats vergeben wurde.

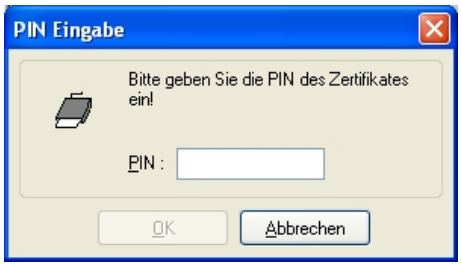


Abb. 81: PIN Eingabe

Abb. 82: FEC Secure IPSec Client

4.2.6 Zusätzliche Absicherung des VPN IPSec-Tunnels über ein Einmal-Passwort (optional)

Um den VPN IPSec-Tunnel weiter abzusichern besteht die Möglichkeit eine Einmal-Passwort-Abfrage zu aktivieren. In diesem Beispiel wird die **KOBIL SecOVID** One-Time-Password Lösung beschrieben. Das Einmal-Passwort wird über einen Token generiert. Beim Aufbau des VPN IPSec-Tunnels wird dieses Einmal-Passwort am **KOBIL SecOVID** Radius Server authentifiziert.

Installation des KOBIL SecOVID Servers auf einem 32Bit Windows 2003 Server

Das Installationsprogramm des **KOBIL SecOVID** Servers wird auf der CD über den Aufruf der Datei `win32\server\SECOVID Server.exe` gestartet. Bitte lesen Sie die Ausgaben des Setups zu Ihrer Information und folgen Sie den Anweisungen und Empfehlungen der Installationsroutine. Nach Abschluss der Installationsroutine sollte das Logfile des **KOBIL SecOVID** Servers überprüft werden um sicher zu stellen das der Server gestartet wurde.

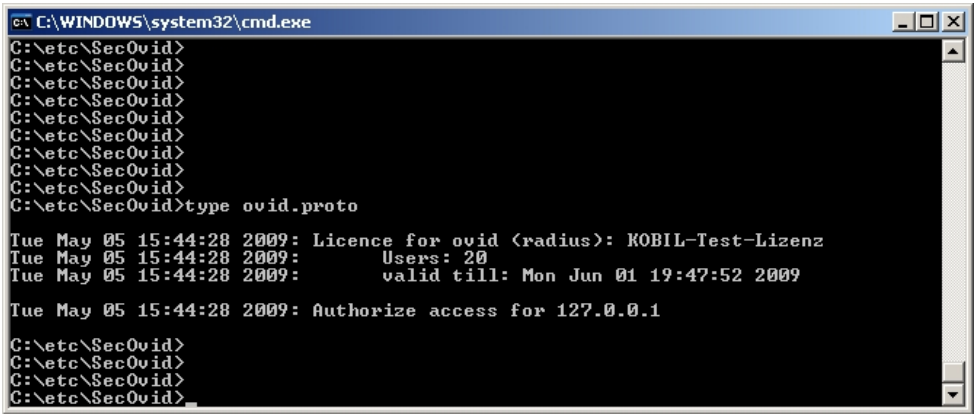


Abb. 83: Installation des **KOBIL SecOVID**

Installation des KOBIL SecOVID Administrationstools

Zur Installation des **KOBIL SecOVID** Administrationstools unter Win32-Systemen gehen Sie wie folgt vor:

- Starten Sie das Setup-Programm für die Treiber Ihres KOBIL-Chipkartenterminals über `/Treiber-Setup/KOBILTreiberSetup.exe`
- Folgen Sie den Anweisungen des Setup-Programms und schließen Sie das Chipkartenterminal an wenn Sie dazu aufgefordert werden. Das Chipkartenterminal wird benötigt um den **KOBIL SecOVID** Server per Remoteconsole zu administrieren. Für die lokale Administration des **KOBIL SecOVID** Server wird das KOBIL-Chipkartenterminal nicht benötigt.

  Zur Installation des **KOBIL SecOVID** Administrationstools muss das Setup-Programm `/win32/admin/Setup_admintools.exe`, der Installations-CD, gestartet werden. Bitte folgen Sie bei der Installation den weiteren Anweisungen des Setup-Programms.

Starten des KOBIL SecOVID Administrationstools

Das **KOBIL SecOVID** Administrationstool wird über das Menü **Start** -> **Programme** -> **SecOVID Admintools** -> **WxOvid** gestartet. Nach dem ersten Start des **KOBIL SecOVID** Admintools können die geheimen Tokendaten importiert und zur SecOVID-Datenbank hinzugefügt werden. Bei einer SecOVID Teststellung liegen die Tokendaten im Klartext vor. Wenn Sie die SecOVID Tokens gekauft haben, werden die Tokendaten in der Regel verschlüsselt geliefert. Der Import der Tokendaten (z. B. `tokendaten_firma.db`) erfolgt über das Menü **Sonstige Token** -> **Token importieren**.

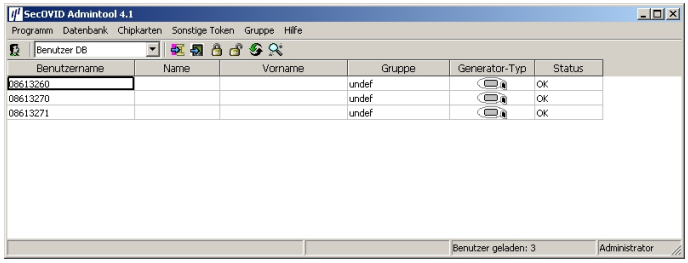


Abb. 84: Starten des **KOBIL SecOVID** *Admintools*

Personalisierung der Token

Zur Zuweisung der Token an einen Benutzer müssen die Tokendatensätze gesperrt werden. Nach dem vorübergehenden Sperren eines Tokendatensatzes können durch das Editieren des Eintrags die Benutzerinformationen hinterlegt werden. Die Information im Feld **Benutzername** wird nach erfolgter Konfiguration am **bintec Secure IPSec Client** zur Erweiterten IPSec-Authentifizierung verwendet.

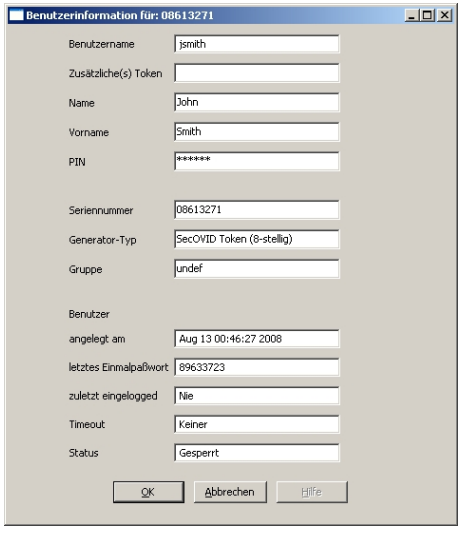


Abb. 85: Benutzerinformation

Anschließend muss die Sperrung des Datensatzes rückgängig gemacht werden.

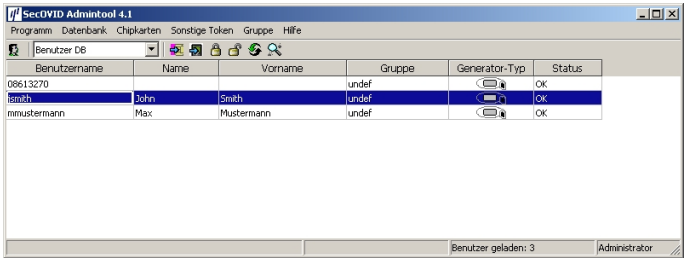


Abb. 86: Sperrung aufheben

Erster Funktionstest des KOBIL SecOVID Servers

Ein erster Funktionstest kann mit dem Kommandozeilen Tool `radping.exe` durchgeführt werden. `Radping` initiiert mit dem Einmal-Passwort eine Authentifizierungsanfrage an den SecOVID RADIUS-Server. Das Tool wurde während der Installation im Verzeichnis `\etc\SecOVID\` hinterlegt.

Mit der Option `-u` wird dem SecOVID Server der Benutzername und das One-Time-Password übergeben. Das Einmal-Passwort muss mit dem Token des Benutzers generiert werden. Mit der Option `-S` wird der SecOVID Server angesprochen. Für den ersten Funktionstest muss `radping` direkt auf dem Server ausgeführt werden. Mit der Option `-k` wird das RADIUS-Passwort übergeben. Der default Wert ist *`geheim`*. Das SecOVID Logfile (`\etc\SecOVID\ovid.proto`) gibt bei einer erfolgreichen Authentifizierung folgende Meldung aus:

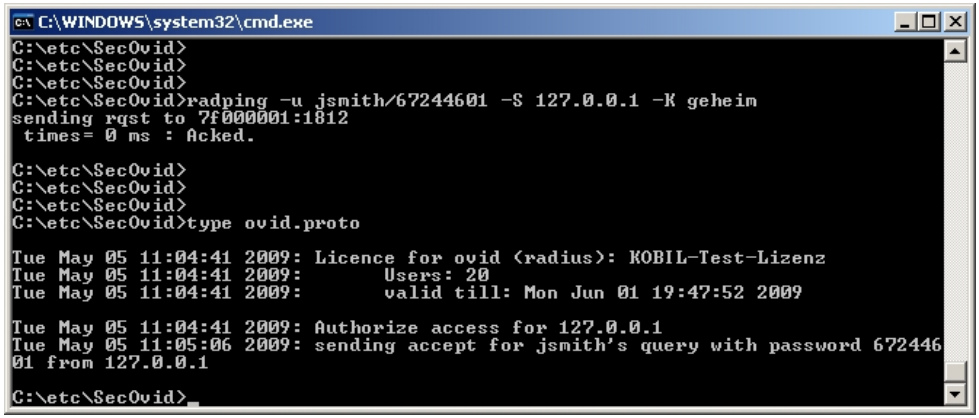


Abb. 87: Funktionstest

Konfiguration des RADIUS-Clients am SecOVID Server

Alle RADIUS-Clients (z. B. das bintec VPN-Gateway oder die Testapplikation `radping`)

müssen am SecOVID Server als RADIUS-Client hinterlegt werden. Dazu wird die Konfigurationsdatei `\etc\SecOVID\clients` bearbeitet. In unserem Beispiel wird das bintec VPN-Gateway mit der IP-Adresse `192.168.0.30` und dem RADIUS-Passowort `radius_PWD` hinzugefügt. Dieses Passwort wird später auch am VPN-Gateway in den RADIUS-Einstellungen hinterlegt. Damit die Änderungen wirksam werden, muss der Dienst SecOVID Server neu gestartet werden.

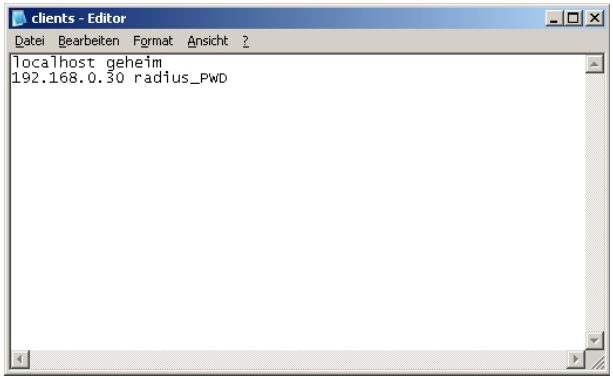


Abb. 88: Clients-Editor

4.2.7 Anpassung der VPN Gateway Konfiguration für die Einmal-Passwort-Abfrage

Radius Einstellungen am VPN-Gateway

Mit den Einstellungen im Menü **RADIUS** wird die erweiterte IPSec-Authentifizierung (XAUTH) mit dem RADIUS-Server des **KOBIL SecOVID** Servers aktiviert. Es ist notwendig den Authentifizierungstyp auf den Wert *XAUTH* zu setzen sowie die IP-Adresse des **KOBIL SecOVID** Servers zu hinterlegen. Die Kommunikation mit dem RADIUS-Server wird mit einem Passwort geschützt. Bitte verwenden Sie hier das am SecOVID Server hinterlegte RADIUS-Passwort (Konfigurationsdatei `\etc\SecOVID\clients`).

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS**.

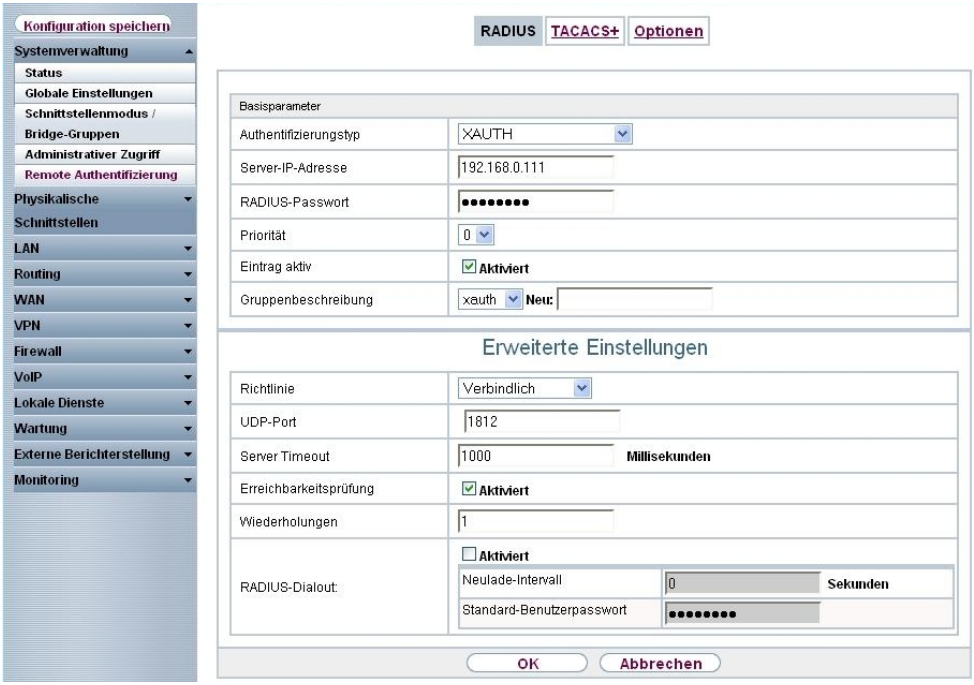


Abb. 89: **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS**

Relevante Felder im Menü RADIUS

Feld	Beschreibung
Authentifizierungstyp	Wählen Sie den **Authentifizierungstyp** *XAUTH* aus.
Server-IP-Adresse	Geben Sie die **Server-IP-Adresse** des **KOBIL SecOVID** Servers ein, z. B. *192.168.0.111*.
RADIUS-Passwort	Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort ein, hier z. B. *radius_PWD*.
Gruppenbeschreibung	Definieren Sie eine neue RADIUS-Gruppenbeschreibung bzw. weisen Sie den neuen RADIUS-Eintrag einer schon definierten Gruppe zu. Die konfigurierten RADIUS-Server einer Gruppe werden gemäß der **Priorität** und der **Richtlinie** abgefragt. Mögliche Werte: • *Neu* (Standardwert): Tragen Sie in das Textfeld eine neue Gruppenbeschreibung ein • <Gruppenname>: Wählen Sie aus der Liste eine schon definierte Gruppe aus, z. B. *xauth*.

XAUTH-Konfiguration

Für die Erweiterte IPSec-Authentifizierung (XAuth) soll ein RADIUS-Server verwendet werden. Die hierfür notwendigen Einstellungen werden im Menü **XAUTH-Profile** vorgenommen.

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

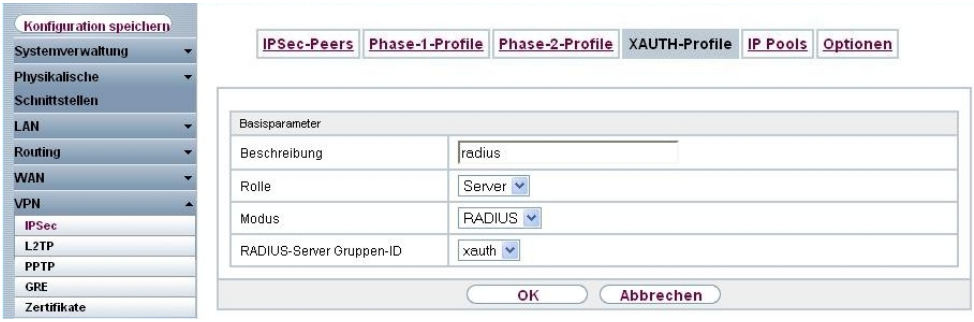


Abb. 90: **VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**

Relevante Felder im Menü XAUTH-Profile

Feld	Bedeutung
Beschreibung	Geben Sie eine Beschreibung für die IPSec-Authentifizierung ein, z. B. `radius`.
Rolle	Wählen Sie hier `Server` aus.
Modus	Bei **Modus** wählen Sie `RADIUS` aus.
RADIUS-Server Gruppen-ID	Wählen Sie den RADIUS-Server `xauth` aus.

Aktivieren der Einmal-Passwort-Abfrage am VPN-Peer

Zur Aktivierung der Einmal-Passwort-Abfrage in der jeweiligen VPN Peer-Konfiguration wird das bereits konfigurierte Radius Server Profil ausgewählt.

Unter der Option **XAUTH Profil** wird das Radius Server Profil des **KOBIL SecOVID** Servers ausgewählt. Beim nächsten Aufbau des VPN IPSec-Tunnels wird das Einmal-Passwort abgefragt und mit dem **KOBIL SecOVID** Server abgeglichen.

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

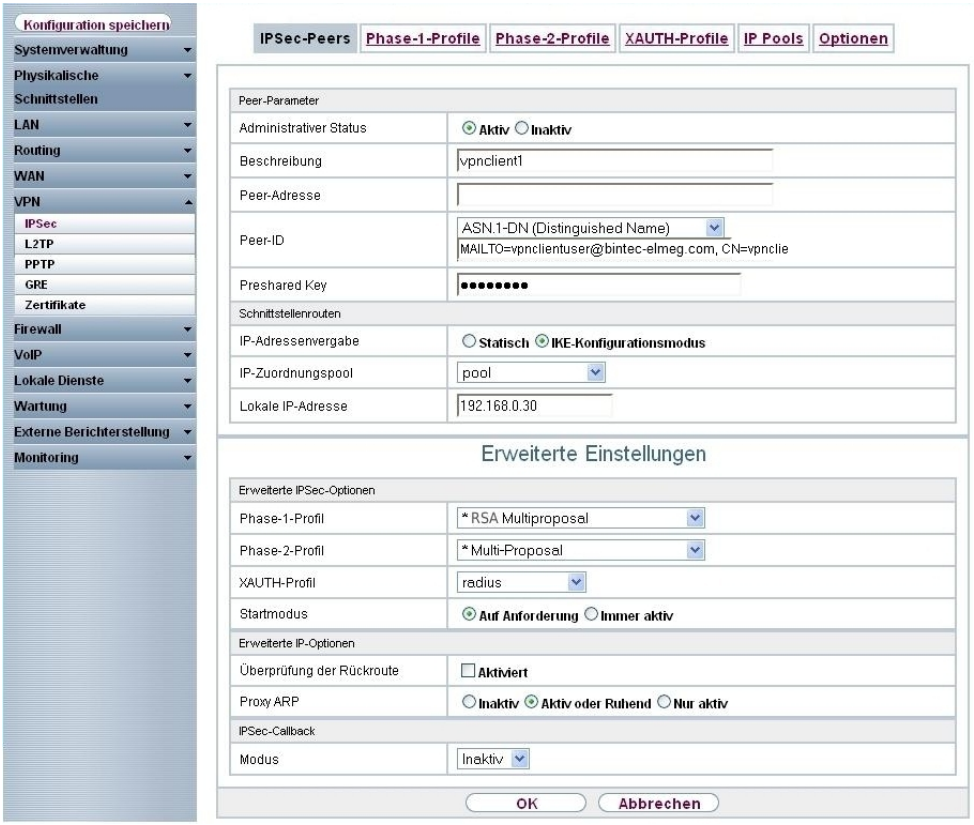


Abb. 91: **VPN** -> **IPSec** -> **IPSec-Peers** ->

Relevante Felder im Menü IPSec-Peers

Feld	Bedeutung
XAUTH	Wählen Sie das Radius Server Profil des **KOBIL SecOVID** Servers aus.

4.2.8 Anpassung der bintec Secure IPSec Konfiguration für die Einmal-Passwort-Abfrage

Das Einmal-Passwort wird beim Aufbau des VPN IPSec-Tunnels über den XAuth-Mechanismus (Erweiterte Authentifizierung) übertragen. Hierzu muss das Profil des VPN IPSec-Tunnels bearbeitet werden. Im Menü **Konfiguration** -> **Profile** -> **Edit** -> **Identität** wird ein im **KOBIL SecOVID** Administrator hinterlegter Benutzer eingetragen.

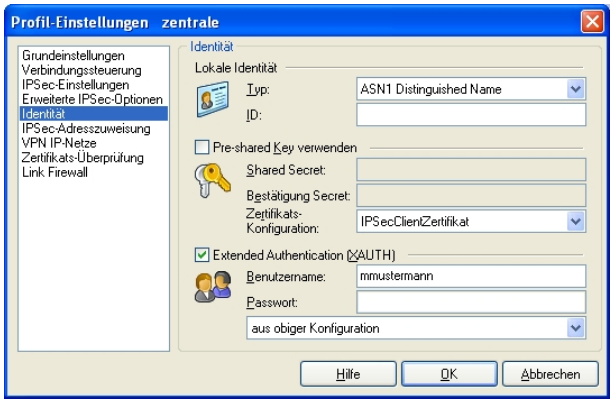


Abb. 92: Identität

Beim nächsten Aufbau des VPN IPSec-Tunnels wird das Einmal-Passwort abgefragt.

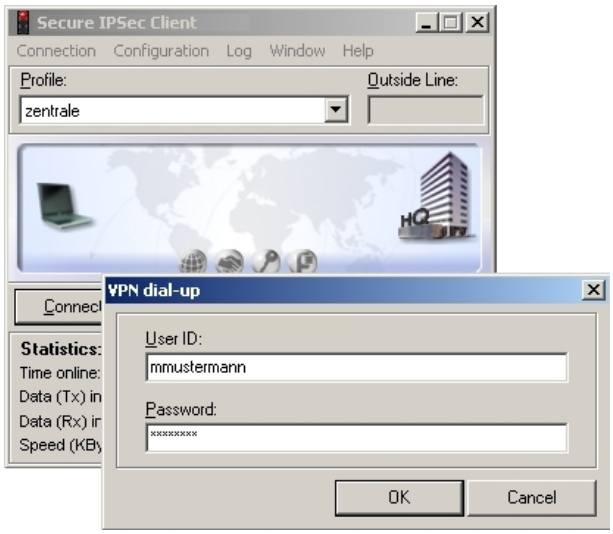


Abb. 93: User ID / Passwort abfrage

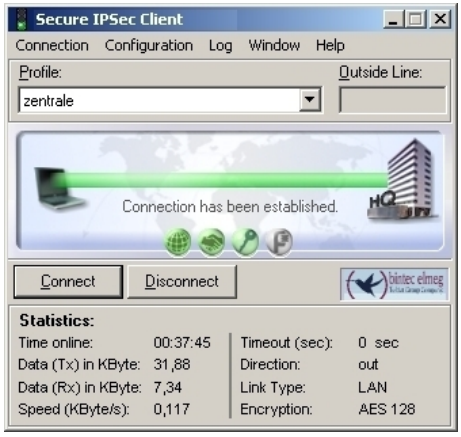


Abb. 94: Aufbau der Verbindung

4.3 Konfigurationsschritte im Überblick

Konfiguration des VPN Gateways

Feld	Menü	Wert
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Statisch*
IP-Adresse / Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	z. B. *192.168.0.30* / *255.255.255.0*
Schnittstellenmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Manuell*
Proxy ARP	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Aktiviert*

VPN Konfiguration

Feld	Menü	Wert
IP-Poolname	**VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**	z. B. *pool*
IP-Poolbereich	**VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**	z. B. *192.168.0.150* - *192.168.0.180*

Zertifikate importieren

Feld	Menü	Wert
Externer Dateiname	**VPN** -> **Zertifikate** -> **Zertifikatsliste** -> **Importieren**	z. B. */usr/*

Feld	Menü	Wert
		lib/ssl/misc/vpn-gateway/vpn-gateway.p12
Lokale Zertifikatsbeschreibung	**VPN** -> **Zertifikate** -> **Zertifikatsliste** -> **Importieren**	z. B. *vpn-gateway*
Passwort	**VPN** -> **Zertifikate** -> **Zertifikatsliste** -> **Importieren**	Passwort des PKCS#12 Zertifikats

Phase-1-Profile Konfiguration

Feld	Menü	Wert
Authentifizierungsmethode	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Bearbeiten**	*RSA-Signatur*
Lokales Zertifikat	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Bearbeiten**	z. B. *vpn-gateway*
Modus	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Bearbeiten**	*Main Modus (ID Protect)*
Lokaler ID-Wert	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Bearbeiten**	*Subjektname aus Zertifikat verwenden* aktivieren

IPSec-Peers Konfiguration

Feld	Menü	Wert
Administrativer Status	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*Aktiv*
Beschreibung	**VPN** -> **IPSec** -> **IPSec-Peers** ->	z. B. *vpnclient1*
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*ASN.1-DN (Distinguished Name)* und *MAILTO=vpnclientuser@bintec-elmeg.com, CN=vpnclientuser, OU=sales, O=FEC, L=nuernberg, ST=bavaria, C=DE*
IP-Adressenvergabe	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*IKE-Konfigurationsmo-*

Feld	Menü	Wert
		dus
IP-Zuordnungspool	**VPN** -> **IPSec** -> **IPSec-Peers** ->	*pool*
Lokale IP-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** ->	z. B. *192.168.0.30*
Phase-1-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	** RSA Multipropo-sal*
Phase-2-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	** Multi-Proposal*
Proxy ARP	**VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**	*Aktiv oder Ruhend*

Konfiguration des bintec Secure IPSec Clients

Feld	Menü	Wert
Verbindungstyp	**Assistent für neues Profil**	*Verbindung zum Firmennetz über IPSec*
Profil-Name	**Assistent für neues Profil**	*Zentrale*
Verbindungsmedium	**Assistent für neues Profil**	*LAN (over IP)*
Benutzername	**Assistent für neues Profil**	z. B. *vpngate-way.bintec-elmeg.com*
Austausch-Modus	**Assistent für neues Profil**	Main Mode
PFS-Gruppe	**Assistent für neues Profil**	DH-Gruppe 2 (1024 Bit)
Lokale Identität	**Assistent für neues Profil**	*ASN1 Distinguished Name*
IP-Adres-sen-Zuweisung	**Assistent für neues Profil**	*IKE Config Mode verwenden*
Stateful Inspection	**Assistent für neues Profil**	*aus*
NetBIOS über IP	**Assistent für neues Profil**	Aktiviert

Zertifikate kopieren

Feld	Menü	Wert
Name	**Konfiguration** -> **Zertifikate** -> **Hinzufü-gen**	*IPSecClientZerti-fikat*
Zertifikat	**Konfiguration** -> **Zertifikate** -> **Hinzufü-gen**	*aus PKCS#12-Datei*
PK-	**Konfiguration** -> **Zertifikate** -> **Hinzufü-**	*bintec Secure IP-*

Feld	Menü	Wert
CS#12-Dateiname	**gen**	*Sec Client\vpnclientuser1.p12*

Profil-Einstellungen

Feld	Menü	Wert
Gateway (Tunnel-Endpunkt)	**Konfiguration** -> **Profile** -> **Edit** -> **IPSec-Einstellungen**	*vpngateway.bintec-elmeg.com*
IKE-Richtlinie	**Konfiguration** -> **Profile** -> **Edit** -> **IPSec-Einstellungen**	*RSA Signature*
IPSec-Richtlinie	**Konfiguration** -> **Profile** -> **Edit** -> **IPSec-Einstellungen**	*ESP - AES128 - MD5*
Austauschmodus	**Konfiguration** -> **Profile** -> **Edit** -> **IPSec-Einstellungen**	*Main Mode*
PFS-Gruppe	**Konfiguration** -> **Profile** -> **Edit** -> **IPSec-Einstellungen**	*DH-Gruppe 2 (1024 Bit)*
Typ	**Konfiguration** -> **Profile** -> **Edit** -> **Identität**	ASN1 Distinguished Name
Zertifikats-Konfiguration	**Konfiguration** -> **Profile** -> **Edit** -> **Identität**	IPSecClientZertifikat

Aufbau des VPN IPSec-Tunnels

Feld	Menü	Wert
PIN	**PIN Eingabe**	*Passwort des PKCS#12 Zertifikats*

RADIUS-Einstellungen

Feld	Menü	Wert
Authentifizierungstyp	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	*XAUTH*
Server-IP-Adresse	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *192.168.0.111*
RADIUS-Passwort	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	Das am SecOVID Server hinterlegte Radius Passwort
Gruppenbeschreibung	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	*xauth*

XAUTH Konfiguration

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	z. B. *radius*
Rolle	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	*Server*
Modus	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	*RADIUS*
RADIUS-Server Gruppen -ID	**VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**	*xauth*

IPSec-Peers Konfiguration

Feld	Menü	Wert
XAUTH-Profil	**VPN** -> **IPSec** -> **IPSec-Peers** ->  -> **Erweiterte Einstellungen**	*radius*

Profil-Einstellungen

Feld	Menü	Wert
Typ	**Konfiguration** -> **Profile** -> **Edit** -> **Identität**	ASN1 Distinguished Name
Zertifikats-Konfiguration	**Konfiguration** -> **Profile** -> **Edit** -> **Identität**	IPSecClientZertifikat
Benutzername	**Konfiguration** -> **Profile** -> **Edit** -> **Identität**	z. B. *mmustermann*

Kapitel 5 Sicherheit - VPN IPSec-Tunnel über HTTPS zwischen dem bintec Secure IPSec Client und einem bintec Router

5.1 Einleitung

Dieses Kapitel beschreibt die VPN IPSec-Anbindung des **bintec Secure IPSec Client** an ein **bintec R3502** VPN-Gateway über das HTTPS-Protokoll. An öffentlichen Hotspots oder z. B. in Hotels soll unter Umständen die VPN-Nutzung durch das Sperren der typischen Ports UDP500 und UDP4500 verhindert werden. In diesem Fall wird der VPN IPSec-Tunnel bei aktivierter IPSec-Pathfinder-Funktion über den HTTPS-Port (TCP 443) getunnelt.

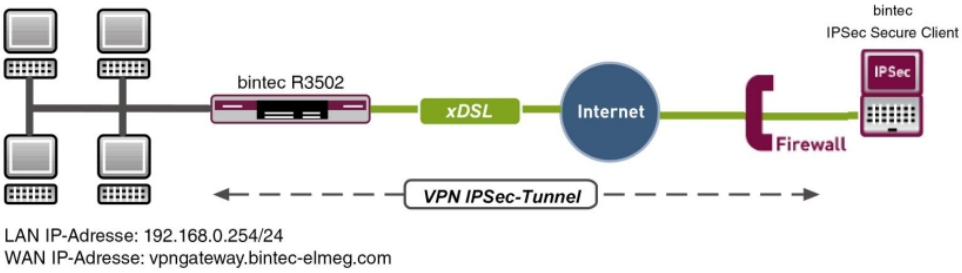


Abb. 95: Beispielszenario

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein VPN-Gateway z. B. **bintec R3502** mit Systemsoftware 7.10.1 (IPSec-Pathfinder-Unterstützung)
- Ein **bintec Secure IPSec Client**
- VPN-Gateway und VPN-Client benötigen jeweils eine unabhängige Verbindung zum Internet

5.2 Konfiguration

5.2.1 Konfiguration des VPN-Gateways

Beim Aufbau der VPN IPSec-Verbindung wird dem **bintec Secure IPSec Client** eine dynamische IP-Adresse zugewiesen. Hierzu wird ein IP-Adress-Pool angelegt. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**.

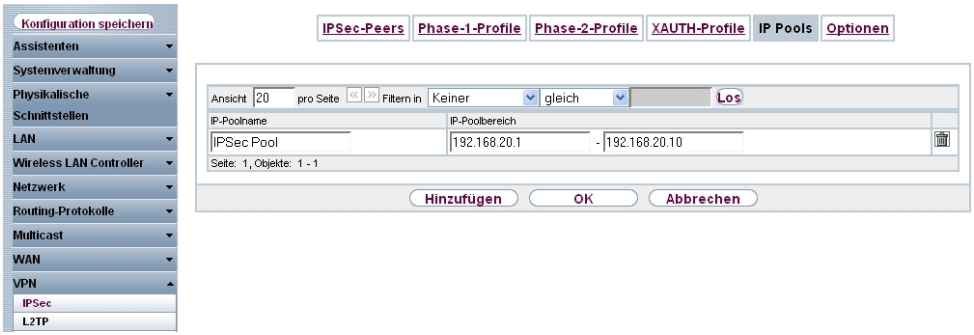


Abb. 96: **VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**

Gehen Sie folgendermaßen vor um ein IP Pool einzurichten:

(1) Bei **IP-Poolname** geben Sie die Bezeichnung des IP-Pools ein, z. B. `IPSec Pool`.

(2) Bei **IP-Poolbereich** werden in unserem Beispiel für VPN IPSec Client Verbindungen die Adressen `192.168.20.1` bis `192.168.20.10` vergeben.

(3) Bestätigen Sie mit **OK**.

5.2.2 Konfiguration des VPN IPSec-Tunnels

Im Menü **IPSec-Peers** wird die eigentliche VPN-Verbindung konfiguriert.

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

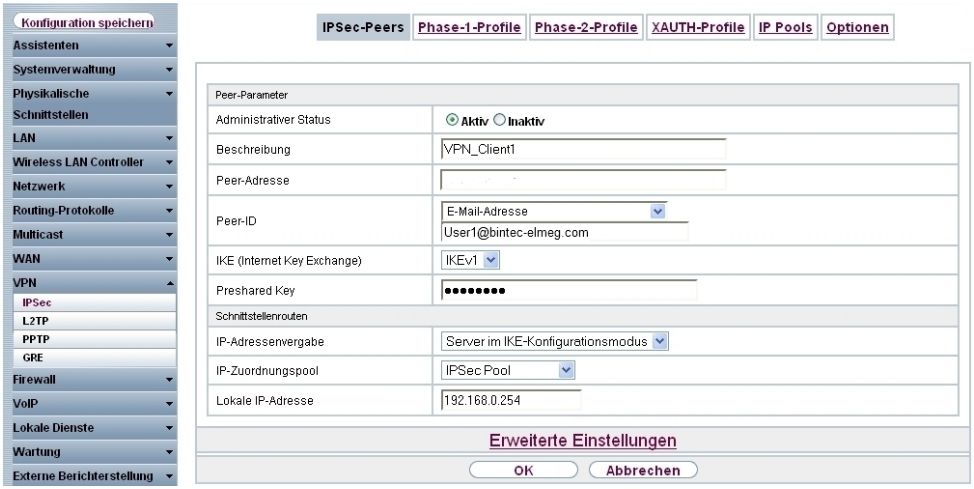


Abb. 97: **VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**

Gehen Sie folgendermaßen vor, um die Einstellungen für den IPSec-Peer vorzunehmen:

(1) Bei **Beschreibung** geben Sie eine Beschreibung des Peers ein, die diesen identifiziert z. B. *VPN_Client1* ein.

(2) Lassen Sie das Feld **Peer-Adresse** leer.

(3) Die **Peer-ID** muss mit dem Lokalen ID-Wert der Gegenstelle übereinstimmen, z. B. Typ *E-Mail-Adresse* und geben Sie *User1@bintec-elmeg.com* ein.

(4) Im **Preshared Key** tragen Sie ein Passwort für die verschlüsselte Verbindung, z. B. *test* ein.

(5) Bei **IP-Adressenvergabe** wählen Sie die Einstellung *Server im IKE-Konfigurationsmodus* aus. Dem bintec Secure IPSec Client wird beim Verbindungsaufbau eine IP-Adresse zugewiesen.

(6) Wählen Sie bei **IP-Zuordnungspool** den *IPSec Pool* aus.

(7) Unter **Lokale IP-Adresse** tragen Sie die IP-Adresse der LAN-Schnittstelle des Routers ein, z. B. *192.168.0.254* .

(8) Bestätigen Sie Ihre Eingaben mit **OK**.

5.2.3 Aktivieren der IPSec-Pathfinder-Funktion

Die IPSec-Pathfinder-Funktion ist im Auslieferungszustand nicht aktiviert. Durch das Einschalten des IPSec-Pathfinders reagiert das VPN-Gateway auch auf dem HTTPS-Port auf VPN IPSec-Anfragen.

(1) Gehen Sie zu **VPN** -> **IPSec** -> **Optionen** -> **Erweiterte Einstellungen**.

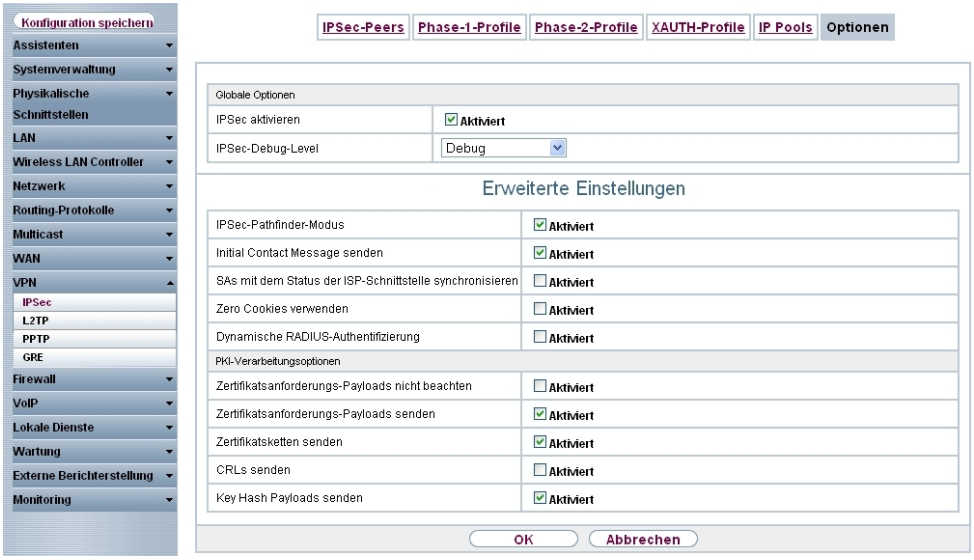


Abb. 98: **VPN** -> **IPSec** -> **Optionen** -> **Erweiterte Einstellungen**

Gehen Sie folgendermaßen vor:

(1) Aktivieren Sie den **IPSec-Pathfinder -Modus**.

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

5.2.4 Konfiguration des bintec Secure IPSec Clients

Der **bintec Secure IPSec Client** wird über **Start** -> **Programme** -> **FEC Secure IPSec Client** -> **Secure Client Modus** aufgerufen. Die Konfiguration des **bintec Secure IPSec Clients** wird über den Assistenten durchgeführt. Beim ersten Start des **bintec Secure IPSec Clients** wird der **Assistent für neues Profil** automatisch gestartet.

Wählen Sie die Auswahl **Verbindung zum Firmennetz über IPSec** aus.

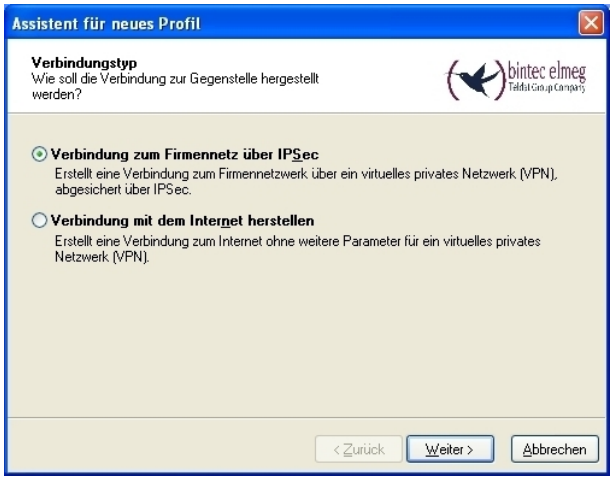


Abb. 99: Verbindungstyp

Geben Sie einen Namen für das Profil ein z. B. `VPN Firmenzentrale`.

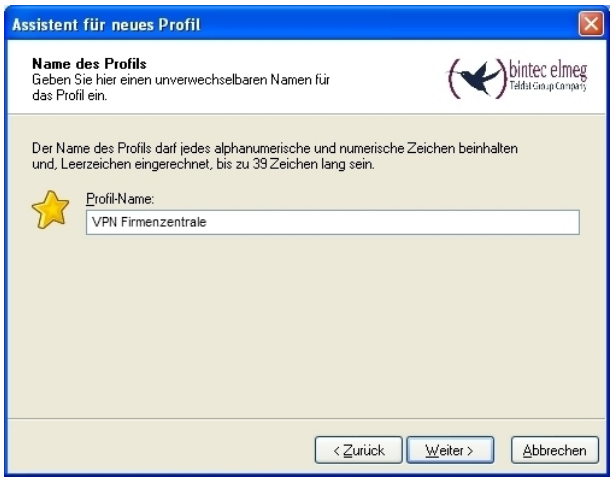


Abb. 100: Profil-Name

Im nächsten Schritt des Assistenten muss ein **Verbindungsmedium** ausgewählt werden über welches eine Verbindung zum Internet aufgebaut wird. In unserem Beispiel wird die Auswahl `LAN (over IP)` verwendet da der **bintec Secure IPSec Client** keinen direkten Zugang zum Internet herstellt sondern einen Internetzugangsrouter verwendet.

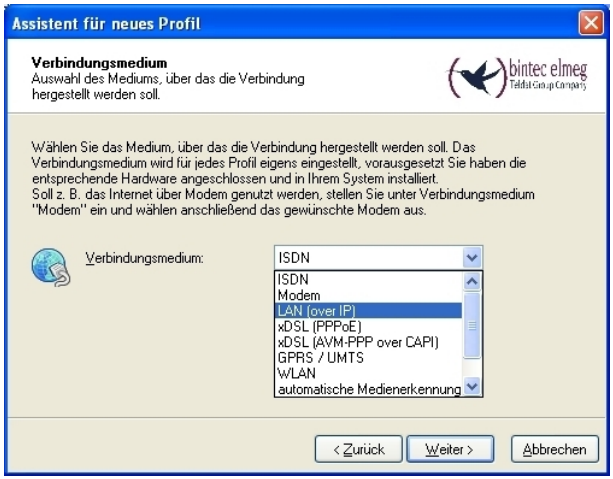


Abb. 101: Verbindungsmedium

Im Fenster **VPN Gateway-Parameter** ist die feste offizielle IP-Adresse oder der DynDNS-Name der Gegenstelle einzutragen, zu der der IPSec-Tunnel aufgebaut werden soll, z. B. *vpngateway.bintec-elmeg.com*.

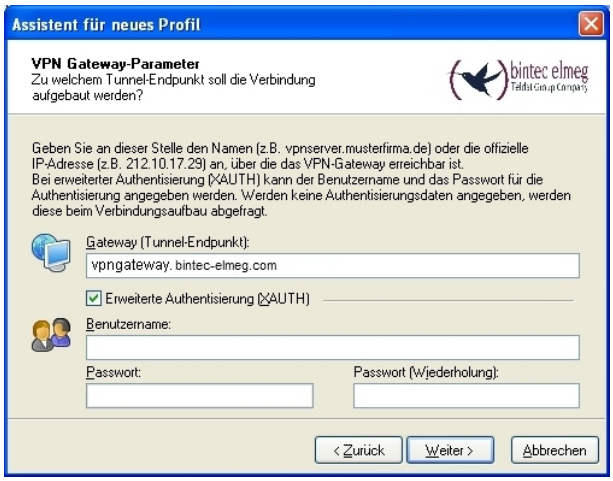


Abb. 102: VPN Gateway Parameter

Anschließend wird als **Austausch-Modus** der *Aggressive Mode* verwendet, da dem **bintec R3502** Router und/oder dem **bintec Secure IPSec Client** dynamische IP-Adresse vom Internet-Provider zugewiesen werden. Die **PFS-Gruppe** setzen Sie z. B. auf *DH-Gruppe 2 (1024 Bit)*. Die Option *Benutze IP-Kompression* wird in dieser Konfiguration nicht eingesetzt.

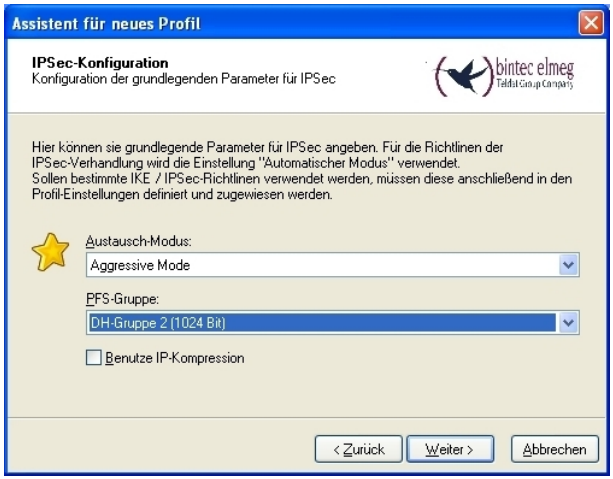


Abb. 103: IPSec-Konfiguration

Im nächsten Schritt des Assistenten wird der am VPN-Gateway konfigurierte **Preshared Key** hinterlegt, z. B. `test`.

Als **Lokale Identität** soll die E-Mail-Adresse des Benutzers mit dem **Type** `Fully Qualified Username` und mit der **ID** `User1@bintec-elmeg.com`verwendet werden. Dieser Typ und die ID müssen mit der am VPN-Gateway konfigurierten Peer-ID übereinstimmen.

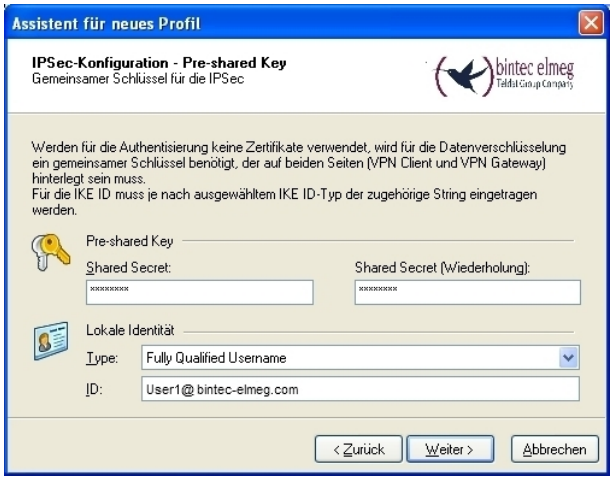


Abb. 104: Pre-shared Key

In diesem Beispiel bezieht der **bintec Secure IPSec Client** eine IP-Adresse aus dem am VPN-Gateway konfigurierten IP Pool. Dazu muss bei **IP-Adressen-Zuweisung** die Option `IKE Config Mode verwenden` ausgewählt werden.

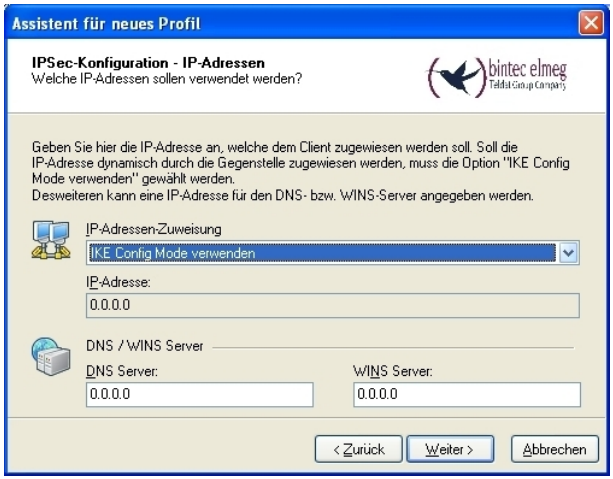


Abb. 105: IKE Config Mode

Im nächsten Schritt wird die **Firewall** des **bintec Secure IPSec Clients** konfiguriert. Wenn der Client direkt mit dem Internet verbunden ist, sollte die Firewall aktiviert sein. Bei aktivierter Firewall kann zusätzlich bestimmt werden, ob Traffic außerhalb des IPSec-Tunnels erlaubt ist oder nicht.

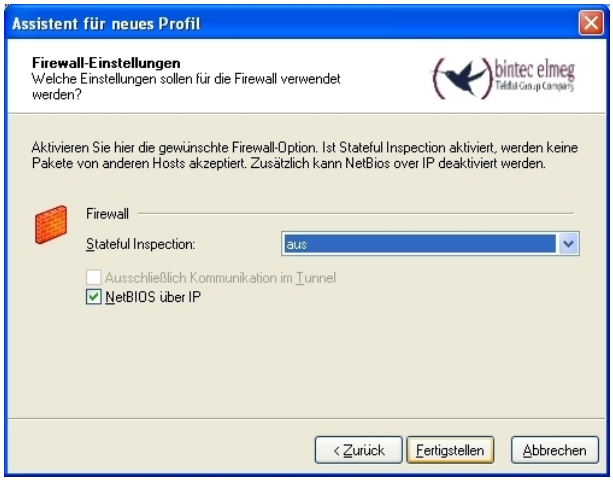


Abb. 106: Firewall

Danach muss noch die IPSec-Pathfinder-Funktion durch das editieren des eben angelegten Profiles seperat aktiviert werden.

(1) Gehen Sie zu **Konfiguration** -> **Profile**.

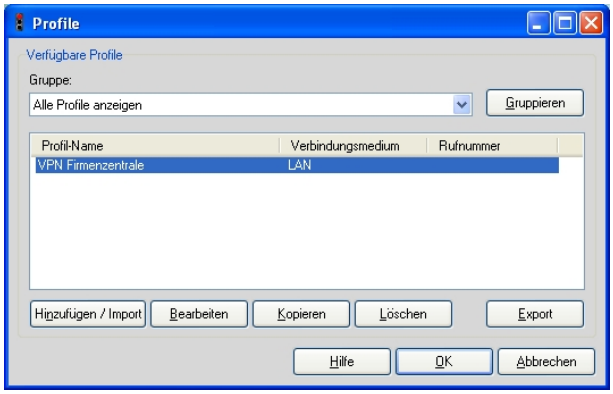


Abb. 107: Verfügbare Profile

Im Menü **Erweiterte IPSec-Optionen** wird die Option *IPSec-Pathfinder-Funktion* aktiviert.

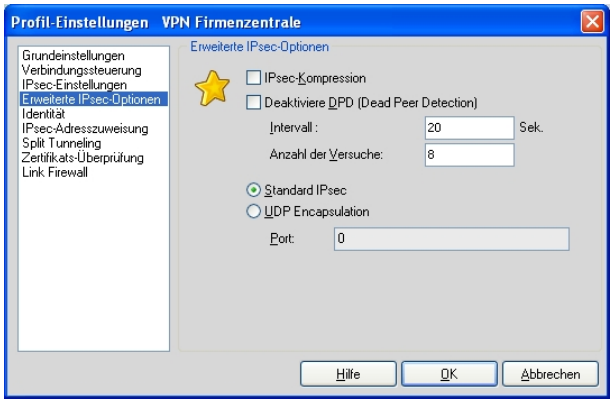


Abb. 108: IPSec-Optionen

Falls ein Proxy-Server für die Verbindung zum Internet verwendet wird bietet der **bintec Secure IPSec Client** im Menü **Konfiguration** -> **Proxy für VPN-Pathfinder** die Möglichkeit die Proxy-Server-Einstellungen zu hinterlegen.

5.3 Konfigurationsschritte im Überblick

Anlegen des IP Pools

Feld	Menü	Wert
IP-Poolname	**VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**	z. B. *IPSes Pool*
IP-Poolbereich	**VPN** -> **IPSec** -> **IP Pools** -> **Hinzufügen**	z. B. *192.168.20.1 - 192.168.20.10*

Konfiguration des VPN IPSec-Tunnels

Feld	Menü	Wert
Administrativer Status	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*Aktiv*
Beschreibung	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *VPNClient1*
Peer-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	leeres Feld
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*E-Mail-Adresse* / *User1@bintec-elmeg.com*
Preshared Key	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *test*
IP-Adressenvergabe	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*Server im IKE-Konfigurationsmodus*
IP-Zuordnungspool	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*IPSec Pool*
Lokale IP-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *192.168.0.254*

Aktivieren der IPSec-Pathfinder-Funktion

Feld	Menü	Wert
IPSec-Pathfinder-Modus	**VPN** -> **IPSec** -> **Optionen** -> **Erweiterte Einstellungen**	*Aktiviert*

Konfiguration des bintec Secure IPSec Clients

Feld	Menü	Wert
Verbindungstyp	**Assistent für neues Profil**	*Verbindung zum Firmennetz über IPSec*
Profil-Name	**Assistent für neues Profil**	*VPN Firmenzentrale*
Verbindungsmedium	**Assistent für neues Profil**	*LAN (over IP)*
Gateway	**Assistent für neues Profil**	z. B. *vpngate-*

Feld	Menü	Wert
(Tunnel-Endpunkt)		*way.bintec-elmeg.com*
Austausch-Modus	**Assistent für neues Profil**	Aggressive Mode
PFS-Gruppe	**Assistent für neues Profil**	DH-Gruppe 2 (1024 Bit)
Shared Secret	**Assistent für neues Profil**	z. B. *test*
Shared Secret (Wiederholung)	**Assistent für neues Profil**	z. B. *test*
Typ	**Assistent für neues Profil**	z. B. *Fully Qualified Username*
ID	**Assistent für neues Profil**	z. B. *User1@bintec-elmeg.com*
IP-Adressen-Zuweisung	**Assistent für neues Profil**	*IKE Config Mode verwenden*
Stateful Inspection	**Assistent für neues Profil**	*aus*
IPSec-Pathfinder-Funktion	**Assistent für neues Profil**	Aktiviert

Kapitel 6 Sicherheit - IPSec mit Zertifikaten

6.1 Einleitung

Im Folgenden wird die Konfiguration einer IPSec-Verbindung mit dynamischen IP-Adressen auf beiden Seiten beschrieben.

Zur Authentifizierung verwenden Sie anstelle des Preshared Keys die Zertifikate. Außerdem werden Sie einen Eintrag für Ihren DynDNS-Namen im Gateway konfigurieren.

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

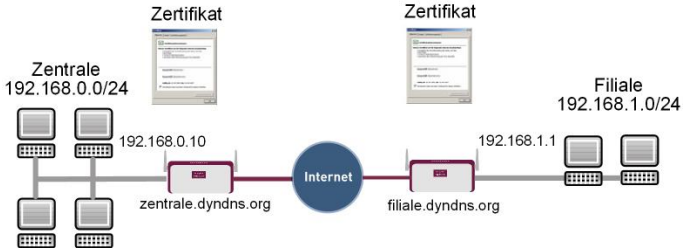


Abb. 109: Beispielszenario IPSec mit Zertifikaten

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration der Gateways, z. B. **bintec be.IP plus**
- Für das IPSec-Gateway ist ein Bootimage ab der Version 10.1.1 zu verwenden
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider
- Für beide Gateways müssen Sie einen DynDNS-Namen, z. B. *zentrale.dyndns.org* und *filiale.dyndns.org*, registriert haben
- Sie brauchen eine Zertifizierungsstelle, bei der Sie Ihre Zertifikate anfordern können. Informieren Sie sich bei der von Ihnen gewählten Zertifizierungsstelle über die notwendigen Angaben für die Zertifikatsanforderung und die Methode der Übermittlung der Anforderung.

6.2 Konfiguration

In unserem Beispiel wird die Konfiguration in der Zentrale beschrieben.

Hinweis

Da die Zertifikats-Implementierung sehr komplex ist, wird empfohlen erst eine funktionsfähige IPSec-Verbindung, z. B. mit dynamischen IP-Adressen, zu konfigurieren und diese dann mit Zertifikaten zu erweitern und anzupassen.

6.2.1 IPSec-Peer erstellen

Im Menü **IPSec-Peers** haben Sie die Möglichkeit mit **Neu** einen neuen Verbindungspartner für IPSec hinzuzufügen.

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

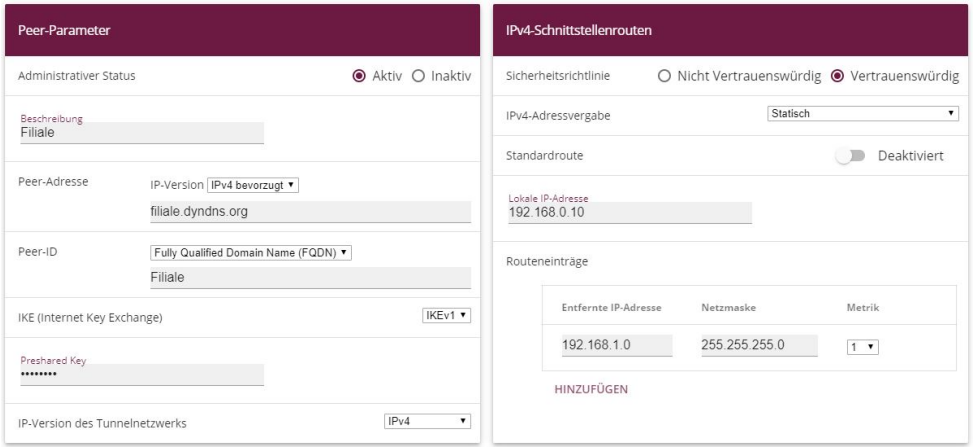


Abb. 110: **VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**

Gehen Sie folgendermaßen vor, um die Einstellungen für den IPSec-Peer vorzunehmen:

(1) Bei **Beschreibung** geben Sie eine Beschreibung für die Verbindung ein, z. B. *Filiale* .

(2) Bei **Peer-Adresse** geben Sie die Gateway-IP-Adresse oder DynDNS-Namen des Verbindungspartners ein, z. B. *filiale.dyndns.org* .

(3) Bei **Peer-ID** belassen Sie *Fully Qualified Domain Name (FQDN)* und geben Sie eine Identifikation für den Partner ein, z. B. *Filiale* .

(4) Im **Preshared Key** tragen Sie das gemeinsame Passwort für die Verbindung ein, z. B. *bintec* .

(5) Deaktivieren Sie die Option **Standardroute**.

(6) Unter **Lokale IP-Adresse** tragen Sie *192.168.0.10* ein

(7) Tragen Sie bei **Entfernte IP-Adresse** das zu erreichende Partnernetz, z. B. *192.168.1.0* und in **Netzmaske** *255.255.255.0* ein.

(8) Bestätigen Sie Ihre Eingaben mit **OK**.

Hinweis

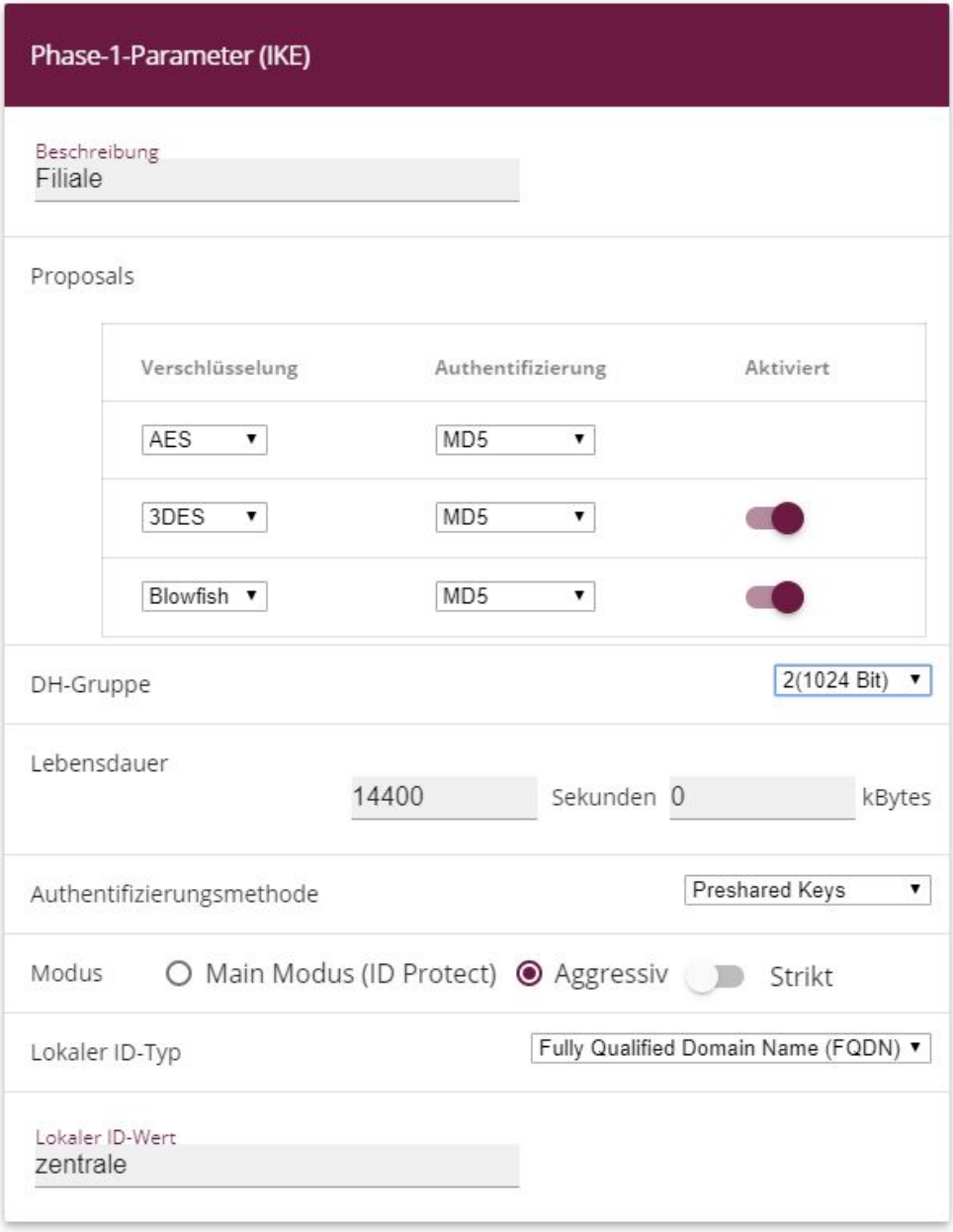
Da Sie später für Ihre Verbindung die Zertifikate einsetzen werden, spielt für die temporäre Verbindung die Komplexität der Preshared Keys keine Rolle.

Durch das anlegen eines IPSec-Peers werden automatisch Standardprofile für Phase 1 und Phase 2 erstellt, die im Folgenden auf die Anforderungen dieses Szenarios angepasst werden.

6.2.2 Anpassen des Phase-1-Profils

Gehen Sie in folgendes Menü, um das Profil für die Phase 1 anzupassen:

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


Phase-1-Parameter (IKE)
Beschreibung
Filiale
Proposals
Verschlüsselung
Authentifizierung
Aktiviert
AES
MD5
3DES
MD5
Blowfish
MD5
DH-Gruppe
2(1024 Bit)
Lebensdauer
14400
Sekunden
0
kBytes
Authentifizierungsmethode
Preshared Keys
Modus
Main Modus (ID Protect)
Aggressiv
Strikt
Lokaler ID-Typ
Fully Qualified Domain Name (FQDN)
Lokaler ID-Wert
zentrale

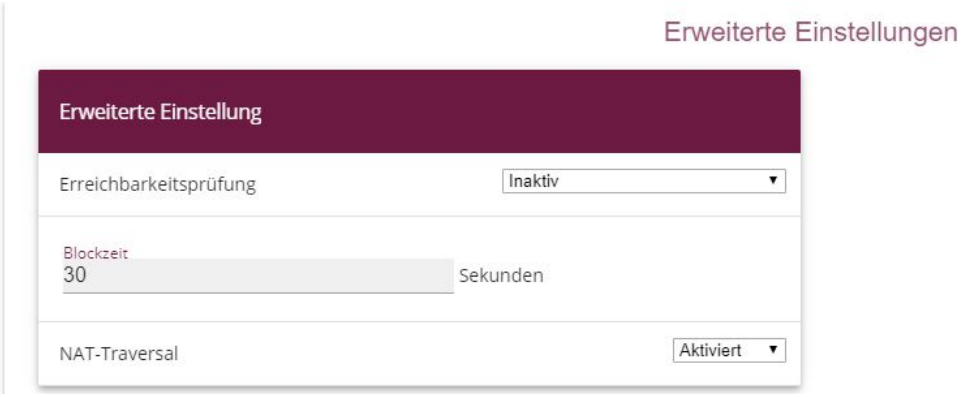


Abb. 112: **VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** ->

Konfigurieren Sie das Phase-1-Profil mit folgenden Parametern:

(1) Bei **Beschreibung** geben Sie einen Namen für das Profil ein, z. B. *Filiale* .

(2) Wählen Sie bei **Proposals Verschlüsselung** *AES*, bei **Authentifizierung** *MD5* .
Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.

(3) Den **Modus** stellen Sie auf *Aggressiv* da Sie dynamische IP-Adressen nutzen.

(4) Unter **Lokaler ID-Typ** wählen Sie *Fully Qualified Domain Name (FQDN)* aus.

(5) Unter **Lokaler ID-Wert** geben Sie die lokale ID des Gateways ein, z. B. *Zentrale* (steht beim Partner unter Peer-ID).

(6) Klicken Sie auf **Erweiterte Einstellungen**.

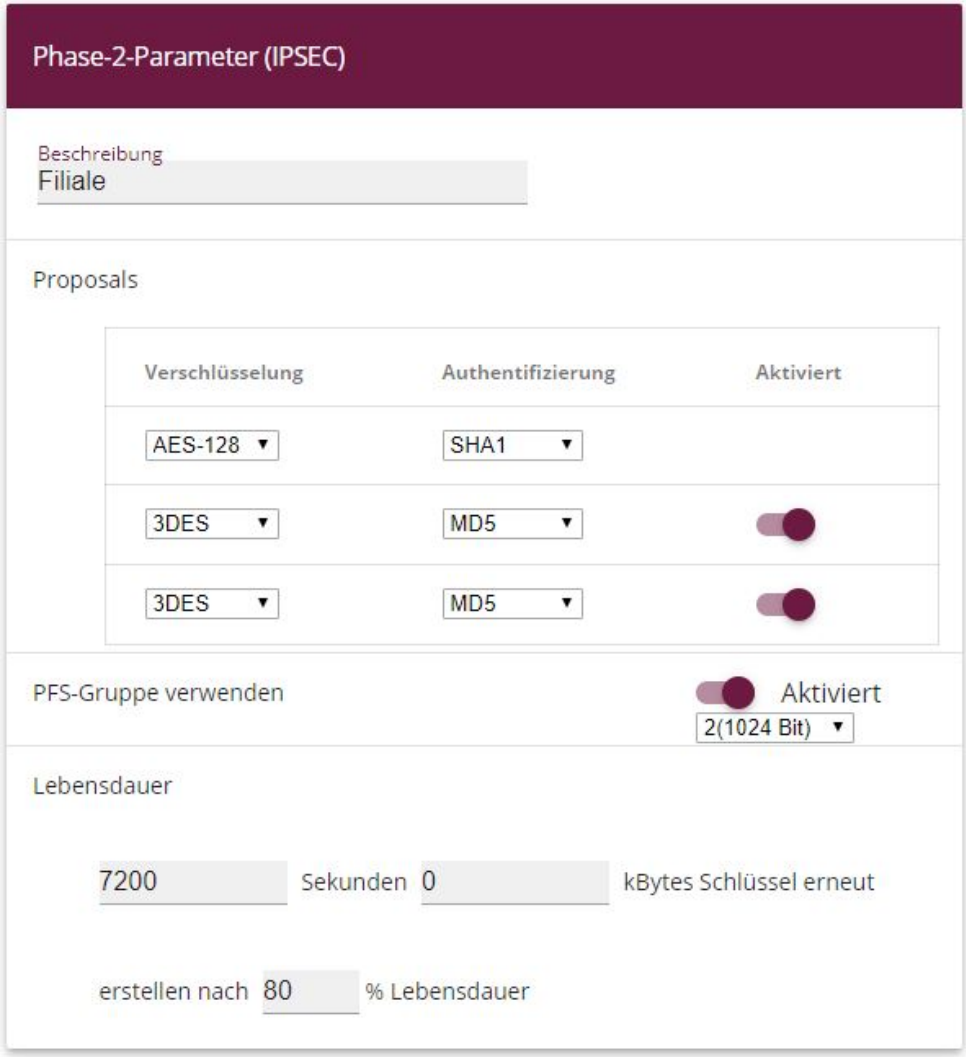
(7) Wählen Sie bei **Erreichbarkeitsprüfung** *Inaktiv*.

(8) Bestätigen Sie mit **OK**.

6.2.3 Anpassen des Phase-2-Profils

Gehen Sie in folgendes Menü, um das Profil für die Phase 2 anzupassen:

(1) Gehen Sie zu **VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** -> .


Phase-2-Parameter (IPSEC)
Beschreibung
Filiale
Proposals
Verschlüsselung
Authentifizierung
Aktiviert
AES-128
SHA1
3DES
MD5
3DES
MD5
PFS-Gruppe verwenden
Aktiviert
2(1024 Bit)
Lebensdauer
7200
Sekunden
0
kBytes Schlüssel erneut
erstellen nach
80
% Lebensdauer

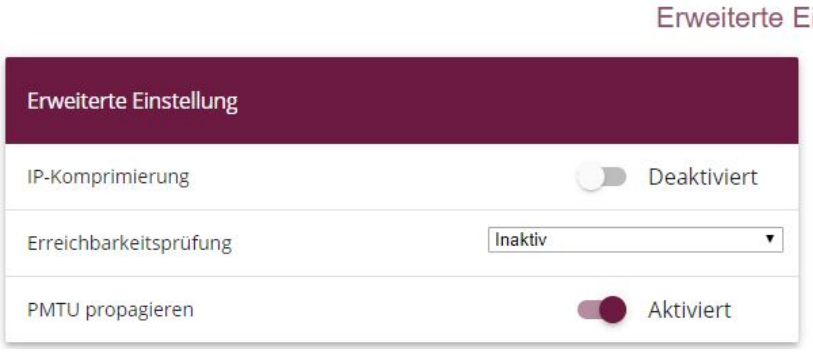


Abb. 114: **VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** ->

Konfigurieren Sie das Phase-2-Profil mit folgenden Parametern:

(1) Bei **Beschreibung** geben Sie einen Namen für das Profil ein, z. B. *Filiale* .

(2) Wählen Sie bei **Proposals Verschlüsselung** *AES-128*, bei **Authentifizierung** *MD5*. Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.

(3) Klicken Sie auf **Erweiterte Einstellungen**.

(4) **Erreichbarkeitsprüfung** setzen Sie auf *Inaktiv*.

(5) Bestätigen Sie mit **OK**.

6.2.4 DynDNS konfigurieren

Erstellen Sie für Ihren registrierten DynDNS Namen, z. B. *zentrale.dyndns.org* , einen Eintrag im Gateway.

Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**.

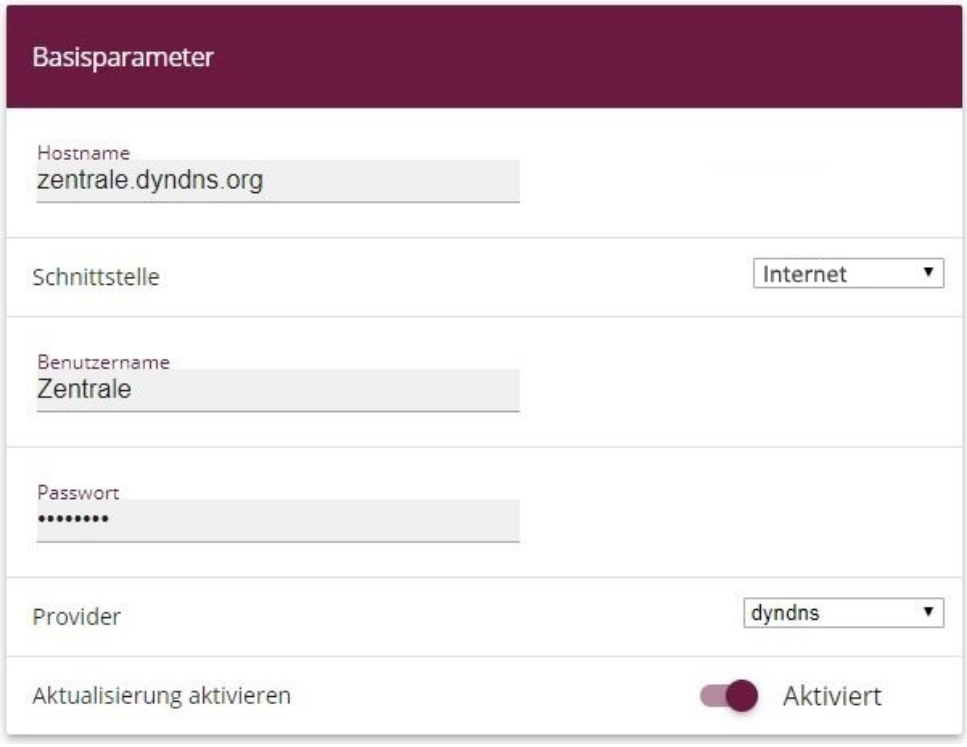


Abb. 115: **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Unter **Hostname** tragen Sie den kompletten Hostnamen den Sie registriert haben ein, z. B. *zentrale.dyndns.org* .

(2) Wählen Sie bei **Schnittstelle** z. B. *Internet* aus.

(3) Tragen Sie unter **Benutzername** z. B. *Zentrale* ein.

(4) Bei **Passwort** geben Sie z. B. *passwort* an.

(5) Der **Provider** bleibt *dyndns*.

(6) Aktivieren Sie **Aktualisierung aktivieren**.

(7) Bestätigen Sie mit **OK**.

Nachdem Sie die IPSec-Verbindung und den DynDNS-Eintrag konfiguriert haben, sollten Sie einen Verbindungstest durchführen. War dieser erfolgreich, passen Sie nun wie folgt die Authentifizierungsparameter an: ein Zertifikat wird angefordert und importiert.

6.2.5 Zertifikate anfordern und importieren

Gehen Sie in folgendes Menü, um eine Zertifikatsanforderung zu konfigurieren:

(1) Gehen Sie zu **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsliste** -> **Anforderung**.

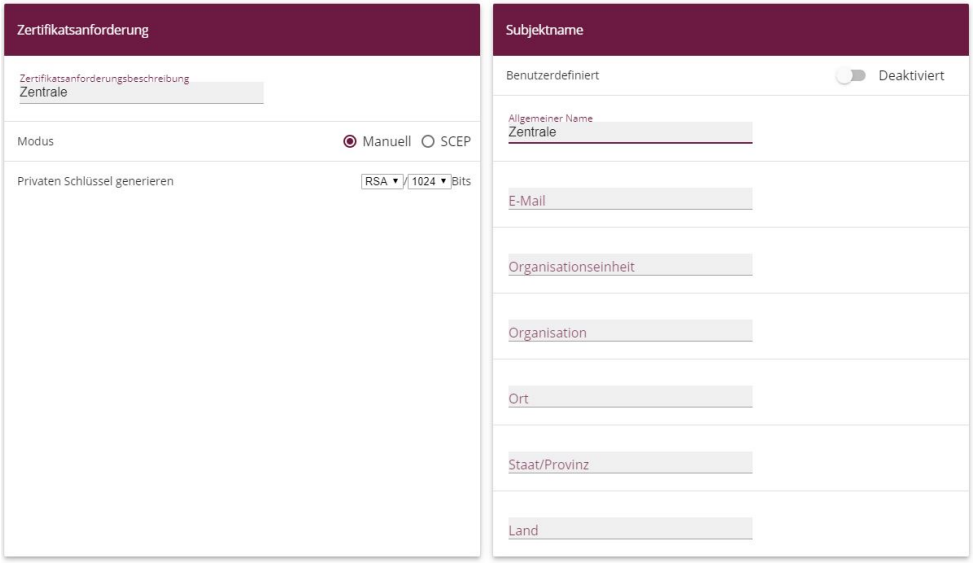


Abb. 116: **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsliste** -> **Anforderung**

Hinweis

Unter Subjektname können Sie wesentlich mehr Identifikationsmerkmale nach dem X.500-Standard für die Zentrale angeben. Der Einfachheit halber wird hier nur ein Merkmal verwendet.

Beachten Sie gegebenenfalls die Anforderungen Ihrer Zertifizierungsstelle.

Gehen Sie folgendermaßen vor:

(1) Unter **Zertifikatsanforderungsbeschreibung** geben Sie z. B. `Zentrale` ein.

(2) Den **Modus** belassen Sie auf `Manuell`.

(3) Bei **Allgemeiner Name** tragen Sie die Identifikation der Zentrale ein, z. B. `Zentrale` .

(4) Bestätigen Sie Ihre Eingaben mit **OK**.

(1) Gehen Sie zu **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsliste**.

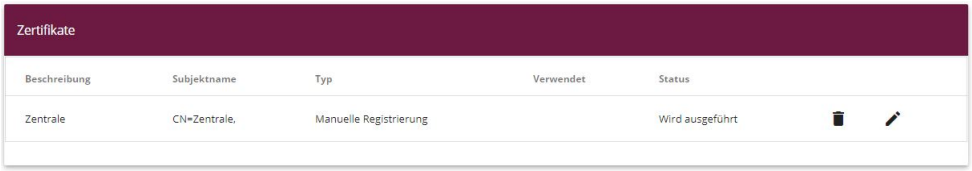


Abb. 117: **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsliste**

Im Hintergrund generiert das IPSec-Gateway den privaten und den öffentlichen Schlüssel.

Sie fahren nun wie folgt fort:

(1) Es sollte sich ein Fenster öffnen, das Sie auffordert, die Zertifikatsanforderungen auf Ihrem Computer unter dem Namen *Zentrale.req* zu speichern. Optional besteht die Möglichkeit, über den rechten grünen Pfeil die Datei zu sichern.

(2) Nun müssen Sie mit der Zertifikatsanforderung bei Ihrer Zertifizierungsstelle ein Zertifikat anfordern. Folgen Sie dazu den Anweisungen Ihrer Zertifizierungsstelle.
Die Anforderung sieht z. B. aus wie folgt:

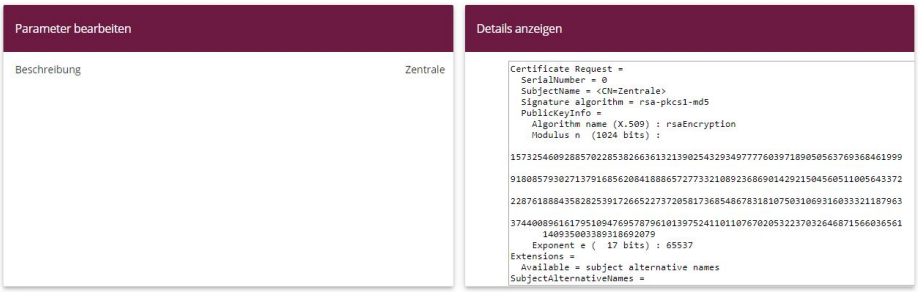


Abb. 118: **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsliste**

(3) Das Zertifikat, das die Zertifizierungsstelle ausstellt, müssen Sie nun auf den Computer kopieren.

(4) Benennen Sie das Zertifikat *Zentrale.crt* .

(5) Sie brauchen ausserdem das Zertifikat der Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Kopieren Sie auch dieses auf den Computer.

(6) Benennen Sie das Zertifikat der Zertifizierungsstelle *Ca.crt*.

Danach gehen sie in folgendes Menü, um Ihr eigenes Zertifikat und das Zertifizierungsstellen-Zertifikat in das IPSec-Gateway zu importieren:

(1) Gehen SIe zu **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsliste** -> **Importieren**.

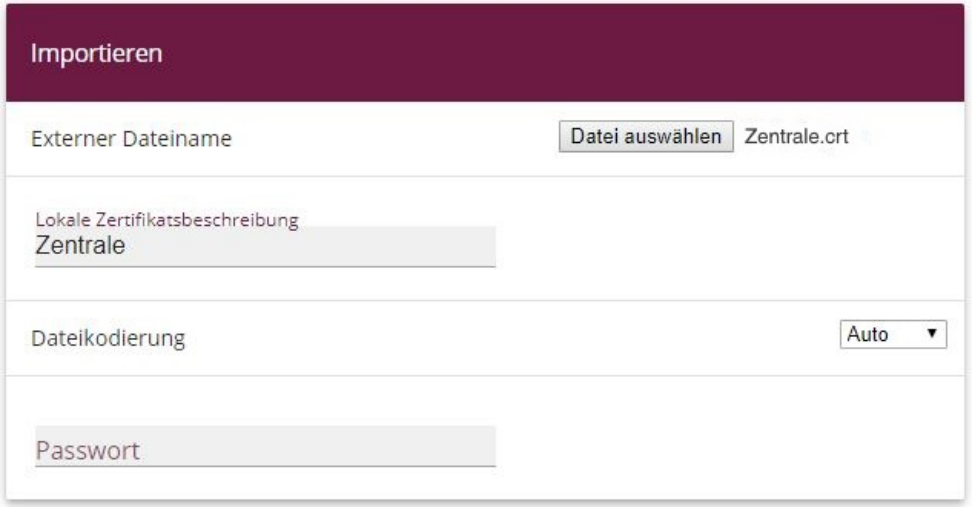


Abb. 119: **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsliste** -> **Importieren**

Gehen Sie folgendermaßen vor, um das eigene Zertifikat zu importieren:

(1) Unter **Externer Dateiname** wählen Sie über die **Durchsuchen..**.-Schaltfläche die Datei aus z. B. `C:\Zentrale.crt` .

(2) Bei **Lokale Zertifikatsbeschreibung** geben Sie z. B. `Zentrale` an.

(3) Bestätigen Sie Ihre Eingaben mit **OK**.

Gehen Sie folgendermaßen vor, um das Zertifikat der Zertifizierungsstelle zu importieren:

(1) Unter **Externer Dateiname** wählen Sie über die **Durchsuchen..**.-Schaltfläche die Datei aus z. B. `C:\Ca.crt` .

(2) Bei **Lokale Zertifikatsbeschreibung** geben Sie z. B. `CA` an.

(3) Bestätigen Sie Ihre Eingaben mit **OK.**

6.2.6 IPSec-Verbindung anpassen

Um die importierten Zertifikate nutzen zu können, müssen Sie in folgendem Menü Anpassungen vornehmen:

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

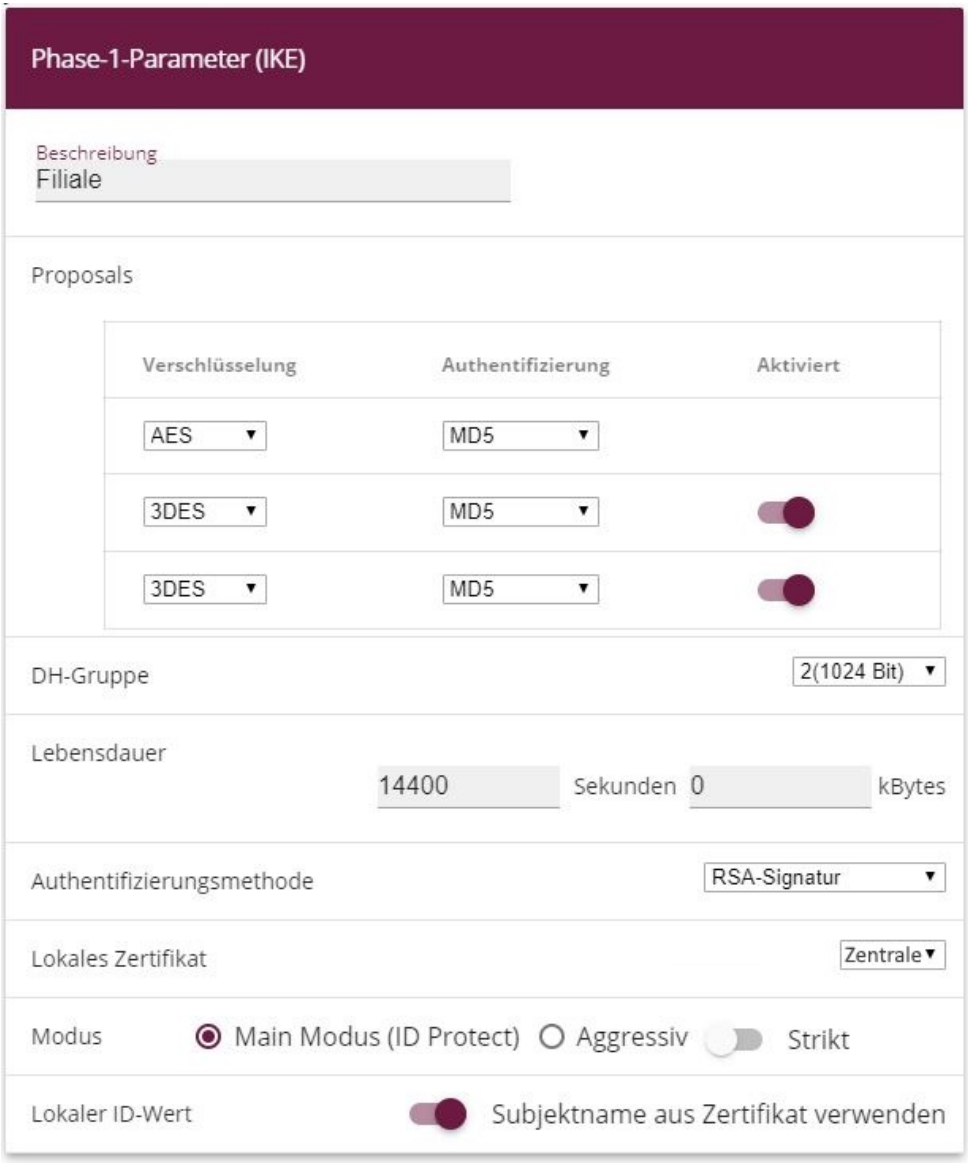


Abb. 120: **VPN** -> **IPSec** -> **Phase-1 -Profile** -> **<Filiale>** -> ✎

Gehen Sie folgendermaßen vor, um den Eintrag zu verändern:

(1) Unter **Authentifizierungsmethode** wählen Sie *RSA-Signatur*.

(2) Als **Lokales Zertifikat** wählen Sie das eigene Zertifikat aus, hier *Zentrale*.

(3) Den **Modus** stellen Sie auf *Main Modus (ID Protect)*.

(4) Unter **Lokaler ID-Wert** setzen Sie den Haken auf *Subjektname aus Zertifikat*

verwenden.

(5) Bestätigen Sie Ihre Eingaben mit **OK.**

Ein weiteres Menü erfordert Anpassungen für die Verwendung von Zertifikaten:

(1) Gehen Sie zu **VPN** -> **IPSec** -> **IPSec-Peers** -> **<Filiale>** -> ✎.

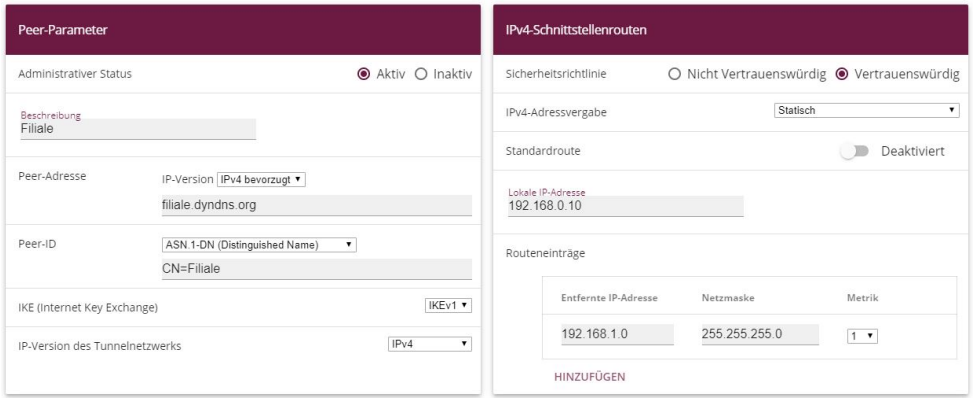


Abb. 121: **VPN** -> **IPSec** -> **IPSec-Peers** -> **<Filiale>** -> ✎

Gehen Sie folgendermaßen vor, um den Eintrag zu ändern:

(1) Unter **Peer-ID** wählen Sie die Identifikation des Partners ein (in der Filiale unter **Lokale ID** eingetragen) z. B. *ASN.1-(Distinguished Name)* aus und geben z. B. *CN=Filiale* ein.

(2) Bestätigen Sie Ihre Eingaben mit **OK.**

6.3 Ergebnis

Sie haben eine IPSec-Verbindung mit Zertifikaten zwischen zwei Gateways konfiguriert. Dazu haben Sie dynamische IP-Adressen in Kombination mit DynDNS verwendet. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter auf der Filialseite konfigurieren.

6.4 Kontrolle

Um die IPSec-Verbindung zu testen, gehen Sie in folgendes Menü:

(1) Gehen Sie zu **Wartung** -> **Diagnose** -> **Ping-Test**.

Nachdem Sie eine IP-Adresse des entfernten Standorts bei **Ping-Befehl testweise an Adresse senden** eingegeben und die **Los**-Schaltfläche gedrückt haben, sollten Sie eine

ähnliche Meldung erhalten:

Abb. 122: **Wartung** -> **Diagnose** -> **Ping-Test**

Hinweis

Sollte die Verbindung nicht ordnungsgemäß aufgebaut werden, könnte das mit den Einstellungen für das lokale Datum oder die lokale Uhrzeit des Gateways zusammenhängen. Überprüfen Sie das aktuelle Datum damit die Zertifikate gültig sind.

6.5 Konfigurationsschritte im Überblick

IPSec-Peer anlegen

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *Filiale*
Peeradresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*filiale.dyndns.org*
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*Fully Qualified Domain Name (FQDN)* und *Filiale*
Preshared Key	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *bintec*
Standardroute	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*Deaktiviert*
Lokale IP-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *192.168.0.10*
Routeneinträge	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	für **IP-Adresse** *192.168.1.0* und für *255.255.255.* **Netzmaske** *0*

Phase-1-Profil anpassen

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** -> ✎	z. B. *Filiale*
Proposals	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** -> ✎	*AES/MD5*
Modus	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** -> ✎	*Aggresiv*
Lokaler ID-Typ	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** -> ✎	*Fully Qualified Domain Name (FQDN)*
Lokaler ID-Wert	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** -> ✎	*Zentrale*
Erreichbarkeitsprüfung	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Multi-Proposal>** -> ✎ -> **Erweiterte Einstellungen**	*Inaktiv*

Phase-2-Profile anpassen

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** -> ✎	z. B. *Filiale*
Proposal	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** -> ✎	*AES-128/MD5*
Erreichbarkeitsprüfung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **<Multi-Proposal>** -> ✎ -> **Erweiterte Einstellungen**	*Inaktiv*

DynDNS

Feld	Menü	Wert
Hostname	**Lokale Dienste** -> **DynDNS-**	z. B. *zentra-*

Feld	Menü	Wert
	Client -> **DynDNS-Aktualisierung** -> **Neu**	*le.dyndns.org*
Schnittstelle	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *Internet*
Benutzername	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *Zentrale*
Passwort	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *passwort*
Provider	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	*dyndns*
Aktualisierung aktivieren	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	Aktiviert

Zertifikate anfordern und importieren

Feld	Menü	Wert
Zertifikatsanforderungsbeschreibung	**Systemverwaltung** -> **Zertifikate** -> **Anforderung**	z. B. *Zentrale*
Modus	**Systemverwaltung** -> **Zertifikate** -> **Anforderung**	*Manuell*
Allgemeiner Name	**Systemverwaltung** -> **Zertifikate** -> **Anforderung**	z. B. *Zentrale*
Externer Dateiname	**Systemverwaltung** -> **Zertifikate** -> **Importieren**	z. B. *C:\Zentrale.crt*
Lokale Zertifikatsbeschreibung	**Systemverwaltung** -> **Zertifikate** -> **Importieren**	z. B. *Zentrale*
Externer Dateiname	**Systemverwaltung** -> **Zertifikate** -> **Importieren**	z. B. *C:\Ca.crt*
Lokale Zertifikatsbeschreibung	**Systemverwaltung** -> **Zertifikate** -> **Importieren**	z. B. *CA*

IPSec-Verbindung anpassen

Feld	Menü	Wert
Authentifizierungsmethode	**VPN** -> **IPSec** -> **Phase-**	*RSA-Signatur*

Feld	Menü	Wert
	1-Profile -> **<Filiale>** ->	
Lokales Zertifikat	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Filiale>** ->	*Zentrale*
Modus	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Filiale>** ->	*Main Modus (ID Protect)*
Lokaler ID-Wert	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **<Filiale>** ->	*Subjektname aus Zertifikat verwenden*

IPSec-Peers anpassen

Feld	Menü	Wert
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** -> **<Filiale>** ->	*ASN.1-DN (Distinguished Name)* und *CN=Filiale*

Ping-Test

Feld	Menü	Wert
Ping-Befehl testweise an Adresse senden	**Wartung** -> **Diagnose** -> **Ping-Test**	*192.168.0.10*

Kapitel 7 Sicherheit - IPSec mit dynamischen IP-Adressen und DynDNS

7.1 Einleitung

Dieses Kapitel beschreibt eine IPSec-Konfiguration an bintec Routern (hier **bintec be.IP plus**), um eine sichere IPSec-Verbindung zwischen zwei Netzwerken zu ermöglichen.

Die Nutzung dynamischer IP-Adressen hat den Nachteil, dass ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. DynDNS sorgt dafür, dass Ihr Gerät auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

Als Authentifizierung wird Preshared Keys verwendet.

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

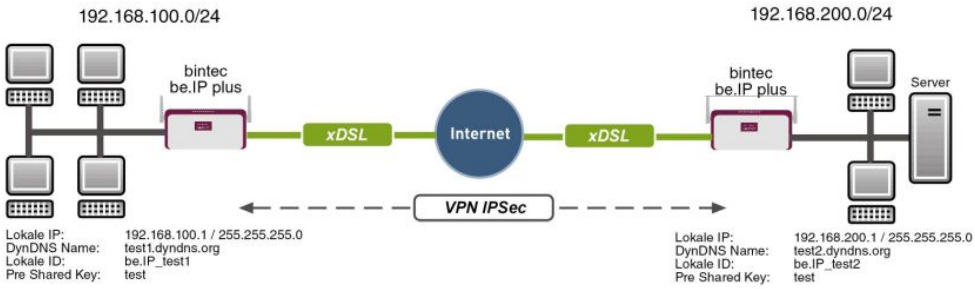


Abb. 123: Beispielszenario

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Zwei bintec Router (z. B. **bintec be.IP plus**) mit Systemsoftware 10.1.1
- Beide Router haben eine bestehende Verbindung zum Internet-Provider
- In diesem Beispiel sind die beiden Router über eine A-DLS-Flatrate mit dem Internet verbunden
- Beide Router bekommen dynamisch eine offizielle IP-Adresse zugewiesen und haben einen DynDNS-Account eingerichtet

7.2 Konfiguration

7.2.1 Konfiguration am ersten Router (Standort A)

DynDNS-Account einrichten

Im Menü DynDNS-Aktualisierung wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt. Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Registrierungen vorzunehmen.

(1) Gehen Sie zu **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**.

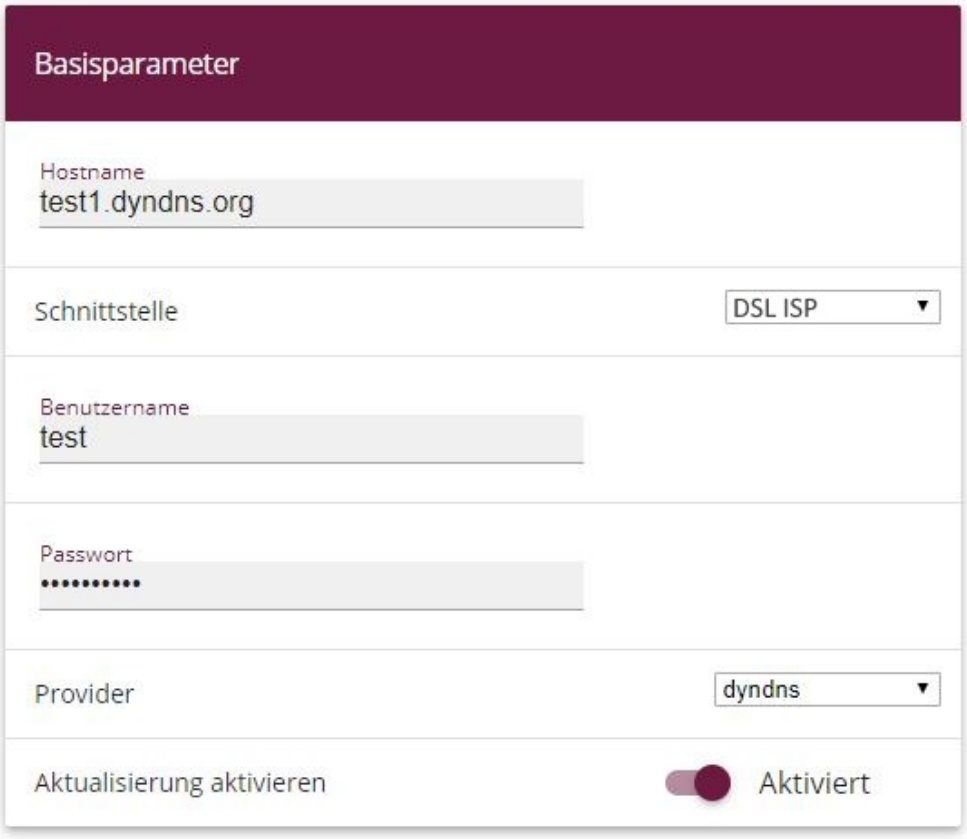


Abb. 124: **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Unter **Hostname** tragen Sie den vollständigen Hostnamen ein, wie er beim DynDNS-Provider registriert ist, z. B. *test1.dyndns.org*.

(2) Wählen Sie die WAN-**Schnittstelle** aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. *DSL ISP*, die Schnittstelle des Internet Service Providers).

(3) Geben Sie den **Benutzernamen** ein, wie er beim DynDNS-Provider registriert ist.

(4) Geben Sie das **Passwort** ein, wie es beim DynDNS-Provider registriert ist.

(5) Wählen Sie den DynDNS-**Provider** aus, bei dem oben genannte Daten registriert sind.

(6) Aktivieren Sie die Funktion **Aktualisierung aktivieren**, der hier konfigurierte DynDNS-Eintrag wird aktiviert.

(7) Bestätigen Sie mit **OK**.

IPSec-Peer-Konfiguration

Als Peer wird ein Endpunkt einer Kommunikation in einem Computernetzwerk bezeichnet.

Wählen Sie die Schaltfläche **Neu**, um einen neue IPSec-Peer einzurichten.

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

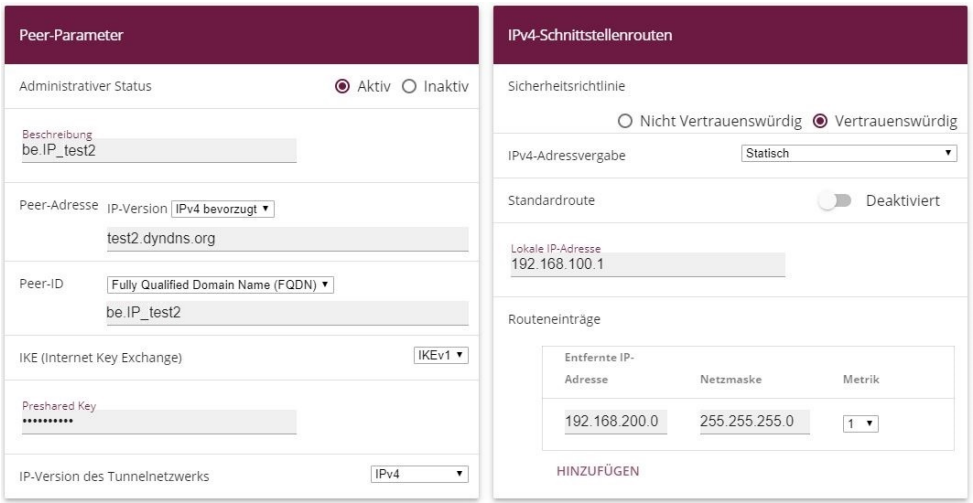


Abb. 125: **VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**

Gehen Sie folgendermaßen vor, um die Einstellungen für den IPSec-Peer vorzunehmen:

(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) Geben Sie eine **Beschreibung** des Peers ein, die diesen identifiziert.

(3) Geben Sie die **Peer-Adresse** der Gegenstelle an (hier der DynDNS Account der bi.IP).

(4) Die **Peer-ID** muss mit dem **Lokalen ID-Wert** der Gegenstelle übereinstimmen. Wählen Sie *Full Qualified Domain Name (FQDN)* aus und geben Sie eine Identifikation für den Partner ein, z. B. *be.IP_test2*.

(5) Bei **Preshared Key** geben Sie ein Passwort für die verschlüsselte Verbindung ein.

(6) Wählen Sie bei **IPv4-Adressvergabe** *Statisch* aus.

(7) Deaktivieren Sie die Option **Standardroute**.

(8) Die **Lokale IP-Adresse** ist die IP-Adresse der LAN-Schnittstelle des Routers.

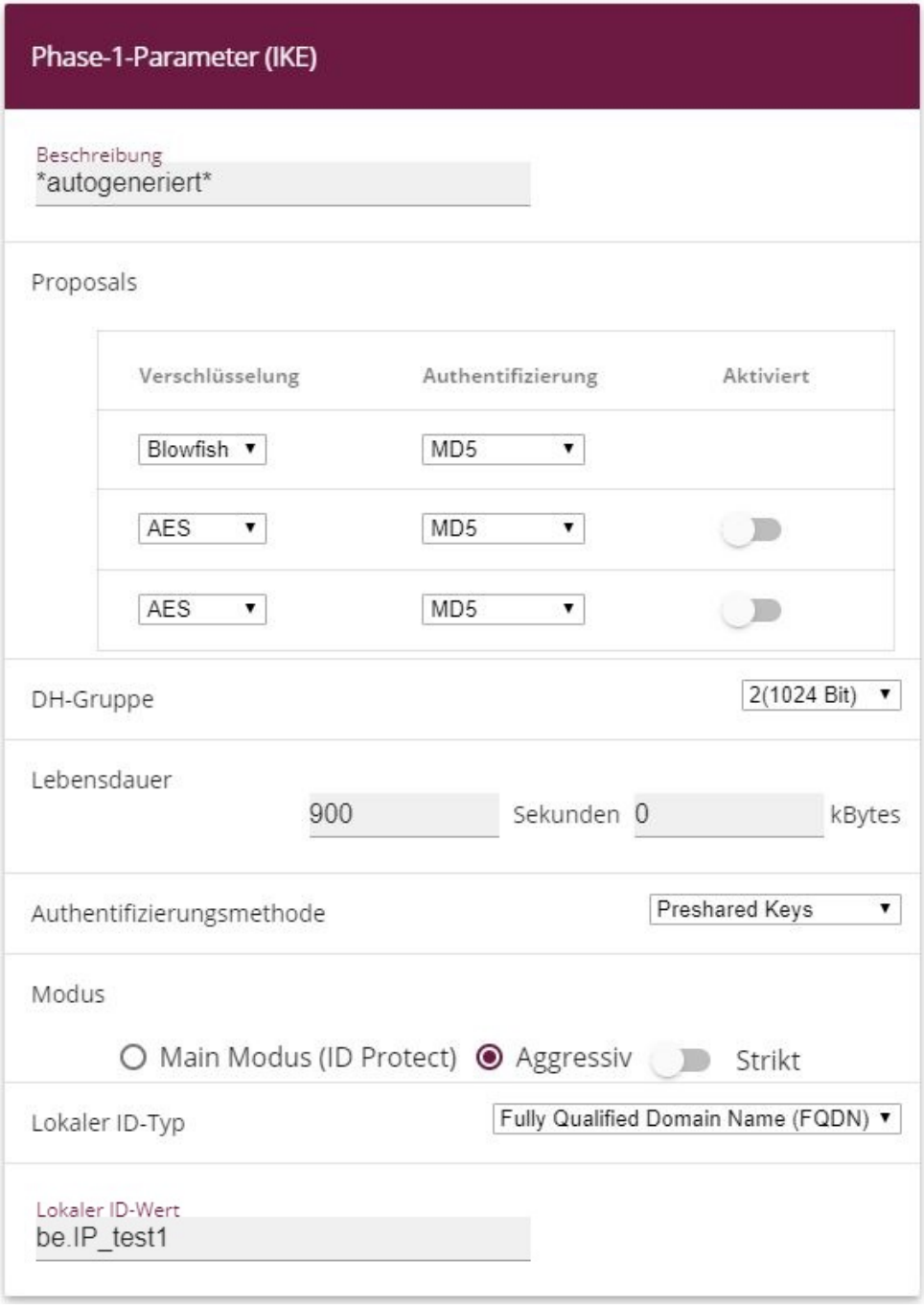
(9) Tragen Sie bei **Entfernte IP-Adresse** das zu erreichende Partnernetz, z. B. *192.168.200.0* und in Netzmaske *255.255.255.0* ein.

(10) Bestätigen Sie Ihre Eingaben mit **OK**.

Phase-1-Profile

Im Menü **Phase-1-Profile** können Sie die Phase 1 (IKE) Einstellungen festlegen. Klicken Sie auf das -Symbol, um vorhanden Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Profile hinzuzufügen.

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


Phase-1-Parameter (IKE)
Beschreibung
autogeneriert
Proposals
Verschlüsselung
Authentifizierung
Aktiviert
Blowfish
MD5
AES
MD5
AES
MD5
DH-Gruppe
2(1024 Bit)
Lebensdauer
900
Sekunden
0
kBytes
Authentifizierungsmethode
Preshared Keys
Modus
Main Modus (ID Protect)
Aggressiv
Strikt
Lokaler ID-Typ
Fully Qualified Domain Name (FQDN)
Lokaler ID-Wert
be.IP_test1

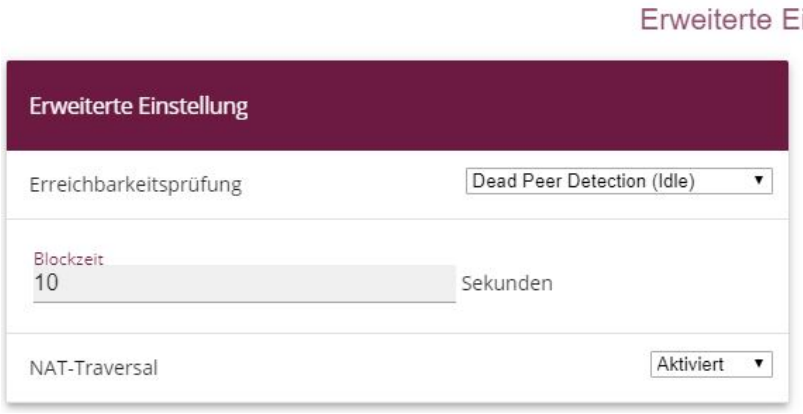


Abb. 127: **VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie eine **Beschreibung** ein, welche die Art der Regel eindeutig identifiziert.

(2) Wählen Sie bei **Proposals Verschlüsselung** *Blowfish* und bei **Authentifizierung** *MD5* ein. Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.

(3) Wählen Sie bei **DH-Gruppe** *2 (1024 Bit) aus.*

(4) Legen Sie die **Lebensdauer** für Phase-1-Schlüssel fest. Geben Sie für die Lebensdauer *900* Sekunden ein. Geben Sie für die Lebensdauer als Menge der verarbeitenden Daten *0* KByts an.

(5) Wählen Sie die **Authentifizierungsmethode** *Preshared Keys* aus.

(6) Den **Modus** stellen Sie auf *Aggressiv* da Sie dynamische IP-Adressen nutzen.

(7) Unter **Lokaler ID-Typ** wählen Sie *Fully Qualified Domain Name (FQDN)* aus.

(8) Unter **Lokaler ID-Wert** geben Sie die lokale ID des Gateways ein, z. B. *be.IP_test1* (steht beim Partner unter Peer-ID).

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

(10) Wählen Sie bei **Erreichbarkeitsprüfung** *Dead Peer Detection (Idle)* aus.

(11) Legen Sie unter **Blockzeit** fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist.

(12) Belassen Sie **NAT-Traversal** auf **Aktiviert**.

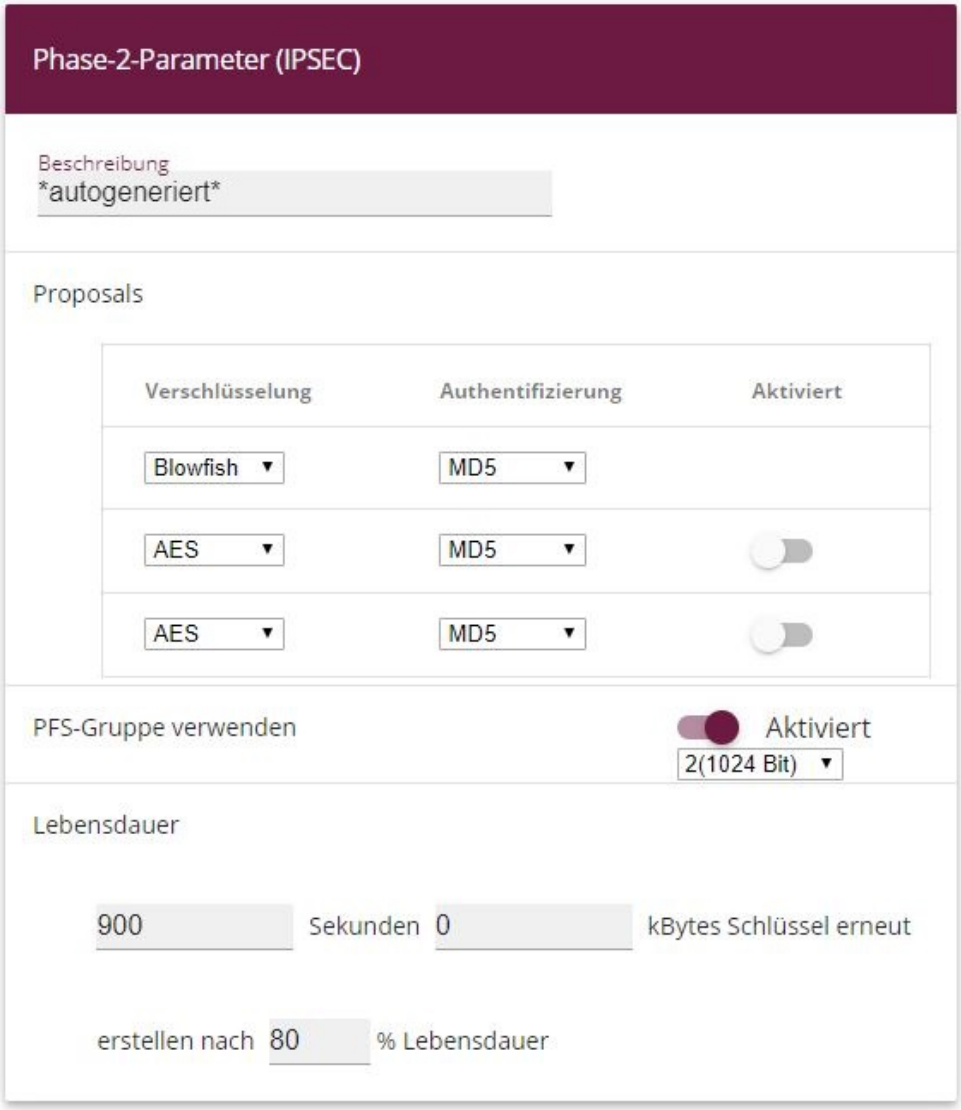
(13) Bestätigen Sie mit **OK**.

Phase-2-Profile

Ebenso wie für Phase 1 können Sie Profile für die Phase 2 des Tunnelaufbaus definieren. Klicken Sie auf das -Symbol, um vorhanden Einträge zu bearbeiten. Wählen Sie die

Schaltfläche **Neu**, um neue Profile hinzuzufügen.

(1) Gehen Sie zu **VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**.



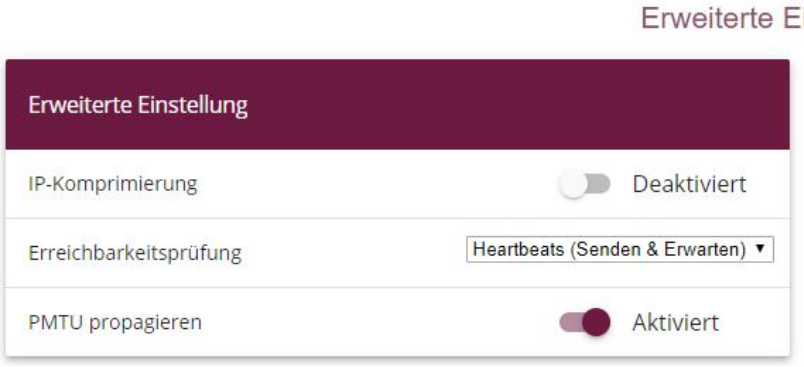


Abb. 129: **VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie eine **Beschreibung** ein, die das Profil eindeutig identifiziert.

(2) Wählen Sie bei **Proposals Verschlüsselung** `Blowfish` , bei **Authentifizierung** `MD5` . Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.

(3) Aktivieren Sie die Option **PFS-Gruppe verwenden** und wählen Sie `2 (1024 Bit)` aus.

(4) Legen Sie die **Lebensdauer** für Phase-2-Schlüssel fest. Geben Sie für die Lebensdauer `900` Sekunden ein. Geben Sie für die Lebensdauer als Menge der verarbeitenden Daten `0` KByts an.

(5) Klicken Sie auf **Erweiterte Einstellungen**.

(6) Wählen Sie bei **Erreichbarkeitsprüfung** `Heartbeats (Senden & Erwarten)` aus.

(7) Aktivieren Sie **PMTU propagieren**.

(8) Bestätigen Sie mit **OK**.

7.2.2 Konfiguration am zweiten Router (Standort B)

DynDNS-Account einrichten

Im Menü DynDNS-Aktualisierung wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt. Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Registrierungen vorzunehmen.

(1) Gehen Sie zu **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**.

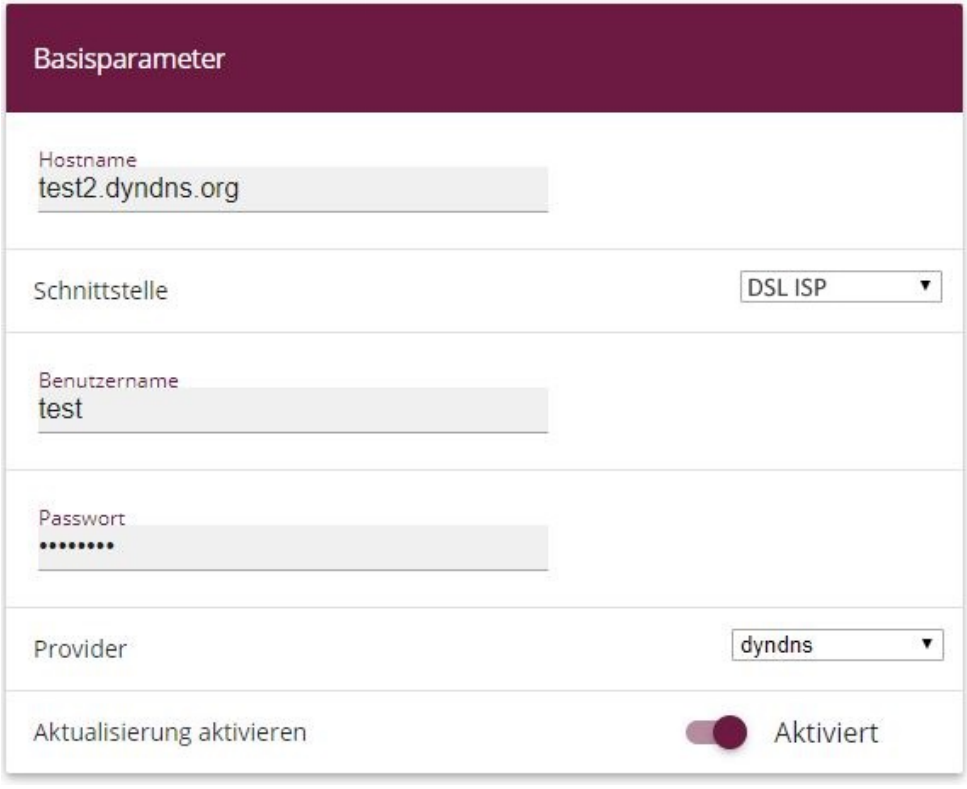


Abb. 130: **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Unter **Hostname** tragen Sie den vollständigen Hostnamen ein, wie er beim DynDNS-Provider registriert ist, z. B. *test2.dyndns.org*.

(2) Wählen Sie die WAN-**Schnittstelle** aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. *DSL ISP*, die Schnittstelle des Internet Service Providers).

(3) Geben Sie den **Benutzernamen** ein, wie er beim DynDNS-Provider registriert ist.

(4) Geben Sie das **Passwort** ein, wie es beim DynDNS-Provider registriert ist.

(5) Wählen Sie den DynDNS-**Provider** aus, bei dem oben genannte Daten registriert sind.

(6) Aktivieren Sie die Funktion **Aktualisierung aktivieren**, der hier konfigurierte DynDNS-Eintrag wird aktiviert.

(7) Bestätigen Sie mit **OK**.

IPSec-Peer-Konfiguration

Als Peer wird ein Endpunkt einer Kommunikation in einem Computernetzwerk bezeichnet.

Wählen Sie die Schaltfläche **Neu**, um einen neue IPSec-Peer einzurichten.

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

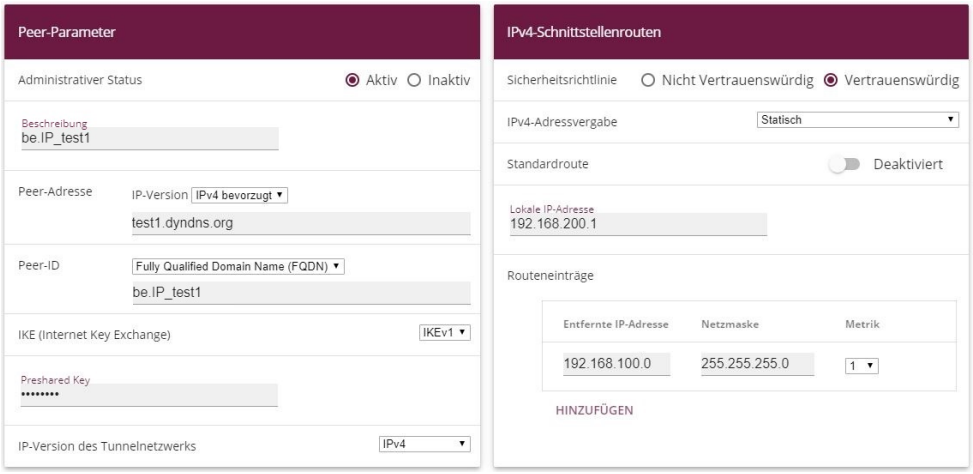


Abb. 131: **VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**

Gehen Sie folgendermaßen vor, um die Einstellungen für den IPSec-Peer vorzunehmen:

(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) Geben Sie eine **Beschreibung** des Peers ein, die diesen identifiziert.

(3) Geben Sie die **Peer-Adresse** der Gegenstelle an (hier der DynDNS Account der bi.IP).

(4) Die **Peer-ID** muss mit dem **Lokalen ID-Wert** der Gegenstelle übereinstimmen. Wählen Sie *Full Qualified Domain Name (FQDN)* aus und geben Sie eine Identifikation für den Partner ein, z. B. *be.IP_test1*.

(5) Bei **Preshared Key** geben Sie ein Passwort für die verschlüsselte Verbindung ein.

(6) Wählen Sie bei **IPv4-Adressvergabe** *Statisch* aus.

(7) Deaktivieren Sie die Option **Standardroute**.

(8) Die **Lokale IP-Adresse** ist die IP-Adresse der LAN-Schnittstelle des Routers.

(9) Tragen Sie bei **Entfernte IP-Adresse** das zu erreichende Partnernetz, z. B. *192.168.100.0* und in Netzmaske *255.255.255.0* ein.

(10) Bestätigen Sie Ihre Eingaben mit **OK**.

Phase-1-Profile

Im Menü **Phase-1-Profile** können Sie die Phase 1 (IKE) Einstellungen festlegen. Klicken Sie auf das -Symbol, um vorhanden Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Profile hinzuzufügen.

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


Phase-1-Parameter (IKE)
Beschreibung
autogeneriert
Proposals
Verschlüsselung
Authentifizierung
Aktiviert
Blowfish
MD5
AES
SHA1
AES
SHA1
DH-Gruppe
2(1024 Bit)
Lebensdauer
900
Sekunden
0
kBytes
Authentifizierungsmethode
Preshared Keys
Modus
Main Modus (ID Protect)
Aggressiv
Strikt
Lokaler ID-Typ
Fully Qualified Domain Name (FQDN)
Lokaler ID-Wert
be.IP_test2

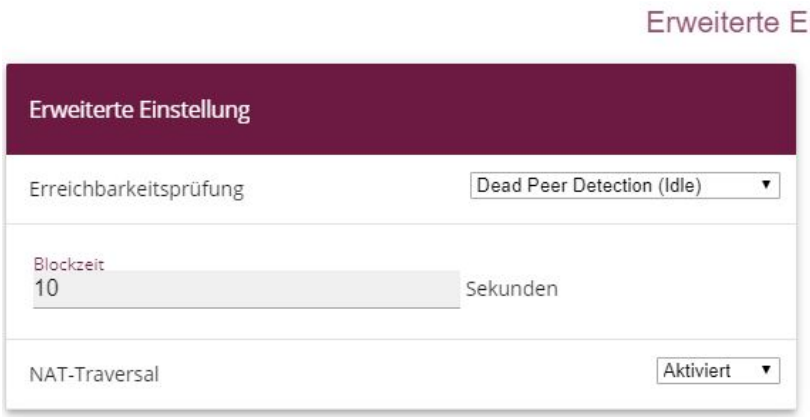


Abb. 133: **VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie eine **Beschreibung** ein, welche die Art der Regel eindeutig identifiziert.

(2) Wählen Sie bei **Proposals Verschlüsselung** *Blowfish* und bei **Authentifizierung** *MD5* ein. Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.

(3) Wählen Sie bei **DH-Gruppe** *2 (1024 Bit) aus.*

(4) Legen Sie die **Lebensdauer** für Phase-1-Schlüssel fest. Geben Sie für die Lebensdauer *900* Sekunden ein. Geben Sie für die Lebensdauer als Menge der verarbeitenden Daten *0* KByts an.

(5) Wählen Sie die **Authentifizierungsmethode** *Preshared Keys* aus.

(6) Den **Modus** stellen Sie auf *Aggressiv* da Sie dynamische IP-Adressen nutzen.

(7) Unter **Lokaler ID-Typ** wählen Sie *Fully Qualified Domain Name (FQDN)* aus.

(8) Unter **Lokaler ID-Wert** geben Sie die lokale ID des Gateways ein, z. B. *be.IP_test2* (steht beim Partner unter Peer-ID).

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

(10) Wählen Sie bei **Erreichbarkeitsprüfung** *Dead Peer Detection (Idle)* aus.

(11) Legen Sie unter **Blockzeit** fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist.

(12) Belassen Sie **NAT-Traversal** auf **Aktiviert**.

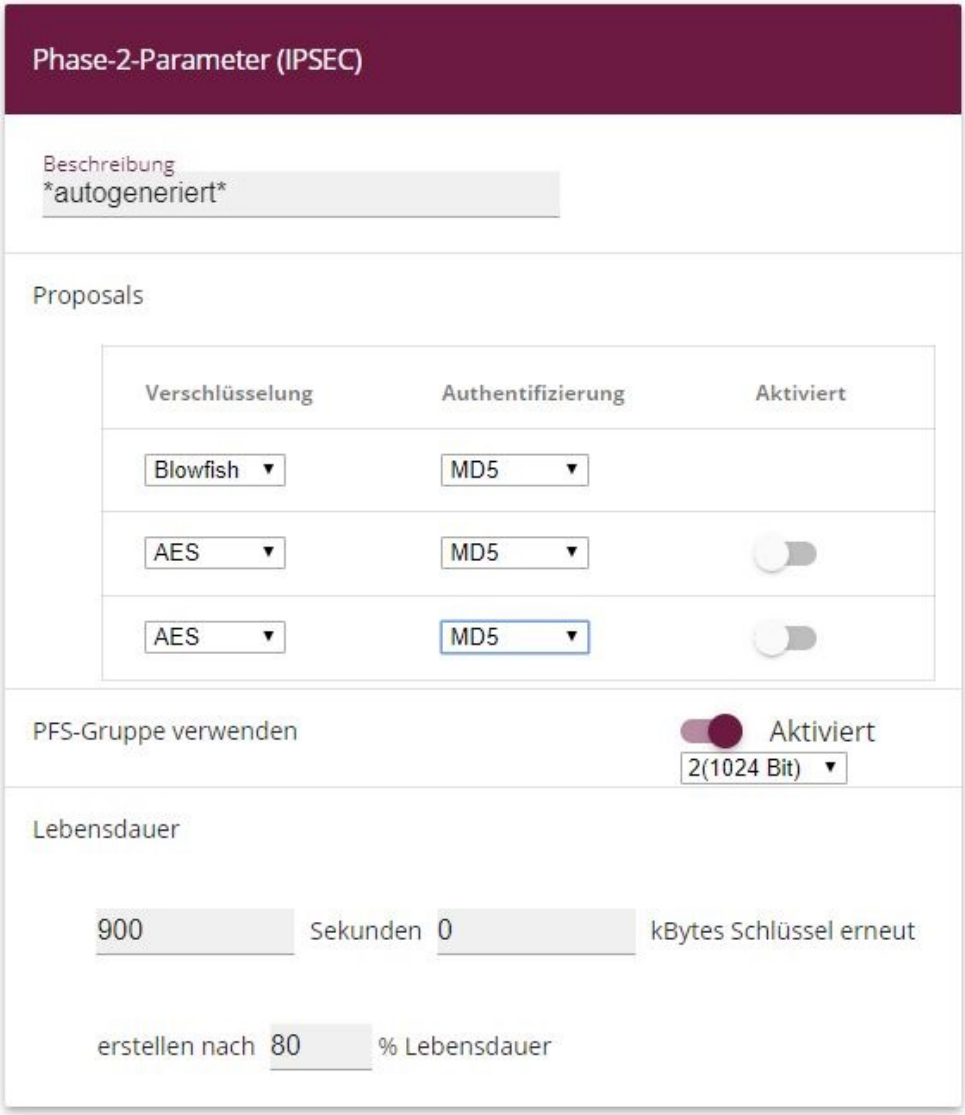
(13) Bestätigen Sie mit **OK**.

Phase-2-Profile

Ebenso wie für Phase 1 können Sie Profile für die Phase 2 des Tunnelaufbaus definieren. Klicken Sie auf das -Symbol, um vorhanden Einträge zu bearbeiten. Wählen Sie die

Schaltfläche **Neu**, um neue Profile hinzuzufügen.

(1) Gehen Sie zu **VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**.



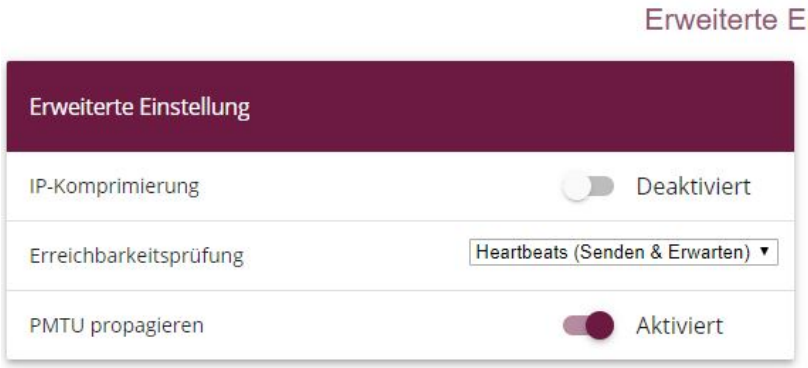


Abb. 135: **VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie eine **Beschreibung** ein, die das Profil eindeutig identifiziert.

(2) Wählen Sie bei **Proposals Verschlüsselung** `Blowfish` , bei **Authentifizierung** `MD5` . Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.

(3) Aktivieren Sie die Option **PFS-Gruppe verwenden** und wählen Sie `2 (1024 Bit)` aus.

(4) Legen Sie die **Lebensdauer** für Phase-2-Schlüssel fest. Geben Sie für die Lebensdauer `900` Sekunden ein. Geben Sie für die Lebensdauer als Menge der verarbeitenden Daten `0` KByts an.

(5) Klicken Sie auf **Erweiterte Einstellungen**.

(6) Wählen Sie bei **Erreichbarkeitsprüfung** `Heartbeats (Senden & Erwarten)` aus.

(7) Aktivieren Sie **PMTU propagieren**.

(8) Bestätigen Sie mit **OK**.

7.3 Kontrolle

Mit dem **Ping-Test** können Sie die Funktionalität der VPN IPSec-Verbindung überprüfen. Mit der Eingabe der internen IP-Adresse des Remote Gateways (hier 192.168.200.1) und durch Drücken der **Los**-Schaltfläche wird der Ping-Test gestartet. Dadurch wird der Aufbau des VPN IPSec-Tunnels initiiert. Wenn das Ausgabefeld eine Antwort in Millisekunden anzeigt, ist der Ping-Test erfolgreich.

(1) Gehen Sie zu **Wartung** -> **Diagnose** -> **Ping-Test**.

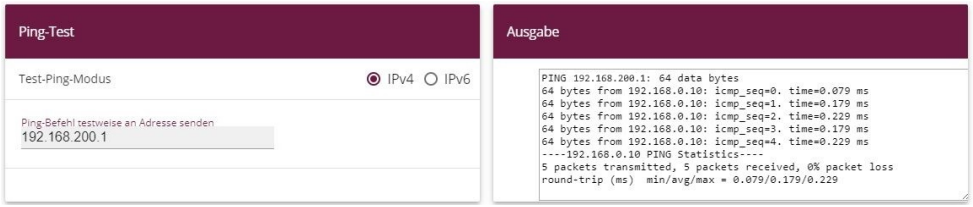


Abb. 136: **Wartung -> Diagnose -> Ping-Test**

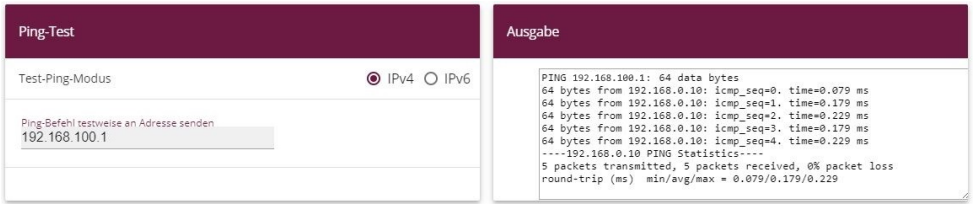


Abb. 137: **Wartung -> Diagnose -> Ping-Test**

7.4 Konfigurationsschritte im Überblick

DynDNS Account am ersten Router einrichten (Standort A)

Feld	Menü	Wert
Hostname	**Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu**	z. B. *test1.dyndns.org*
Schnittstelle	**Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu**	*DSL ISP*
Benutzername	**Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu**	z. B. *test*
Passwort	**Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu**	z. B. *test*
Provider	**Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu**	*dyndns*
Aktualisierung aktivieren	**Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu**	Deaktiviert

IPSec-Konfiguration - IPSec-Peers

Feld	Menü	Wert
Administrativer Status	**VPN -> IPSec -> IPSec-Peers -> Neu**	Aktiv

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *be.IP_test2*
Peer-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *test2.dyndns.org*
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*Fully Qualified Domain Name (FQDN)* / *be.IP_test2*
Preshared Key	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *test*
IP-Adressenvergabe	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	Statisch
Standardroute	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	Deaktiviert
Lokale IP-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*192.168.100.1*
Routeneinträge	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*192.168.200.0* / *255.255.255.0*

IPSec-Konfiguration - Phase-1

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	z. B. **autogeneriert**
Proposals	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*Blowfish, MD5*
DH-Grupe	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*2 (1024 Bit)*
Lebensdauer	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*900* Sekunden, *0* kBytes
Authentifizierungsmethode	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*Preshared Keys*
Modus	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*Aggresiv*
Lokaler ID-Typ	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*Fully Qualified Domain Name (FQDN)*
Lokaler ID-Wert	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*be.IP_test1*
Erreichbarkeitsprüfung	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu** -> **Erweiterte Einstellungen**	*Dead Peer Detection (Idle)*
Blockzeit	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu** -> **Erweiterte Einstellungen**	*10* Sekunden
NAT-Traversal	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu** -> **Erweiterte Einstellungen**	Aktiviert

IPSec-Konfiguration - Phase-2

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**	z. B. **autogeneriert**
Proposals	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**	*Blowfish, MD5*
PFS-Grupe verwenden	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**	*2 (1024 Bit)*
Lebensdauer	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**	*900* Sekunden, *0* kBytes
IP-Komprimierung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu** -> **Erweiterte Einstellungen**	*Deaktiviert*
Erreichbarkeitsprüfung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu** -> **Erweiterte Einstellungen**	*Heartbeats (Senden & Erwarten)*
PMTU propagieren	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu** -> **Erweiterte Einstellungen**	Aktiviert

DynDNS Account am zweiten Router einrichten (Standort B)

Feld	Menü	Wert
Hostname	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *test2.dyndns.org*
Schnittstelle	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	*DSL ISP*
Benutzername	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *test*
Passwort	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *test*
Provider	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	*dyndns*
Aktualisierung aktivieren	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	Aktiviert

IPSec-Konfiguration - IPSec-Peers

Feld	Menü	Wert
Administrativer Status	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	Aktiv
Beschreibung	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *be.IP_test1*
Peer-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *test1.dyndns.org*
Peer-ID	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*Fully Qualified Domain Name (FQDN)*

Feld	Menü	Wert
		/ *be.IP_test1*
Preshared Key	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	z. B. *test*
IP-Adressenvergabe	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	Statisch
Standardroute	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	Deaktiviert
Lokale IP-Adresse	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*192.168.200.1*
Routeneinträge	**VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**	*192.168.100.0* / *255.255.255.0*

IPSec-Konfiguration - Phase-1

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	z. B. **autogeneriert**
Proposals	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*Blowfish, MD5*
DH-Grupe	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*2 (1024 Bit)*
Lebensdauer	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*900* Sekunden, *0* kBytes
Authentifizierungsmethode	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*Preshared Keys*
Modus	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*Aggresiv*
Lokaler ID-Typ	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*Fully Qualified Domain Name (FQDN)*
Lokaler ID-Wert	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu**	*be.IP_test2*
Erreichbarkeitsprüfung	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu** -> **Erweiterte Einstellungen**	*Dead Peer Detection (Idle)*
Blockzeit	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu** -> **Erweiterte Einstellungen**	*10* Sekunden
NAT-Traversal	**VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu** -> **Erweiterte Einstellungen**	Aktiviert

IPSec-Konfiguration - Phase-2

Feld	Menü	Wert
Beschreibung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**	z. B. **autogeneriert**
Proposals	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**	*Blowfish, MD5*
PFS-Grupe verwenden	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**	*2 (1024 Bit)*
Lebensdauer	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu**	*900* Sekunden, *0* kBy-

Feld	Menü	Wert
		tes
IP-Komprimierung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu** -> **Erweiterte Einstellungen**	*Deaktiviert*
Erreichbarkeitsprüfung	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu** -> **Erweiterte Einstellungen**	*Heartbeats (Senden & Erwarten)*
PMTU propagieren	**VPN** -> **IPSec** -> **Phase-2-Profile** -> **Neu** -> **Erweiterte Einstellungen**	Aktiviert

Kapitel 8 Sicherheit - Bridging über eine IPSec-Verbindung

8.1 Einleitung

Die vorliegende Lösung zeigt eine Möglichkeit zur Verbindung zweier Standorte über IPSec deren IP-Netzbereiche überlappen oder identisch sind (z. B. Standort A: 192.168.1.0/24 und Standort B: 192.168.1.0/24).

In diesem Fall funktioniert IPSec nicht, da IPSec als Layer3 (IP-Layer) Protokoll zur Funktion unterschiedliche IP-Netze zwischen den zu vernetzenden Standorten erfordert. Wie in einem solchen Fall trotzdem die Sicherheit von IPSec für die Standortvernetzung genutzt werden kann zeigt dieser Workshop.

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

Zur Lösung dieses Problems bietet sich L2TP (Layer2 Tunneling Protokoll) als Transportprotokoll an. L2TP bietet die Möglichkeit Bridge Verbindungen über geroutete IP-Verbindungen aufzubauen. In unserem Fall bedeutet dies, dass die Standorte über IPSec verbunden werden und der eigentliche Nutztraffic in L2TP getunnelt über die IPSec-Verbindung übertragen wird.

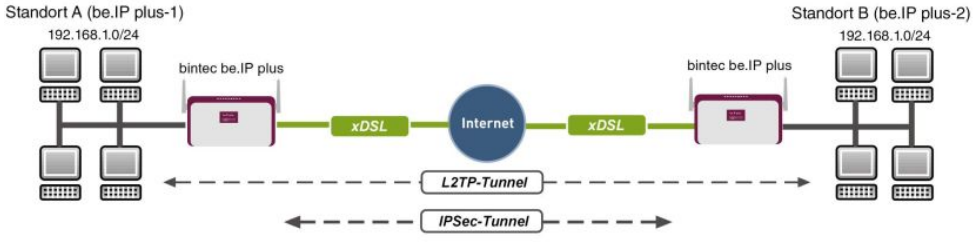


Abb. 138: Beispielszenario

Die Nutzdaten werden über den L2TP-Tunnel und die L2TP-Pakete wiederum über den IPSec-Tunnel übertragen.

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

(1) Zwei bintec ADSL-Gateways z. B. **bintec be.IP plus**

(2) Ein Bootimage der Version 7.9.1.

(3) Beide Gateways benötigen eine unabhängige Verbindung zum Internet.

Hinweise zum Test Setup

bintec be.IP plus Standort A

System-Name	be.IP_plus-1
LAN IP-Adresse	192.168.1.253
LAN IP-Subnetzmaske	255.255.255.0
Öffentliche Internet IP-Adresse	10.1.1.1 (hier kann auch ein Hostname verwendet werden)
Lokale IP-Adresse der IPSec-Schnittstelle	1.1.1.1 (eine beliebige private IP-Adresse)
Lokale IP-Adresse der L2TP-Schnittstelle	1.1.1.3

bintec be.IP plus Standort B

System-Name	be.IP_plus-2
LAN IP-Adresse	192.168.1.254
LAN IP-Subnetzmaske	255.255.255.0
Öffentliche Internet IP-Adresse	10.1.1.4 (hier kann auch ein Hostname verwendet werden)
Lokale IP-Adresse der IPSec-Schnittstelle	1.1.1.2 (eine beliebige private IP-Adresse)
Lokale IP-Adresse der L2TP-Schnittstelle	1.1.1.4

8.2 Konfiguration am Standort A (bintec be.IP_plus-1)

Konfiguration der IPSec-Verbindung mit dem VPN-Assistenten

Fügen Sie im VPN-Assistenten eine neue Verbindung hinzu. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**.

Abb. 139: **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **VPN-Szenario** *IPSec-LAN-zu-LAN-Verbindung* aus.

(2) Klicken Sie auf **Weiter**, um eine neue VPN-Verbindung zu konfigurieren.

Geben Sie die erforderlichen Daten für die VPN-Verbindung ein.

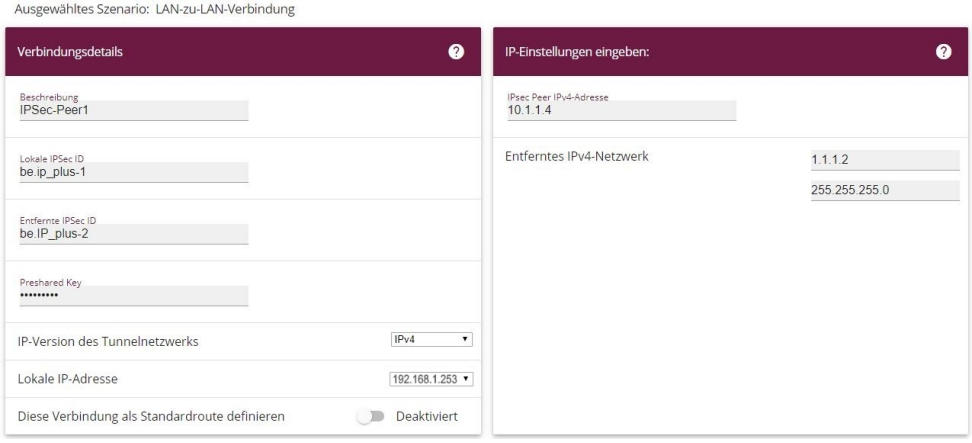


Abb. 140: **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Weiter**

Gehen Sie folgendermaßen vor, um eine neue VPN-Verbindung zu konfigurieren:

(1) Bei **Beschreibung** tragen Sie z. B. *IPSec-Peer1* ein.

(2) Unter **Lokale IPSec ID** tragen Sie die ID Ihres eigenen IPSec-Gateways ein, z. B. *be.IP_plus-1*.

(3) Unter **Entfernte IPSec ID** tragen Sie z. B. *be.IP_plus-2* ein.

(4) Für die Authentifizierung geben Sie **Preshared Key** ein, z. B. *geheim*. Der Preshared Key muss auf beiden Seiten identisch sein.

(5) Wählen Sie die **Lokale IP-Adresse** des Gateways aus, z. B. *192.168.1.253*.

(6) **Diese Verbindung als Standardroute definieren** belassen Sie auf deaktiviert.

(7) Bei **IPSec-Peer-Adresse** geben Sie die IP-Adresse oder den Hostnamen des entfernten IPSec-Partners ein, z. B. `10.1.1.4`.

(8) Bei **IP-Adresse des Remote-Netzwerks** geben Sie die Zieladresse für die Verbindung ein, z. B. `1.1.1.2`.

(9) Geben Sie bei **Netzmaske** die Hostmaske ein, z. B. `255.255.255.255`.

(10) Bestätigen Sie Ihre Angaben mit **OK**.

Zum Ändern der Lokalen IP-Adresse gehen Sie in folgendes Menü:

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

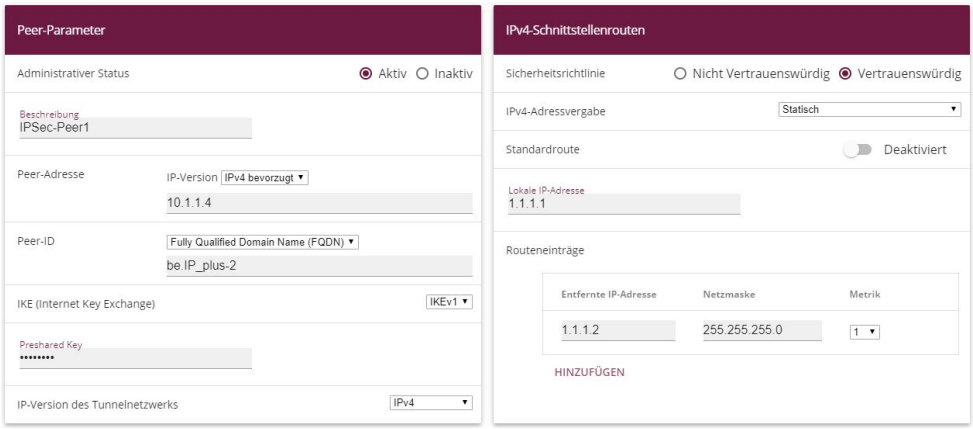


Abb. 141: **VPN** -> **IPSec** -> **IPSec-Peers** -> ✎

Gehen Sie folgendermaßen vor:

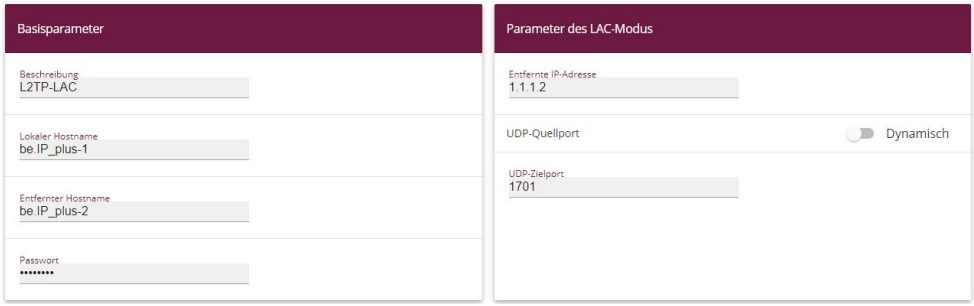
(1) Unter **Lokale IP-Adresse** tragen Sie z. B. `1.1.1.1` ein.

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

Konfiguration der L2TP-Verbindung

Um ein Tunnelprofil anzulegen, gehen Sie in folgendes Menü:

(1) Gehen Sie zu **VPN** -> **L2TP** -> **Tunnelprofile** -> **Neu**.



(1) Bei **Beschreibung** tragen Sie z. B. *L2TP-LAC* ein.

(2) Unter **Lokaler Hostname** tragen Sie die ID Ihres eigenen IPSec-Gateways ein, z. B. *be.IP_plus-1*.

(3) Unter **Entfernter Hostname** tragen Sie z. B. *be.IP_plus-2* ein.

(4) Für die Authentifizierung geben Sie das **Passwort** ein, z. B. *geheim*.

(5) Bei **Entfernte IP-Adresse** geben Sie die Zieladresse die für die Verbindung genutzt wird ein, z. B. *1.1.1.2*.

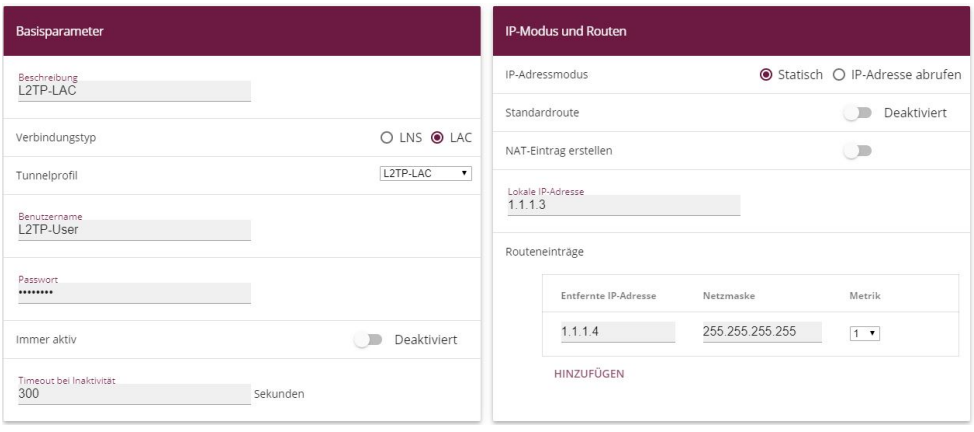
(6) Klicken Sie auf **Erweiterte Einstellungen**.

(7) Tragen Sie die **Lokale IP-Adresse** ein, z. B. *1.1.1.1*.

(8) Belassen SIe die restlichen Einstellungen und bestätigen Sie mit **OK**.

Im nächsten Schritt muss ein Benutzer konfiguriert werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **VPN** -> **L2TP** -> **Benutzer** -> **Neu**.



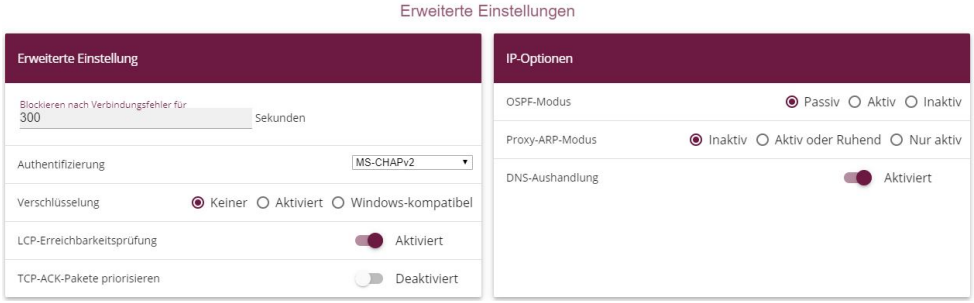


Abb. 145: **VPN** -> **L2TP** -> **Benutzer** -> **Neu**

Gehen Sie folgendermaßen vor, um einen neuen Benutzer anzulegen.

(1) Bei **Beschreibung** geben Sie z. B. `L2TP-LAC` ein.

(2) Wählen Sie den **Verbindungstyp** `LAC` aus.

(3) Bei **Tunnelprofil** wählen Sie `L2TP-LAC` aus.

(4) Geben Sie bei **Benutzername** z. B. `L2TP-User` ein.

(5) Tragen Sie das **Passwort** ein, z. B. `geheim`.

(6) Geben Sie die **Lokale IP-Adresse** ein, z. B. `1.1.1.3`. Um Konflikte mit anderen Schnittstellen oder existierenden Routen zu vermeiden muss die Lokale IP-Adresse eindeutig sein.

(7) Bei **Routeneinträge** geben Sie die Entfernte IP-Adresse z. B. `1.1.1.4` und die Netzmaske z. B. `255.255.255.255` ein.

(8) Klicken Sie auf **Erweiterte Einstellungen**.

(9) Bei **Verschlüsselung** klicken Sie auf `Keine`. Da eine sichere IPSec-Verbindung bereits besteht, ist eine zusätzliche Verschlüsselung nicht notwendig.

(10) Belassen SIe die restlichen Einstellungen und bestätigen Sie mit **OK**.

Konfiguration der Bridge-Gruppe

Zur Aktivierung des Bridging zwischen der LAN-Schnittstelle und der L2TP-Schnittstelle müssen die beiden Schnittstellen einer Bridge-Gruppe zugewiesen werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**.

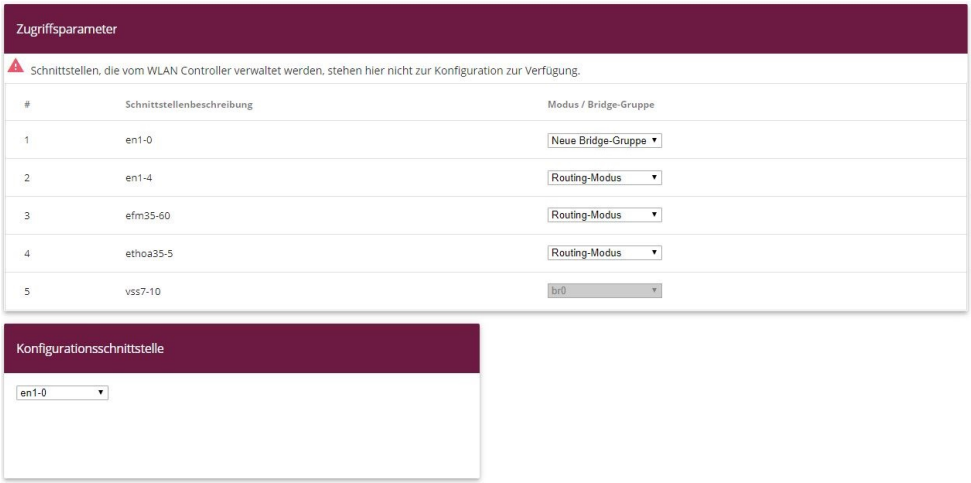


Abb. 146: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Modus / Bridge-Gruppe** *Neue Bridge-Gruppe* aus. In unserem Beispiel wird als LAN-Schnittstelle die Schnittstelle *en1-0* verwendet.

(2) Bei **Konfigurationsschnittstelle** wählen Sie die *en1-0* aus.

(3) Bestätigen Sie mit **OK**. Nach Klicken des **OK**-Buttons wird automatisch eine neue Bridge-Gruppe erzeugt.

Wenn noch keine Bridge-Gruppe existiert wird die neu erzeugte Schnittstelle den Alias *br0* verwenden (ansonsten *br1*, *br2* usw.).

Die Konfiguration sieht wie folgt aus:

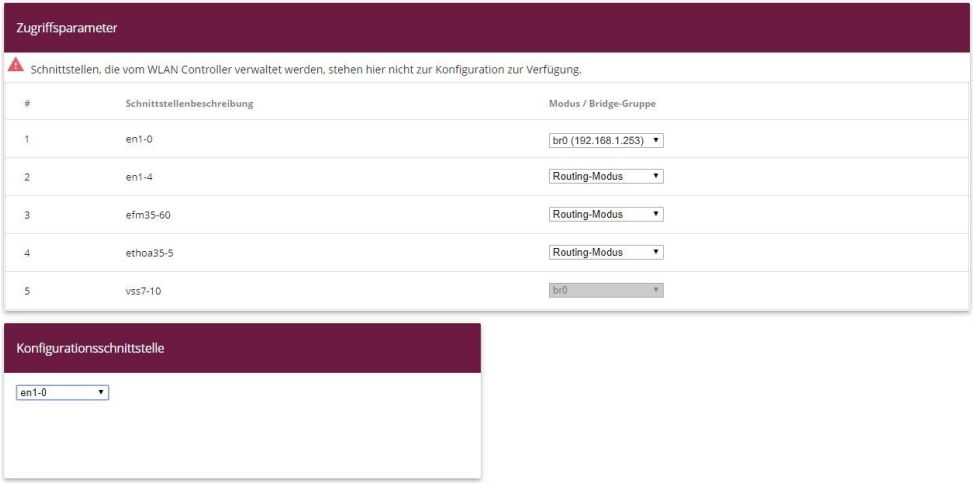


Abb. 147: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**

Nun wird zu der eben erzeugten Bridge-Grupppe die L2TP-Schnittstelle zugewiesen. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen** -> **Hinzufügen**.

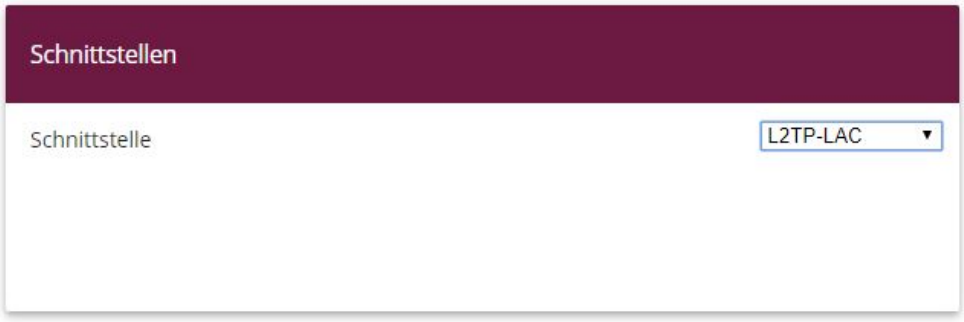


Abb. 148: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen** -> **Hinzufügen**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Schnittstelle** den WAN-Partner Eintrag aus, hier *L2TP-LAC*.

(2) Bestätigen Sie mit **OK**.

Zur Aktivierung des Bridging zwischen der LAN-Schnittstelle und der L2TP-Schnittstelle müssen die beiden Schnittstellen einer Bridge-Gruppe zugewiesen werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**.

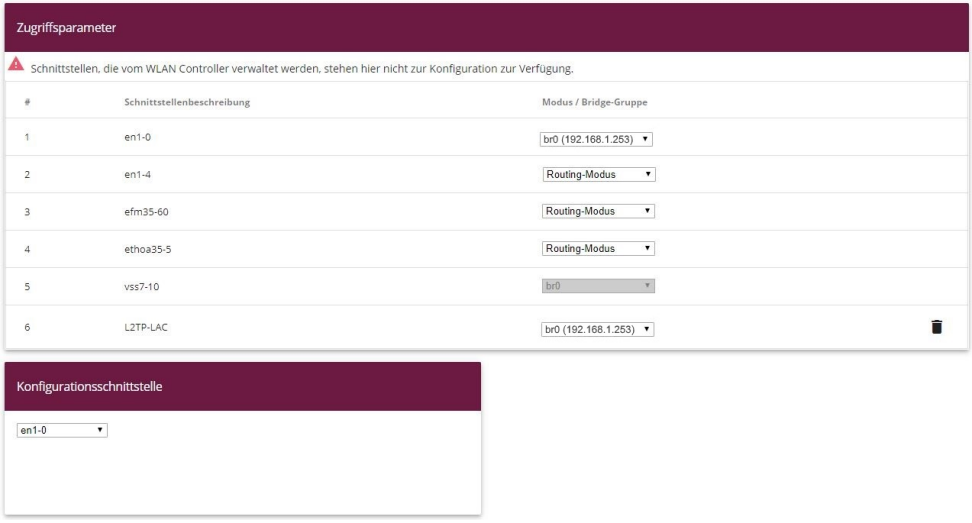


Abb. 149: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Modus / Bridge-Gruppe** `br0(192.168.1.253)` aus.

(2) Bestätigen Sie mit **OK**. Nach Klicken des **OK**-Buttons wird automatisch eine neue Bridge-Gruppe erzeugt.

Hiermit ist die Konfiguration des **bintec be.IP plus** Gateways am Standort A abgeschlossen.

8.3 Konfiguration am Standort B (bintec be.IP_plus-2)

Konfiguration der IPSec-Verbindung mit dem VPN-Assistenten

Fügen Sie im VPN-Assistenten eine neue Verbindung hinzu. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**.

Abb. 150: **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **VPN-Szenario** *IPSec-LAN-zu-LAN-Verbindung* aus.

(2) Klicken Sie auf **Weiter**, um eine neue VPN-Verbindung zu konfigurieren.

Geben Sie die erforderlichen Daten für die VPN-Verbindung ein.

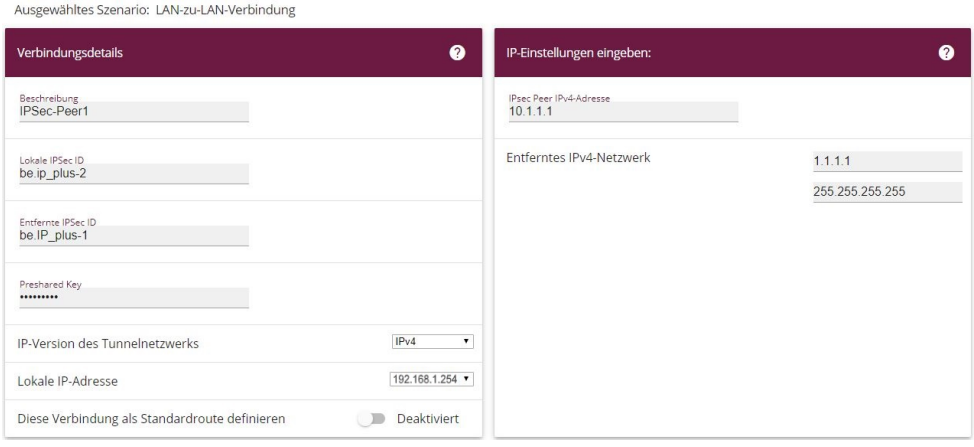


Abb. 151: **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Weiter**

Gehen Sie folgendermaßen vor, um eine neue VPN-Verbindung zu konfigurieren:

(1) Bei **Beschreibung** tragen Sie z. B. *IPSec-Peer1* ein.

(2) Unter **Lokale IPSec ID** tragen Sie die ID Ihres eigenen IPSec-Gateways ein, z. B. *be.IP_plus-2*.

(3) Unter **Entfernte IPSec ID** tragen Sie z. B. *be.IP_plus-1* ein.

(4) Für die Authentifizierung geben Sie **Preshared Key** ein, z. B. *geheim*. Der Preshared Key muss auf beiden Seiten identisch sein.

(5) Wählen Sie die **Lokale IP-Adresse** des Gateways aus, z. B. *192.168.1.254*.

(6) **Diese Verbindung als Standardroute definieren** belassen Sie auf deaktiviert.

(7) Bei **IPSec-Peer-Adresse** geben Sie die IP-Adresse oder den Hostnamen des entfernten IPSec-Partners ein, z. B. `10.1.1.1`.

(8) Bei **IP-Adresse des Remote-Netzwerks** geben Sie die Zieladresse für die Verbindung ein, z. B. `1.1.1.1`.

(9) Geben Sie bei **Netzmaske** die Hostmaske ein, z. B. `255.255.255.255`.

(10) Bestätigen Sie Ihre Angaben mit **OK**.

Zum Ändern der Lokalen IP-Adresse gehen Sie in folgendes Menü:

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

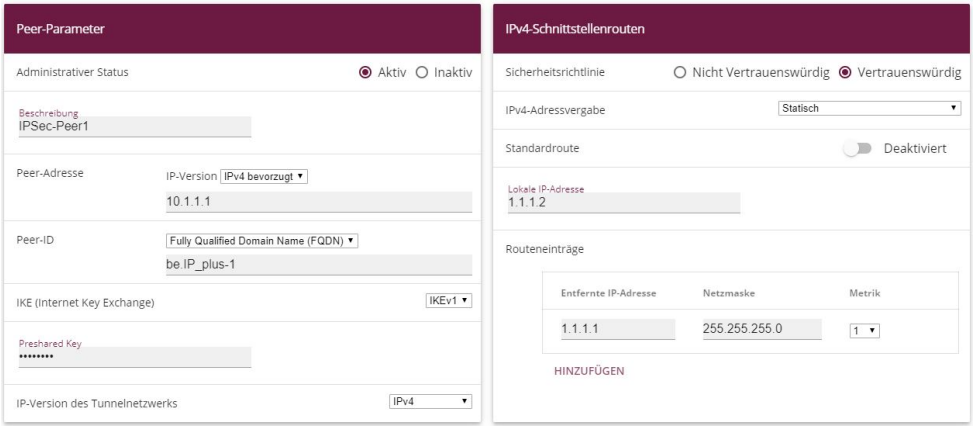


Abb. 152: **VPN** -> **IPSec** -> **IPSec-Peers** -> ✎

Gehen Sie folgendermaßen vor:

(1) Unter **Lokale IP-Adresse** tragen Sie z. B. `1.1.1.2` ein.

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

Konfiguration der L2TP-Verbindung

Um ein Tunnelprofil anzulegen, gehen Sie in folgendes Menü:

(1) Gehen Sie zu **VPN** -> **L2TP** -> **Tunnelprofile** -> **Neu**.

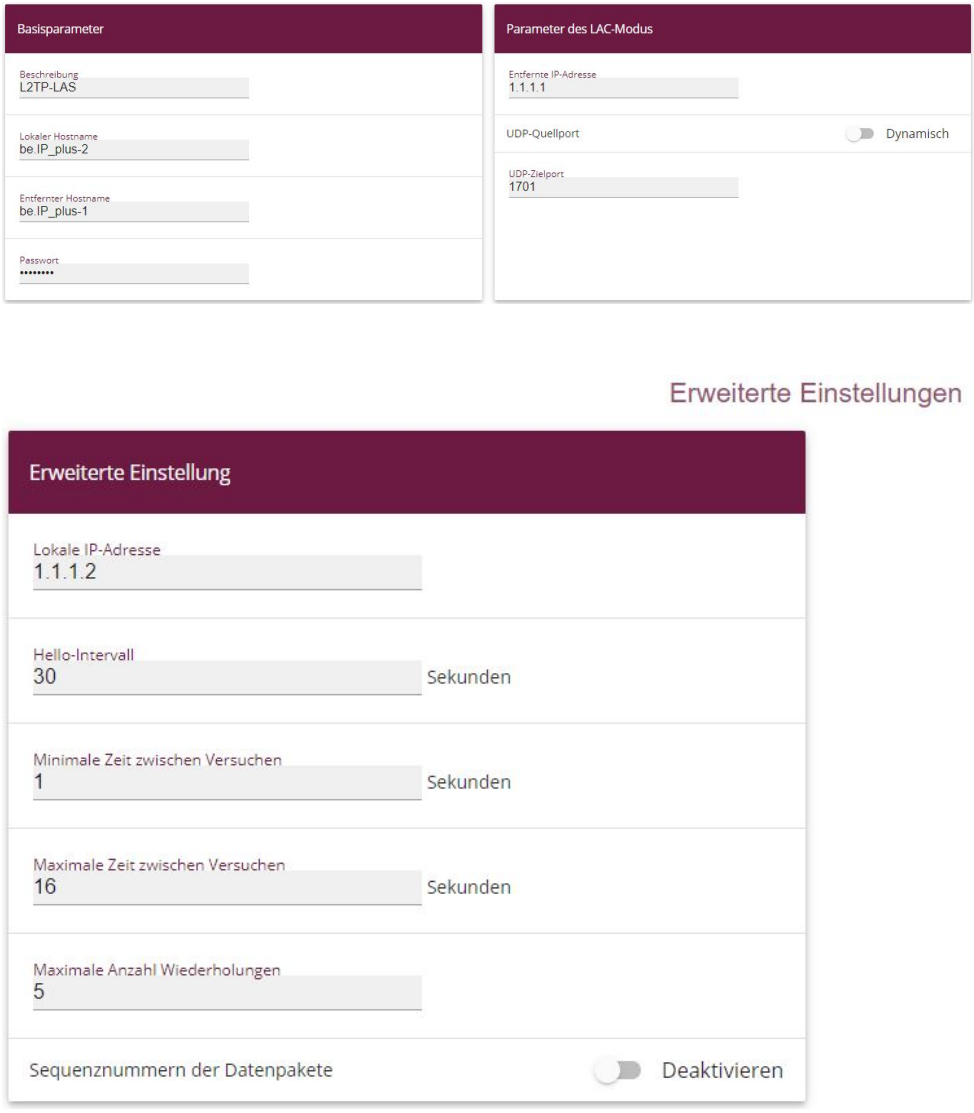


Abb. 154: **VPN** -> **L2TP** -> **Tunnelprofile** -> **Neu**

(1) Bei **Beschreibung** tragen Sie z. B. *L2TP-LAS* ein.

(2) Unter **Lokaler Hostname** tragen Sie die ID Ihres eigenen IPSec-Gateways ein, z. B. *be.IP_plus-2*.

(3) Unter **Entfernter Hostname** tragen Sie z. B. *be.IP_plus-1* ein.

(4) Für die Authentifizierung geben Sie das **Passwort** ein, z. B. *geheim*.

(5) Bei **Entfernte IP-Adresse** geben Sie die Zieladresse die für die Verbindung genutzt wird ein, z. B. *1.1.1.1*.

(6) Klicken Sie auf **Erweiterte Einstellungen**.

(7) Tragen Sie die **Lokale IP-Adresse** ein, z. B. *1.1.1.2*.

(8) Belassen SIe die restlichen Einstellungen und bestätigen Sie mit **OK**.

Im nächsten Schritt muss ein Benutzer konfiguriert werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **VPN** -> **L2TP** -> **Benutzer** -> **Neu**.

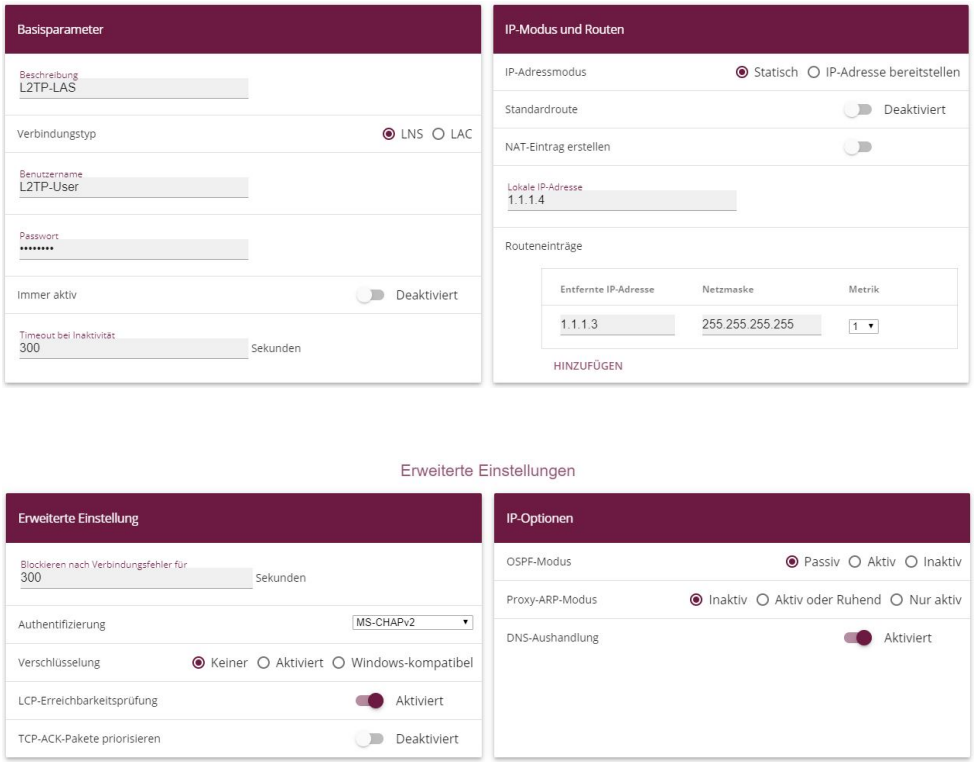


Abb. 156: **VPN** -> **L2TP** -> **Benutzer** -> **Neu**

Gehen Sie folgendermaßen vor, um einen neuen Benutzer anzulegen.

(1) Bei **Beschreibung** geben Sie z. B. *L2TP-LAS* ein.

(2) Wählen Sie den **Verbindungstyp** *LNS* aus.

(3) Geben Sie bei **Benutzername** z. B. *L2TP-User* ein.

(4) Tragen Sie das **Passwort** ein, z. B. *geheim*.

(5) Geben Sie die **Lokale IP-Adresse** ein, z. B. *1.1.1.4*. Um Konflikte mit anderen Schnittstellen oder existierenden Routen zu vermeiden muss die Lokale IP-Adresse eindeutig sein.

(6) Bei **Routeneinträge** geben Sie die Entfernte IP-Adresse z. B. `1.1.1.3` und die Netzmaske z. B. `255.255.255.255` ein.

(7) Klicken Sie auf **Erweiterte Einstellungen**.

(8) Bei **Verschlüsselung** klicken Sie auf `Keine`. Da eine sichere IPSec-Verbindung bereits besteht, ist eine zusätzliche Verschlüsselung nicht notwendig.

(9) Belassen SIe die restlichen Einstellungen und bestätigen Sie mit **OK**.

Konfiguration der Bridge-Gruppe

Zur Aktivierung des Bridging zwischen der LAN-Schnittstelle und der L2TP-Schnittstelle müssen die beiden Schnittstellen einer Bridge-Gruppe zugewiesen werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**.

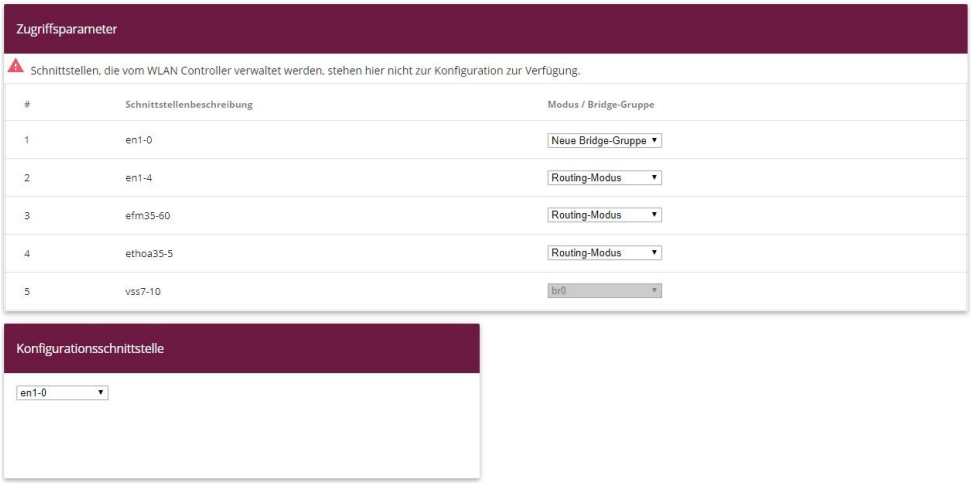


Abb. 157: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Modus / Bridge-Gruppe** `Neue Bridge-Gruppe` aus. In unserem Beispiel wird als LAN-Schnittstelle die Schnittstelle `en1-0` verwendet.

(2) Bei **Konfigurationsschnittstelle** wählen Sie die `en1-0` aus.

(3) Bestätigen Sie mit **OK**. Nach Klicken des **OK**-Buttons wird automatisch eine neue Bridge-Gruppe erzeugt.

Wenn noch keine Bridge-Gruppe existiert wird die neu erzeugte Schnittstelle den Alias `br0` verwenden (ansonsten `br1`, `br2` usw.).

Die fertige Konfiguration sieht wie folgt aus:

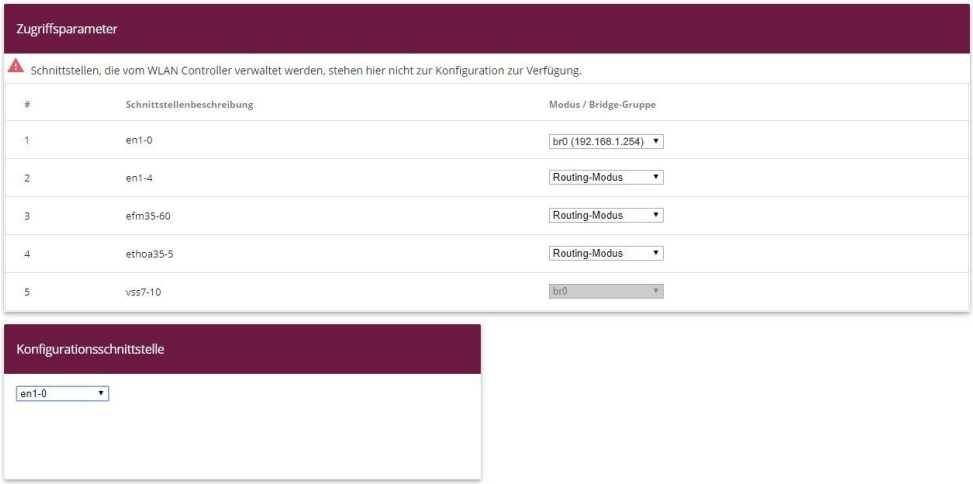


Abb. 158: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**

Nun wird zu der eben erzeugten Bridge-Grupppe die L2TP-Schnittstelle zugewiesen. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen** -> **Hinzufügen**.

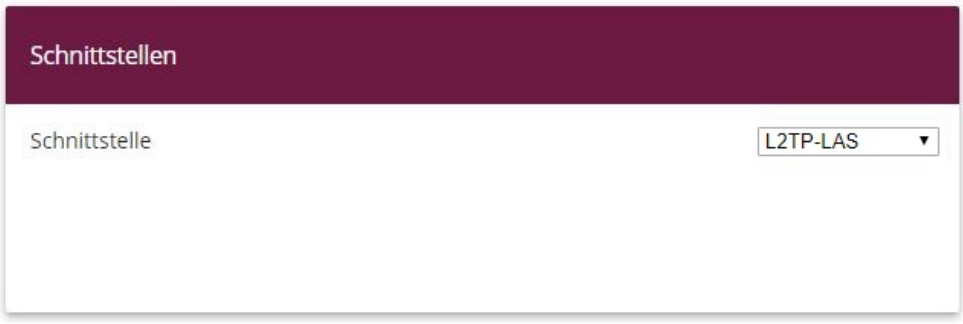


Abb. 159: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen** -> **Hinzufügen**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Schnittstelle** den WAN-Partner Eintrag aus, hier *L2TP-LAS*.

(2) Bestätigen Sie mit **OK**.

Zur Aktivierung des Bridging zwischen der LAN-Schnittstelle und der L2TP-Schnittstelle

müssen die beiden Schnittstellen einer Bridge-Gruppe zugewiesen werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**.

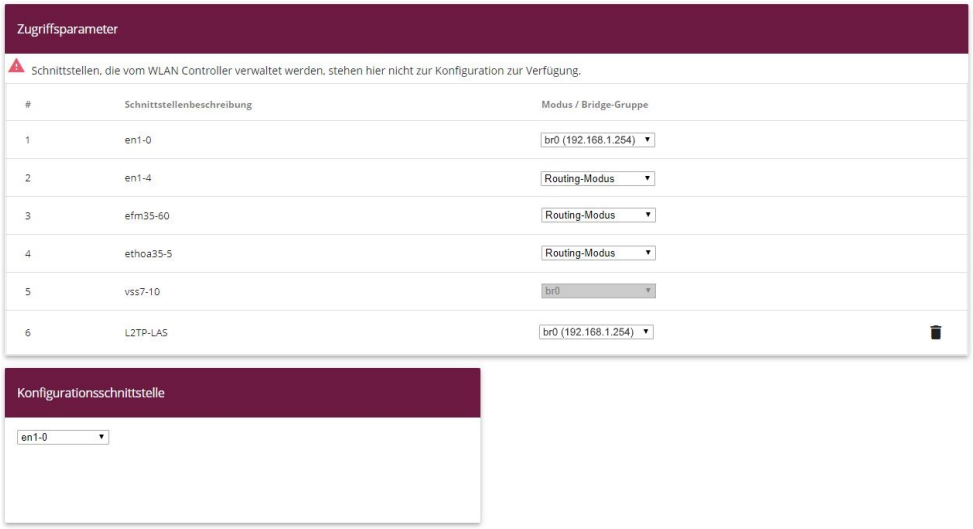


Abb. 160: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Modus / Bridge-Gruppe** *br0(192.168.1.254)* aus.

(2) Bestätigen Sie mit **OK**. Nach Klicken des **OK**-Buttons wird automatisch eine neue Bridge-Gruppe erzeugt.

Hiermit ist die Konfiguration des **bintec be.IP plus** Gateways am Standort B abgeschlossen.

8.4 Konfigurationsschritte im Überblick

Konfiguration Standort A

Feld	Menü	Wert
VPN-Szenario	**Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**	*IPSec-LAN-zu-LAN-Verbindung*

VPN-Assistenten konfiguration

Feld	Menü	Wert
Beschreibung	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *IPSec-Peer1*
Lokale IPSec ID	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *be.IP_plus-1*
Entfernte IPSec ID	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *be.IP_plus-2*
Preshared Key	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *geheim*
Lokale IP-Adresse	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *192.168.1.253*
IPSec-Peer-Adresse	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *10.1.1.4*
IP-Adresse des Remote-Netzwerks	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *1.1.1.2*
Netzmaske	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *255.255.255.255*

Ändern der lokalen IP-Adresse

Feld	Menü	Wert
Lokale IP-Adresse	**VPN -> IPSec -> IPSec-Peers ->** 	z. B. *1.1.1.1*

Tunnelprofile konfigurieren

Feld	Menü	Wert
Beschreibung	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *L2TP-LAC*
Lokaler Hostname	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *be.IP_plus-1*
Entfernter Hostname	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *be.IP_plus-2*
Passwort	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *geheim*
Entfernte IP-Adresse	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *1.1.1.2*
Lokale IP-Adresse	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *1.1.1.1*

Neuen Benutzer konfigurieren

Feld	Menü	Wert
Beschreibung	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *L2TP-LAC*
Verbindungstyp	**VPN -> L2TP -> Benutzer -> Neu**	*LAC*
Tunnelprofil	**VPN -> L2TP -> Benutzer -> Neu**	*L2TP-LAC*
Benutzername	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *L2TP-User*
Passwort	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *geheim*
Lokale IP-Adresse	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *1.1.1.3*
Entfernte IP-Adresse	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *1.1.1.4*
Netzmaske	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *255.255.255.255*
Verschlüsselung	**VPN -> L2TP -> Benutzer -> Neu**	*Keine*

Bridge-Gruppe konfigurieren

Feld	Menü	Wert
Modus / Bridge-Gruppe	**Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen**	*Neue Bridge-Gruppe*
Konfigurationsschnittstelle	**Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen**	*en1-0*

L2TP-Schnittstelle zuweisen

Feld	Menü	Wert
Schnittstelle	**Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen -> Hinzufügen**	*L2TP-LAC*
Modus / Bridge-Gruppe	**Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen**	*br0(192.168.1.253)*

Konfiguration Standort B

Feld	Menü	Wert
VPN-Szenario	**Assistenten -> VPN -> VPN-Verbindungen -> Neu**	*IPSec-LAN-zu-LAN-Verbindung*

VPN-Assistenten konfiguration

Feld	Menü	Wert
Beschreibung	**Assistenten -> VPN -> VPN-**	z. B. *IPSec-Peer1*

Feld	Menü	Wert
	Verbindungen -> Weiter	
Lokale IPSec ID	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *be.IP_plus-2*
Entfernte IPSec ID	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *be.IP_plus-1*
Preshared Key	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *geheim*
Lokale IP-Adresse	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *192.168.1.254*
IPSec-Peer-Adresse	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *10.1.1.1*
IP-Adresse des Remote-Netzwerks	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *1.1.1.1*
Netzmaske	**Assistenten -> VPN -> VPN-Verbindungen -> Weiter**	z. B. *255.255.255.255*

Ändern der lokalen IP-Adresse

Feld	Menü	Wert
Lokale IP-Adresse	**VPN -> IPSec -> IPSec-Peers ->** 	z. B. *1.1.1.2*

Tunnelprofile konfigurieren

Feld	Menü	Wert
Beschreibung	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *L2TP-LAS*
Lokaler Hostname	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *be.IP_plus-2*
Entfernter Hostname	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *be.IP_plus-1*
Passwort	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *geheim*
Entfernte IP-Adresse	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *1.1.1.1*
Lokale IP-Adresse	**VPN -> L2TP -> Tunnelprofile -> Neu**	z. B. *1.1.1.2*

Neuen Benutzer konfigurieren

Feld	Menü	Wert
Beschreibung	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *L2TP-LAS*
Verbindungstyp	**VPN -> L2TP -> Benutzer -> Neu**	*LNS*
Benutzername	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *L2TP-User*
Passwort	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *geheim*
Lokale IP-Adresse	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *1.1.1.4*
Entfernte IP-Adresse	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *1.1.1.3*
Netzmaske	**VPN -> L2TP -> Benutzer -> Neu**	z. B. *255.255.255.255*
Verschlüsselung	**VPN -> L2TP -> Benutzer -> Neu**	*Keine*

Bridge-Gruppe konfigurieren

Feld	Menü	Wert
Modus / Bridge-Gruppe	**Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen**	*Neue Bridge-Gruppe*
Konfigurationsschnittstelle	**Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen**	*en1-0*

L2TP-Schnittstelle zuweisen

Feld	Menü	Wert
Schnittstelle	**Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen -> Hinzufügen**	*L2TP-LAS*
Modus / Bridge-Gruppe	**Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen**	*br0(192.168.1.254)*

Kapitel 9 Sicherheit - Stateful Inspection Firewall (SIF)

9.1 Einleitung

Im Folgenden wird die Konfiguration der SIF (Stateful Inspection Firewall) mit einer **bintec be.IP** beschrieben.

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

Den Mitarbeitern eines Unternehmens sollen nur bestimmte Dienste im Internet zur Verfügung stehen (HTTP, HTTPS, FTP, DNS). Das Gateway soll dabei als DNS-Proxy arbeiten, das heißt die Clients verwenden das Gateway als DNS-Server. Nur der Systemadministrator und der Geschäftsführer sollen eine HTTP- und eine Telnetverbindung zum Gateway herstellen können. Außerdem soll der Geschäftsführer alle Dienste im Internet nutzen können. Jeglicher anderer Datenverkehr soll geblockt werden.

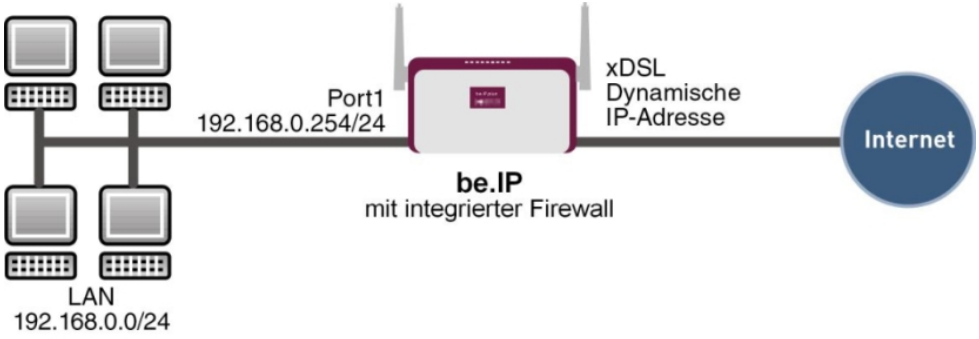


Abb. 161: Beispielszenario SIF

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Eine **bintec be.IP**.
- Ein Bootimage der Version 10.1.1
- Verbindung zum Internet
- Ihr LAN muss mit einem der Ports **1** bis **4** des Gateways verbunden sein

9.2 Konfiguration der Firewall

Wichtig

Bei einer Fehlkonfiguration der Firewall kann die Funktionalität des Gateways bzw. der Verbindungen mitunter stark beeinträchtigt oder sogar unterbrochen werden.

Es gilt der bei Firewalls übliche Grundsatz: Was nicht explizit erlaubt ist, ist verboten.

Daher ist eine genaue Planung der Filterregeln und der Filterregelkette erforderlich um eine korrekte Arbeitsweise sicherzustellen.

9.2.1 Konfiguration der Aliasnamen für IP-Adressen und Netzadresse

Adressalias

Um Benutzer und Netzwerk bei der Konfiguration der Filterregeln identifizieren zu können, müssen Sie Aliasnamen für Ihre Benutzer und Ihr Netzwerk erstellen.

Gehen Sie in folgendes Menü, um Aliasnamen zu erstellen:

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

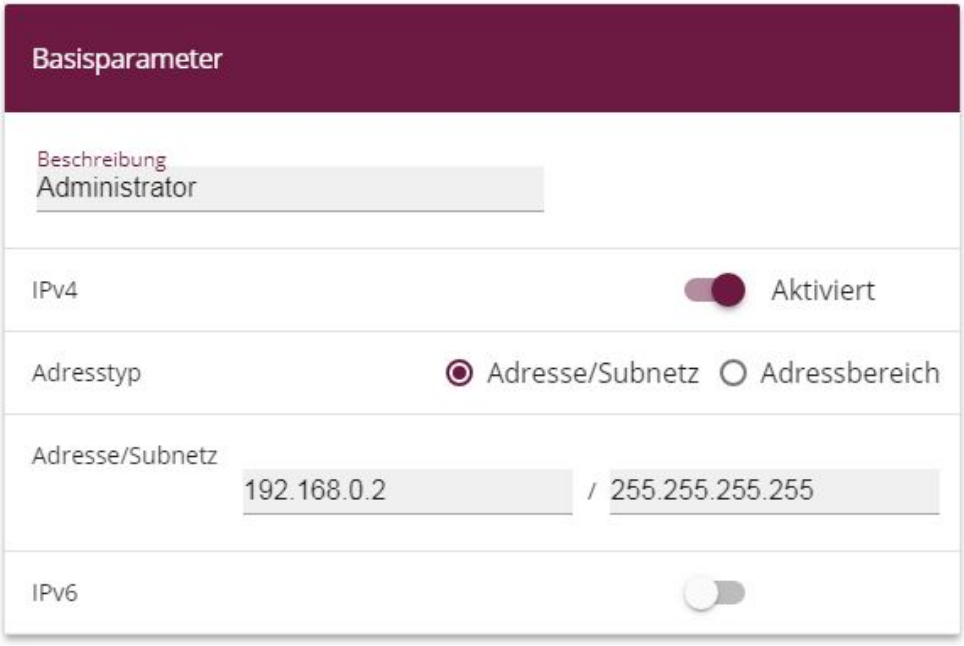


Abb. 162: **Firewall** -> **Adressen** -> **Adressliste** -> **Neu**

Gehen Sie folgendermaßen vor, um einen Aliasnamen für den Administrator zu erstellen:

(1) Tragen Sie bei **Beschreibung** den Namen des Aliases ein, z. B. *Administrator*.

(2) Wählen Sie bei **Adresstyp** *Adresse/Subnetz*.

(3) Tragen Sie bei **Adresse/Subnetz** die IP-Adresse und die zugehörige Subnetzmaske ein, z. B. *192.168.0.2* und *255.255.255.255*.

(4) Bestätigen Sie mit **OK**.

Verfahren Sie analog für die Konfiguration der Aliasnamen für den Geschäftsführer (*Geschäftsführer*), für Ihr Gateway (*be.IP*) und für das Netzwerk (*Netzwerk-Intern*).

Gehen Sie folgendermaßen vor, um einen Aliasnamen für den Geschäftsführer zu erstellen:

(1) Tragen Sie bei **Beschreibung** den Namen des Aliases ein, z. B. *Geschäftsführer*.

(2) Wählen Sie bei **Adresstyp** *Adresse/Subnetz*.

(3) Tragen Sie bei **Adresse/Subnetz** die IP-Adresse und die zugehörige Subnetzmaske ein, z. B. *192.168.0.3* und *255.255.255.255*.

(4) Bestätigen Sie mit **OK**.

Gehen Sie folgendermaßen vor, um einen Aliasnamen für Ihr Gateway zu erstellen:

(1) Tragen Sie bei **Beschreibung** den Namen des Aliases ein, z. B. *be.IP*.

(2) Wählen Sie bei **Adresstyp** *Adresse/Subnetz*.

(3) Tragen Sie bei **Adresse/Subnetz** die IP-Adresse und die zugehörige Subnetzmaske ein, z. B. *192.168.0.254* und *255.255.255.255*.

(4) Bestätigen Sie mit **OK**.

Gehen Sie folgendermaßen vor, um einen Aliasnamen für das interne Netzwerk zu erstellen:

(1) Tragen Sie bei **Beschreibung** den Namen des Aliases ein, z. B. *Netzwerk-Intern*.

(2) Wählen Sie bei **Adresstyp** *Adresse/Subnetz*.

(3) Tragen Sie bei **Adresse/Subnetz** die IP-Adresse und die zugehörige Subnetzmaske ein, z. B. *192.168.0.0* und *255.255.255.0*.

(4) Bestätigen Sie mit **OK**.

Adressgruppen

Um die Konfiguration der Filterregeln zu vereinfachen, können Sie mehrere Aliasnamen zu Gruppen zusammenfassen.

Da sowohl der Administrator als auch der Geschäftsführer per HTTP und Telnet auf das Gateway zugreifen dürfen, werden diese zu einer Gruppe zusammengefasst.

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

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

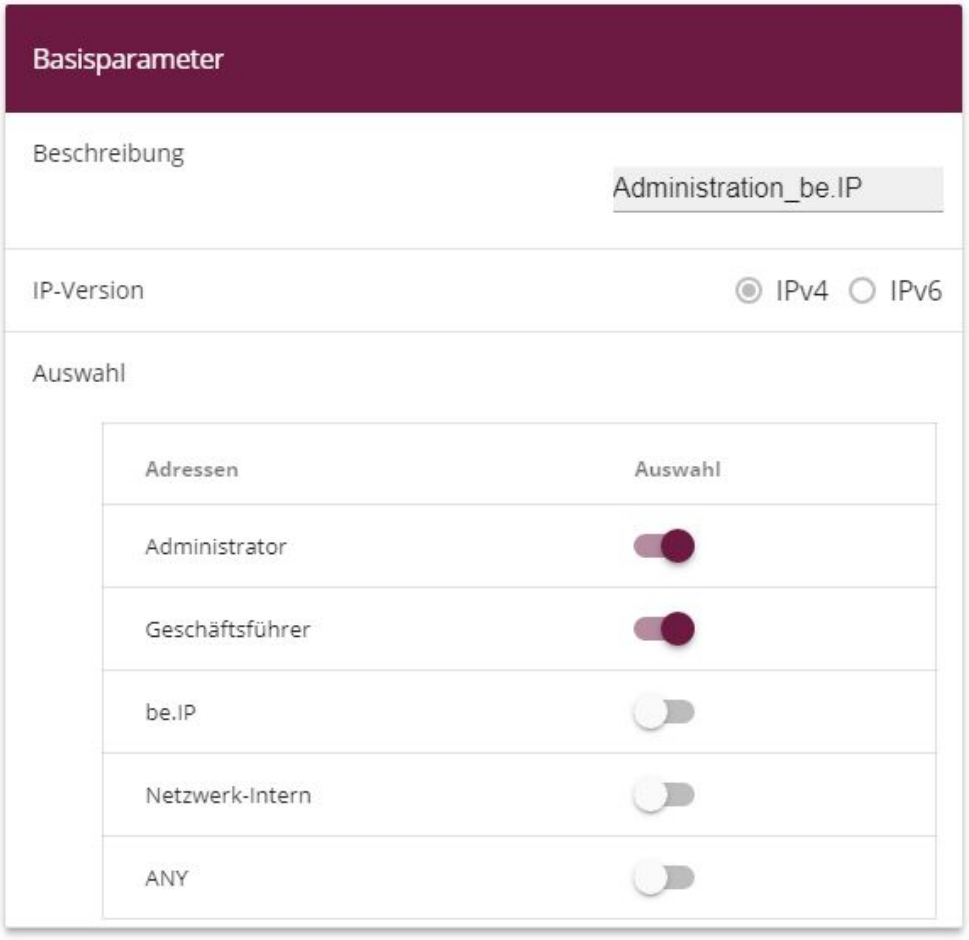


Abb. 163: **Firewall** -> **Adressen** -> **Gruppen** -> **Neu**

Gehen Sie folgendermaßen vor, um eine Gruppe zu erstellen:

(1) Vergeben Sie bei **Beschreibung** einen Namen für die Gruppe, z. B. *Administration_be.IP*.

(2) Aktivieren Sie die Auswahl bei den **Adressen**, die Mitglieder der Gruppe sein sollen, hier *Administrator* und *Geschäftsführer*.

(3) Bestätigen Sie mit **OK**.

9.2.2 Konfiguration von Dienstgruppen

Um bestimmte Dienste bei der Konfiguration der Filterregeln identifizieren zu können, müssen Sie im Menü **Firewall** -> **Dienste** Aliasnamen für die benötigten Dienste erstellen. Es gibt bereits eine große Anzahl sehr häufig benötigter Dienste, die vorkonfiguriert sind. Sollten Sie einen Dienst benötigen, der noch nicht in dieser Liste ist, müssen Sie einen neuen Dienst erstellen.

Um die Konfiguration der Filterregeln zu vereinfachen, können Sie mehrere Dienste zu Gruppen zusammenfassen.

Da die Benutzer im Netzwerk die Dienste HTTP, HTTPS und FTP verwenden dürfen, können Sie diese zu einer Gruppe zusammenfassen.

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

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

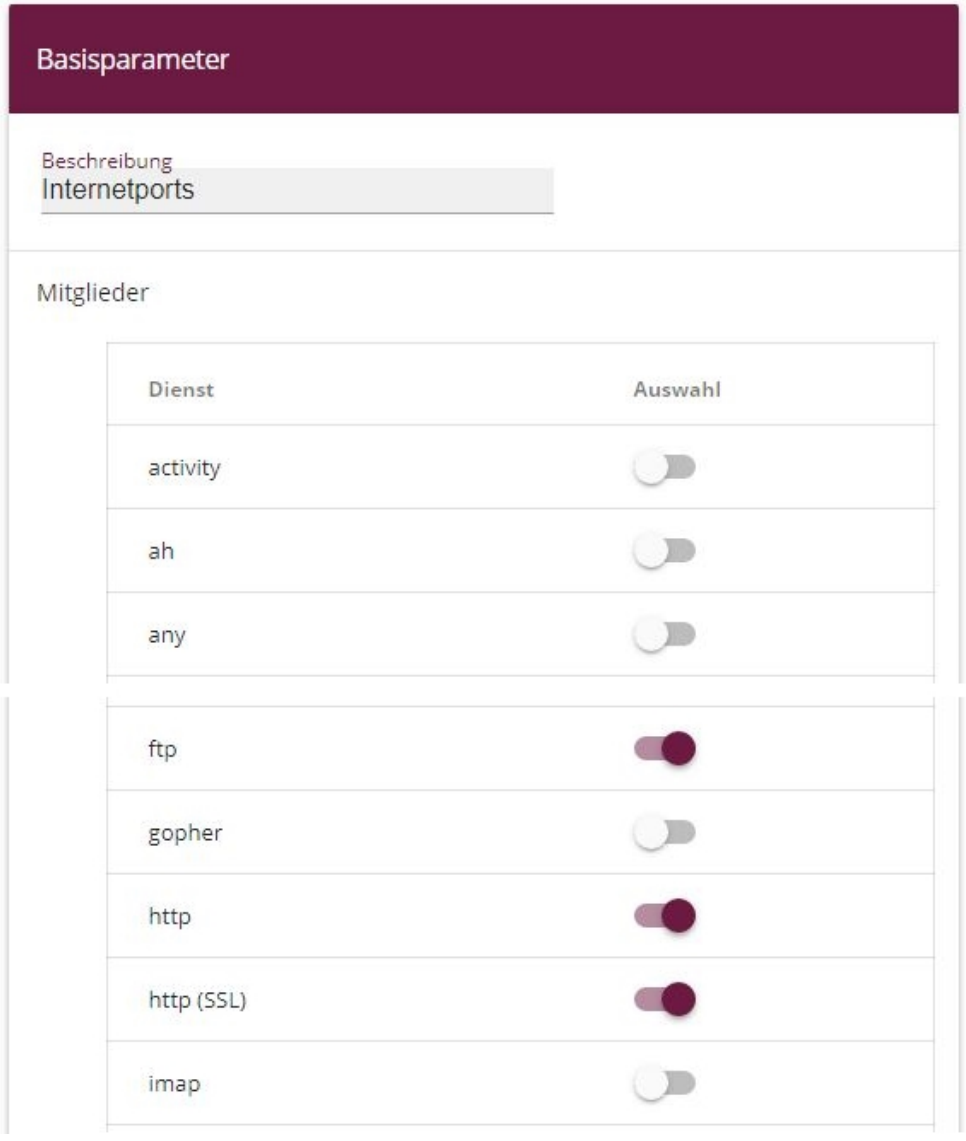


Abb. 164: **Firewall** -> **Dienste** -> **Gruppen** -> **Neu**

Gehen Sie folgendermaßen vor, um eine Gruppe zu erstellen:

(1) Tragen Sie bei **Beschreibung** einen Namen für die Gruppe ein, z. B. *Internet-ports*.

(2) Setzen Sie den Haken bei den **Dienst**, die Mitglieder dieser Gruppe sein sollen, hier *ftp*, *http* und *http (SSL)*.

(3) Bestätigen Sie mit **OK**.

Fassen Sie ebenfalls HTTP und Telnet in die Gruppe *Administrationsports* für die Administration des Gateways zusammen.

9.2.3 Konfiguration der Filterregeln

Nachdem die Konfiguration der Aliasnamen für IP-Adressen und Dienste abgeschlossen ist, können Sie nun im Menü **Firewall** -> **Richtlinien** die Filterregeln definieren.

Eine vollständige Filterregelkette könnte wie folgt aussehen.

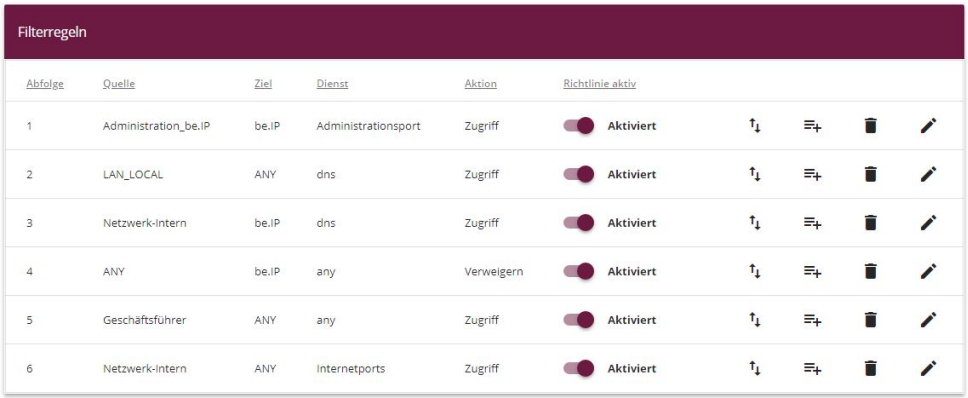


Abb. 165: **Firewall** -> **Richtlinien** -> **Filterregeln**

Wichtig

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 Internet und / oder dem Gateway mehr möglich ist!

Konfigurieren Sie zuerst eine Regel, die es erlaubt, dass der Administrator und der Geschäftsführer per HTTP und per Telnet auf das Gateway zugreifen dürfen. Diese Regel muss als erste definiert werden, da sonst keine Kommunikation mehr zum **GUI** möglich ist.

Gehen Sie in folgendes Menü, um eine neue Regel zu erstellen:

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

(2) Klicken Sie auf **Neu**, um eine neue Regel zu erstellen.

(3) Wählen Sie bei **Quelle** die Gruppe *Administration_be.IP*.

(4) Wählen Sie bei **Ziel** *be.IP*.

(5) Wählen Sie bei **Dienst** *Administrationsports*.

(6) Wählen Sie bei **Aktion** *Zugriff*.

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

Konfigurieren Sie als nächstes eine Regel, die es dem Gateway erlaubt, DNS-Anfragen an das Internet weiterzuleiten.

Gehen Sie in folgendes Menü, um eine neue Regel zu erstellen:

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

(2) Klicken Sie auf **Neu**, um eine neue Regel zu erstellen.

(3) Wählen Sie bei **Quelle** *LOCAL*.

(4) Wählen Sie bei **Ziel** *ANY*.

(5) Wählen Sie bei **Dienst** *dns*.

(6) Wählen Sie bei **Aktion** *Zugriff*.

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

Konfigurieren Sie weiterhin eine Regel, die es dem gesamten Netzwerk erlaubt, DNS-Anfragen an das Gateway zu stellen.

Gehen Sie in folgendes Menü, um eine neue Regel zu erstellen:

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

(2) Klicken Sie auf **Neu**, um eine neue Regel zu erstellen.

(3) Wählen Sie bei **Quelle** *Netzwerk_Intern*.

(4) Wählen Sie bei **Ziel** *be.IP*.

(5) Wählen Sie bei **Dienst** *dns*.

(6) Wählen Sie bei **Aktion** *Zugriff*.

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

Konfigurieren Sie nun eine Regel, die sämtliche andere Anfragen an das Gateway abweist.

Gehen Sie in folgendes Menü, um eine neue Regel zu erstellen:

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

(2) Klicken Sie auf **Neu**, um eine neue Regel zu erstellen.

(3) Wählen Sie bei **Quelle** *ANY*.

(4) Wählen Sie bei **Ziel** *be.IP*.

(5) Wählen Sie bei **Dienst** *any*.

(6) Wählen Sie bei **Aktion** *Verweigern*.

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

Konfigurieren Sie nun eine Regel, die dem Geschäftsführer alle Dienste im Internet erlaubt.

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

(2) Klicken Sie auf **Neu**, um eine neue Regel zu erstellen.

(3) Wählen Sie bei **Quelle** *Geschäftsführer*.

(4) Wählen Sie bei **Ziel** *ANY*.

(5) Wählen Sie bei **Dienst** *any*.

(6) Wählen Sie bei **Aktion** *Zugriff*.

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

Konfigurieren Sie als letztes die Regel, die dem internen Netzwerk die Dienste HTTP, HTTPS und FTP erlaubt.

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

(2) Klicken Sie auf **Neu**, um eine neue Regel zu erstellen.

(3) Wählen Sie bei **Quelle** *Netzwerk_Intern*.

(4) Wählen Sie bei **Ziel** *ANY*.

(5) Wählen Sie bei **Dienst** *Internetports*.

(6) Wählen Sie bei **Aktion** *Zugriff*.

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

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

9.3 Ergebnis

Durch diese Konfiguration haben Sie die Firewall so konfiguriert, dass das Gateway DNS-Anfragen ins Internet weiterleiten darf und dem internen Netzwerk die Dienste HTTP, HTTPS und FTP zu Verfügung stehen. Dem Administrator ist zusätzlich der Zugriff auf das Gateway erlaubt, und der Geschäftsführer kann alle Dienste im Internet nutzen. Sämtlicher anderer Datenverkehr wird durch das Gateway unterbunden.

9.4 Überprüfen der Konfiguration

Wenn Sie auf der Shell des Gateways `debug all` eingeben, können Sie mitverfolgen, wie das Gateway Datenverkehr entsprechend der Filterregeln zulässt oder abweist.

```
be.IP:>    debug all
01:43:23 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.2:1396]   -> be.IP[1:192.168.0.1:53] dns:17
01:43:28 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.2:2389]   -> ANY[10001:66.249.85.99:80] http:6
01:43:41 DEBUG/INET: SIF: No Rule, Ignore [1000:192.168.0.2:8]            -> [10001:62.146.2.103:0] :1
01:44:02 DEBUG/INET: SIF: Accept Administrator[1000:192.168.0.2:2393]     -> be.IP [1:192.168.0.1:23] telnet:6
01:44:31 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.50:1396]  -> be.IP [1:192.168.0.1:53] dns:17
01:44:34 DEBUG/INET: SIF: Accept Geschaeftsfuehrer[1000:192.168.0.50:137] -> ANY[1000:192.168.0.255:137] any:17
01:44:34 DEBUG/INET: SIF: Accept Geschaeftsfuehrer[1000:192.168.0.50:123] -> ANY[10001:207.46.232.189:123] any:17
01:44:41 DEBUG/INET: SIF: Accept Geschaeftsfuehrer[1000:192.168.0.50:8]   -> ANY[10001:62.146.2.103:0] any:1
01:44:43 DEBUG/INET: SIF: Accept Geschaeftsfuehrer[1000:192.168.0.50:138] -> ANY[1000:192.168.0.255:138] any:17
be.IP:>
```

In diesem Debug-Auszug ist z. B. zu sehen, dass ein Pingversuch von 192.168.0.2 auf die Adresse 62.146.2.103 abgewiesen wurde. DNS-Anfragen oder z. B. eine Telnetverbindung des Geschäftsführers wurden zugelassen.

9.5 Konfigurationsschritte im Überblick

Aliasnamen für IP-Adressen und Netzadressen

Feld	Menü	Wert
Beschreibung	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *Administrator*
Adresstyp	**Firewall -> Adressen -> Adressliste -> Neu**	*Adresse/Subnetz*
Adresse/Subnetz	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *192.168.0.2* mit *255.255.255.255*
Beschreibung	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *Geschäftsführer*
Adresstyp	**Firewall -> Adressen -> Adressliste -> Neu**	*Adresse/Subnetz*
Adresse/Subnetz	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *192.168.0.3* mit *255.255.255.255*
Beschreibung	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *be.IP*
Adresstyp	**Firewall -> Adressen -> Adressliste -> Neu**	*Adresse/Subnetz*
Adresse/Subnetz	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *192.168.0.254* mit *255.255.255.255*
Beschreibung	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *Netzwerk-Intern*
Adresstyp	**Firewall -> Adressen -> Adressliste -> Neu**	*Adresse/Subnetz*
Adresse/Subnetz	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *192.168.0.0* mit *255.255.255.0*

Adressgruppen

Feld	Menü	Wert
Beschreibung	**Firewall -> Adressen -> Gruppen -> Neu**	z. B. *Administrati-on_be.IP*
Auswahl	**Firewall -> Adressen -> Gruppen -> Neu**	z. B. *Administrator* und *Geschäftsführer*

Dienstgruppen

Feld	Menü	Wert
Beschreibung	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *Internetports*
Mitglieder	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *http*, *http (SSL)* und *ftp*
Beschreibung	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *Administrations-ports*
Mitglieder	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *http* und *telnet*

Filterregeln

Feld	Menü	Wert
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Administration_be.IP*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*be.IP*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Administrationsports*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LOCAL*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*ANY*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*dns*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Netzwerk_Intern*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*be.IP*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*dns*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** ->	*ANY*

Feld	Menü	Wert
	Filterregeln -> **Neu**	
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*be.IP*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Verweigern*
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Geschäftsführer*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*ANY*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Netzwerk_Intern*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*ANY*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Internetports*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Zugriff*

Kapitel 10 Sicherheit - VPN-Anbindung über einen SMS PASSCODE-Server

10.1 Einleitung

Dieser Workshop beschreibt die VPN IPSec-Client-Anbindung des **bintec Secure IPSec Cliens** an ein bintec VPN-Gateway mit zusätzlicher Einmalpasswort-Authentifizierung. Dieses wird dem Benutzer während dem Verbindungsaufbau in Form einer SMS mitgeteilt (IPSec One-Time-Passwort). Die Benutzer und deren Mobilfunkrufnummern werden im Active Directory eines Windows 2008-Servers verwaltet und zur VPN IPSec-Authentifizierung wird ein bintec VPN-Gateway (z .B. **bintec be.IP**) eingesetzt. Die One-Time-Passwort-Software von **SMS PASSCODE** greift zum SMS-Versand der One-Time-Passwörter auf das Active Directory zu und authentifiziert den Benutzer mit Hilfe des im Windows 2008-Server integrierten RADIUS-Server (NPS).

Zur Konfiguration des bintec VPN-Gateways wird hierbei das **GUI** (Graphical User Interface) verwendet.

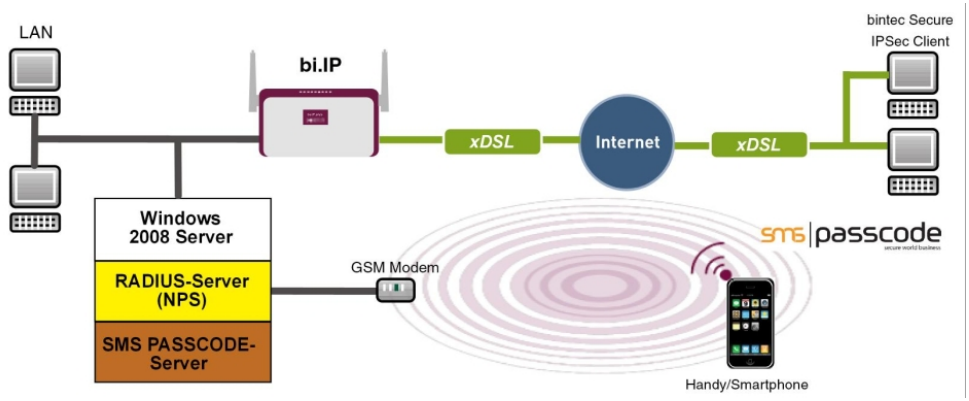


Abb. 166: Beispielszenario

Voraussetzungen

- Ein bintec VPN-Gateway (z. B. **bintec be.IP** Version 10.1.1) welches im Internet per IP-Adresse oder per DNS erreichbar ist
- Ein Windows-Server (z. B. Windows Server 2008 R2) mit installierter Active Directory Rolle und verfügbarem Netzwerkrichtlinien-Server (NPS / RADIUS Server)

- One-Time-Passwort-Software von **SMS PASSCODE** Version 6 mit kompatiblem GSM-Modem / SIM-Karte (siehe dazu *http://www.smspasscode.com*)
- Mindestens ein **bintec Secure IPSec Client**

10.2 Konfiguration

10.2.1 Hinweise während der Installation und Konfiguration des SMS PASSCODE-Servers

Dieser Abschitt des Workshops gibt einige Hinweise zur Installation und Konfiguration des **SMS PASSCODE**-Servers. Hierfür sollte in erster Line das **SMS PASSCODE** Administrations-Handbuch verwendet werden. In diesem Dokument werden die einzelnen Installationsschritte sowie die Konfiguration des RADIUS-Servers sehr ausführlich erläutert (siehe *http://www.smspasscode.com*).

10.2.2 Vorbereitungen zur Installation des SMS PASSCODE-Servers

Vor der Installation des **SMS PASSCODE**-Servers muss ein RADIUS-Server (Bestandteil des Windows Server 2003 / 2008) installiert werden. Bei dem in diesem Beispiel verwendeten Windows-Server 2008 wird der RADIUS-Server durch hinzufügen der NPS-Rolle bzw. des **Netzwerkrichtlinien-Servers (Windows Server 2008 (R2))** installiert.

Vor der Installation der **SMS PASSCODE**-Software muss zum Versenden der SMS-Nachrichten ein GSM-Modem am Windows-Server angebunden werden. **SMS PASSCODE** unterstützt unter anderem GSM-Modem von Cinterion (früher Siemens) wie z. B. die Modelle MC35i, MC52i, MC55i, TC65 oder MC75.

Zum Versand der SMS-Nachrichten wird für das GSM-Modem eine SIM-Karte benötigt.

10.2.3 Installation des SMS PASSCODE-Servers

Bei der eigentlichen Installation der **SMS PASSCODE** Server-Software sollte das Kapitel **Simple Installation** aus dem **SMS PASSCODE** Administrations-Handbuch als Referenz verwendet werden. Bei der Simple Installation werden alle Bestandteile auf einem Server installiert.

Im Installations-Assistententen ist die serielle COM-Schnittstelle des GSM-Modems auszuwählen. In diesem Dialog kann auch die PIN-Nummer der SIM-Karte eingegeben werden.

In einem weiteren Schritt des Installations-Assistenten sind die Authentifizierungsarten aus-

zuwählen.

Zur späteren Anbindung des bintec VPN-Gateways muss in diesem Scenario *RADIUS client protection* ausgewählt werden.

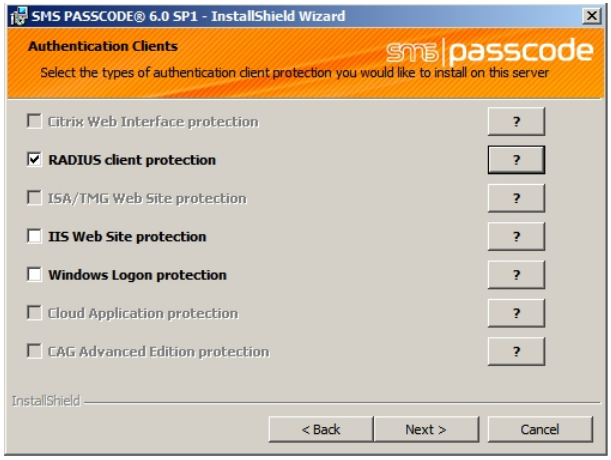


Abb. 167: **SMS PASSCODE**

10.2.4 Konfiguration des Web-Administration-Tools

Nach erfolgreicher Installation des **SMS PASSCODE**-Servers kann die Konfiguration mit dem Web-Administration-Tool begonnen werden. **SMS PASSCODE** bietet eine eigene Benutzerverwaltung oder den Zugriff auf das **Active Directory** des Mirosoft Windows Servers an. In diesem Scenario sollen die Benutzer des **Active Directory** verwenden, welche hierzu in eine eigene Benutzergruppe z. B. **SMS Passcode Users** hinzugefügt wurden. Bitte beachten Sie, dass für jeden Benutzer eine Mobilfunkrufnummer hinterlegt sein muss.

Für den Zugriff des **SMS PASSCODE**-Servers auf die Benutzergruppe **SMS Passcode Users** des **Active Directory** wird im Menü **Settings** -> **General** die *AD Integration* aktiviert.

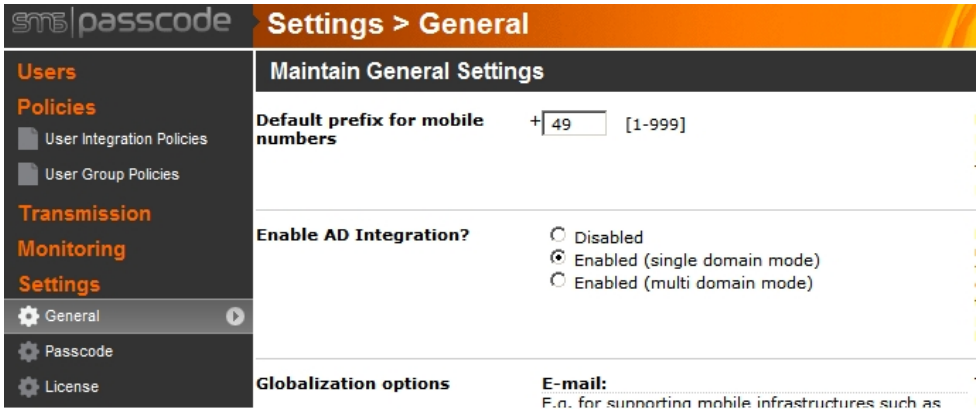


Abb. 168: **Settings** -> **General**

Anschließend können im Menü **Policies** -> **User Integration Policies** weitere Einstellungen zum Zugriff auf die Benutzer des **Active Directory** festgelegt werden.

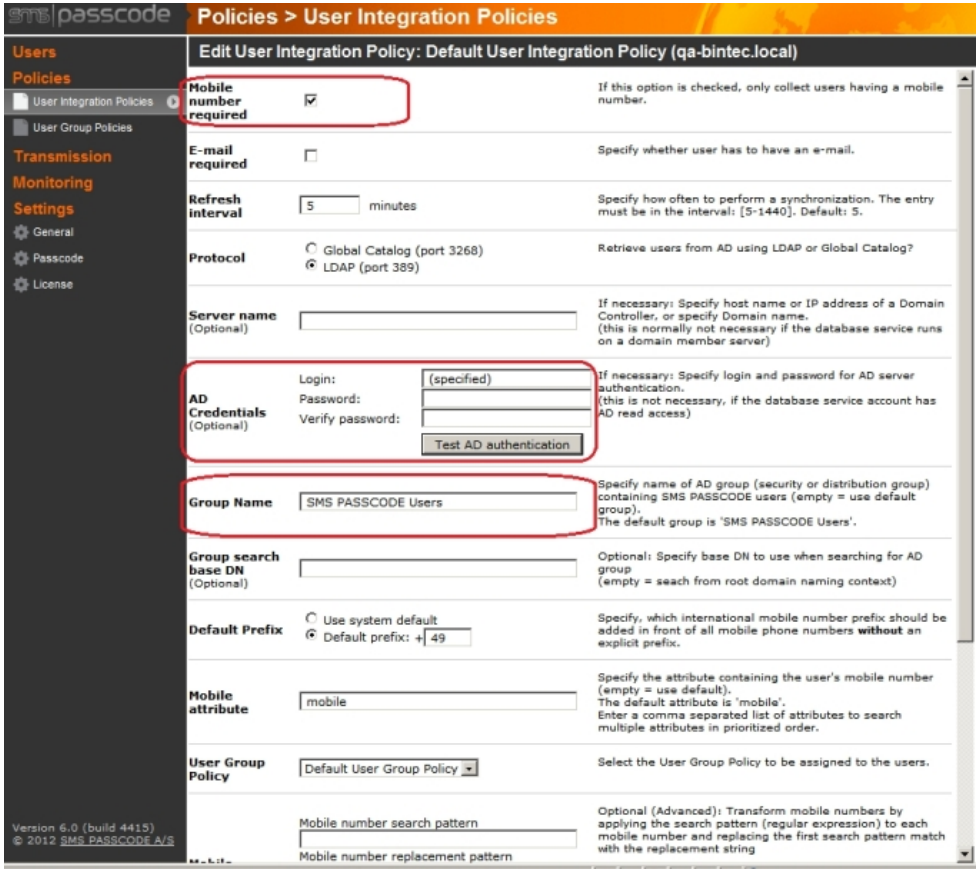


Abb. 169: **Policies** -> **User Integration Policies**

(1) Aktivieren Sie die Option *`Mobile number required`*.

(2) Legen Sie die **Zugangsdaten** für das **Active Directory** und die **Benutzergruppe** der **SMS PASSCODE**-Benutzer fest.

Eine genaue Beschreibung zur **Active Directory**-Integration des **SMS PASSCODE**-Servers ist Bestandteil des **SMS PASSCODE** Administrations-Handbuchs.

10.2.5 Konfiguration des RADIUS-Server zur Anbindung des VPN-Gateways

Die Anbindung des bintec VPN-Gateways erfolgt mit Hilfe des bereits installieren RADIUS-Server (NPS-Server Rolle in Windows 2008 Server). Die Anbindung eines RADIUS-Clients (= bintec VPN-Gateway) am RADIUS-Server erfolgt mit Hilfe der Microsoft Management Console:

- Im Falle eines Windows Server 2003 wird der **Internet Authentication Service (IAS)**

verwendet.

- Bei Verwendung eines Windows Server 2008 wird die Microsoft Management Console für **Network Policy Server (NPS)** verwendet.

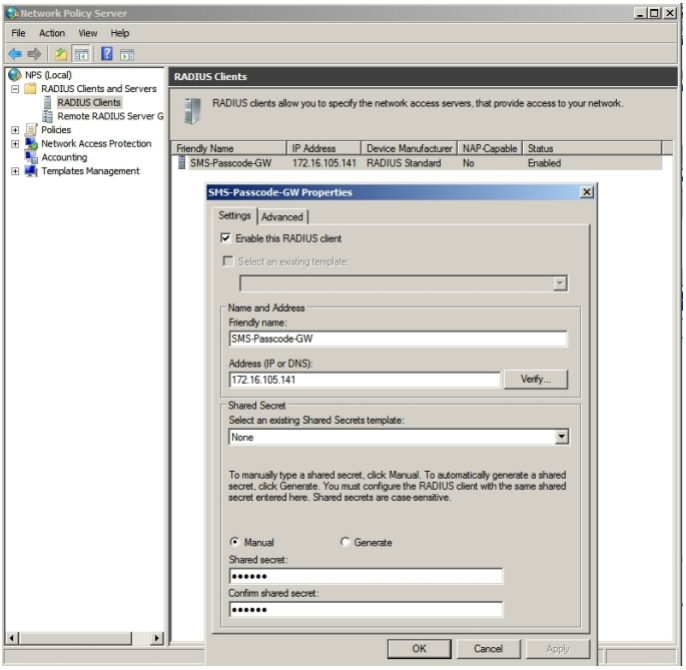


Abb. 170: **Network Policy Server (NPS)**

(1) Aktivieren Sie die Option *Enable this RADIUS client*.

(2) Unter **Friendly name** geben Sie eine Beschreibung für das bintec VPN-Gateway ein, z. B. *SMS Passcode-GW*.

(3) Geben Sie die **IP-Adresse** oder den **Hostnamen** des bintec VPN-Gateways ein, z. B. *172.16.105.141*.

(4) Geben Sie ein **Passwort** für die RADIUS-Kommunikation mit dem VPN-Gateway ein, z. B. *supersecret*.

(5) Bestätigen Sie Ihre Eingaben mit **OK**.

10.2.6 Konfiguration des VPN-Gateways

In diesem Scenario wird bei der VPN-Konfiguration am bintec-Gateway ein IPSec-Peer-Konfigurationseintrag angelegt der den gleichzeitigen Verbindungsaufbau mehrerer Clients ermöglicht (IPSec Multi-User). Im Anschluss an die IPSec Pre-Shared-Key-Authentifizierung erfolgt über den RADIUS-Server die One-Time-Authentifizierung zwischen dem bintec VPN-Client und dem **SMS PASSCODE**-Server.

Hinweis

Anstelle der **Multi-User-IPSec-Konfiguation** besteht auch die Möglichtkeit für jeden VPN-Client einen eigenen IPSec-Peer-Konfigurationseintrag anzulegen.

Die Priorität des Multi-User-IPSec Peers muss immer niedriger als von anderen IPSec-Peer-Konfigurationseinträgen sein.

Zur Anbindung des RADUIS-Server am bintec VPN-Gateway gehen Sie in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**.

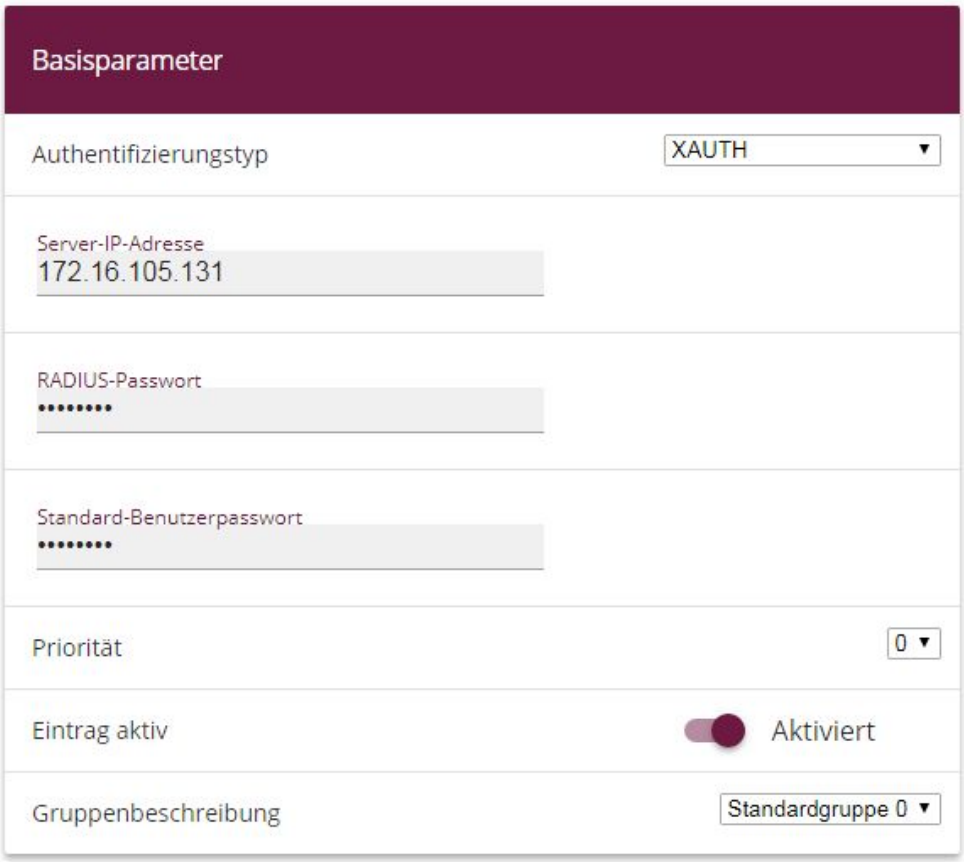


*Abb. 171: 0***Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie den **Authentifizierungstyp** *XAUTH* aus, um die Authentifizierung über

den Windows Server zu ermöglichen.

(2) Zur Kommunikation mit dem Microsoft RADIUS-Server geben Sie die **Server-IP-Adresse** ein, z. B. `172.16.105.131`.

(3) Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte **Passwort**, z. B. `supersecret` ein.

(4) Bestätigen Sie Ihre Eingaben mit **OK**.

Um dem VPN-Profil des Multi-User-IPSec Peers einen IP-Pool zuweisen zu können, muss ein Adresspool angelegt werden.

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

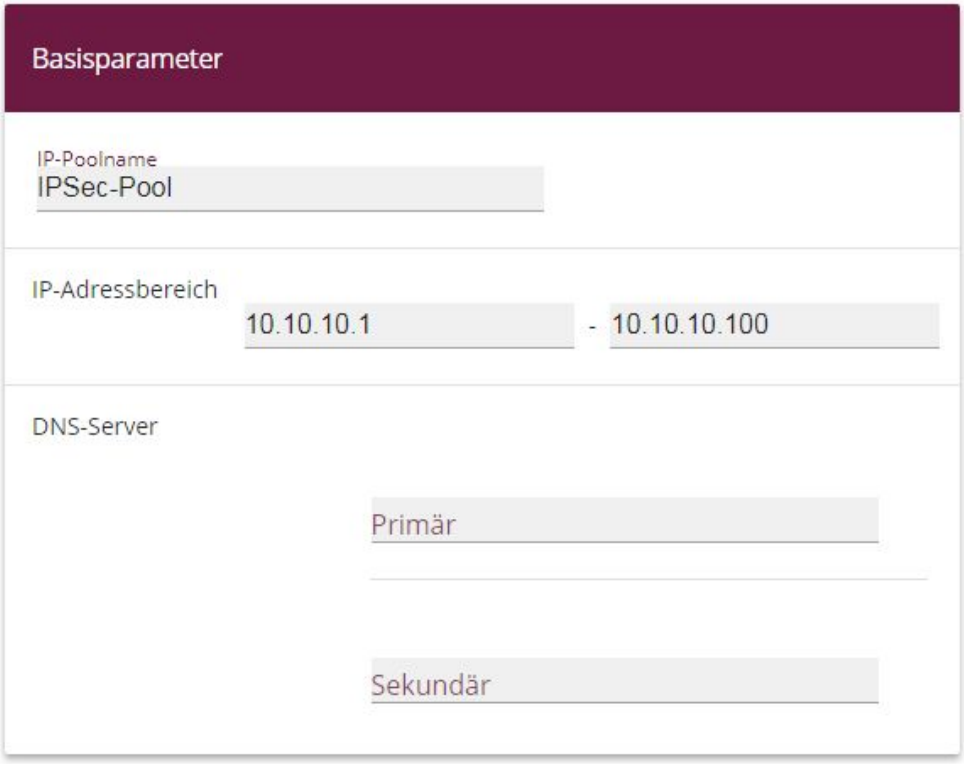


Abb. 172: **VPN** -> **IPSec** -> **IP Pools** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie bei **IP-Poolname** die Bezeichnung des IP Pools ein, z. B. `IPSec-Pool`.

(2) Bei **IP-Adressbereich** geben Sie im ersten Feld die erste IP-Adresse des Adresspools ein, z. B. `10.10.10.1`.

(3) Geben Sie im zweiten Feld die letzte IP-Adresse des Adresspools ein, z. B.

10.10.10.100.

(4) Klicken Sie auf **OK**.

Anschließend muss ein Profil angelegt werden, um auf den RADIUS-Server verweisen zu können.

Gehen Sie zu **VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**.

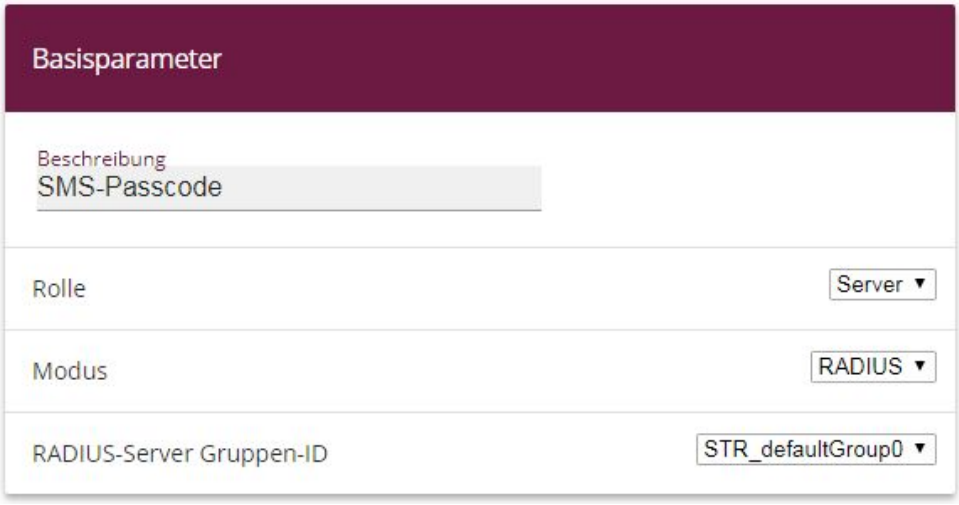


Abb. 173: **VPN** -> **IPSec** -> **XAUTH-Profile** -> **Neu**

Gehen Sie folgendermaßen vor, um ein Profil einzurichten:

(1) Geben Sie eine **Beschreibung** für dieses XAuth-Profil ein, z. B. *SMS Passcode*.

(2) Wählen Sie die **Rolle** des Gateways bei der XAuth-Authentifizierung aus, hier *Server*.

(3) Bei **Modus** wählen Sie *RADIUS* aus. Die Authentifizierung wird über den RADIUS-Server durchgeführt.

(4) Bestätigen Sie mit **OK**.

Nun wird noch der eigentliche **IPSec-Peer** angelegt.

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

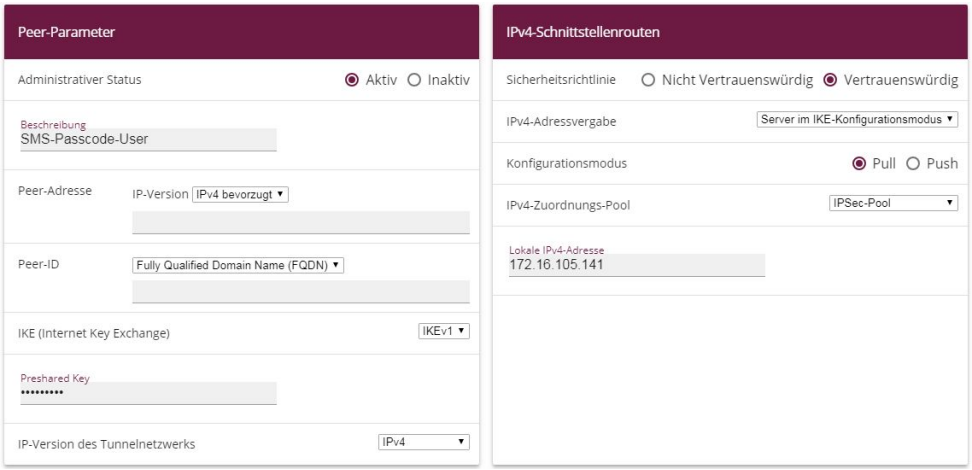


Abb. 174: **VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie eine **Beschreibung** des Peers ein, die diesen identifiziert, z. B. *SMS Passcode-User*.

(2) In diesem Scenario wird keine IPSec-Peer-ID hinterlegt um die Multi-User-IPSec-Verbindungen zu ermöglichen.

(3) Bei **Preshared Key** geben Sie das mit dem Peer vereinbarte Passwort ein, z. B. *supersecret*.

(4) Bei **IPv4-Adressvergabe** wählen Sie den Konfigurationsmodus der Schnittstelle, hier *Server im IKE-Konfigurationsmodus* aus.

(5) Wählen Sie einen konfigurierten **IPv4-Zuordnungs-Pool** aus, z. B. *IPSec-Pool*.

(6) Geben Sie bei **Lokale IPv4-Adresse** die LAN IP-Adresse des VPN-Gateways ein, z. B. *172.16.105.141*.

(7) Klicken Sie auf **Erweiterte Einstellungen**.

Abb. 175: **VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**->**Erweiterte Einstellungen**

(8) Mit der Auswahl *Keines (Standardprofil verwenden)* wird das in **Phase-**

1-Profil / **Phase-2-Profil** als Standard markierte Profil verwendet.

(9) Wählen Sie das bereits konfigurierte **XAUTH-Profil** aus, z. B. `SMS-Pascode`.

(10) Setzen Sie bei **Anzahl erlaubter Verbindungen** auf `Mehrere Benutzer` um den IPSec Multi-User-Modus zu aktivieren.

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

10.2.7 Konfiguration des bintec Secure IPSec Clients

Der **bintec Secure IPSec Clients** wird über **Start** -> **Programme** -> **bintec Secure IPSec Client** -> **Secure Client Monitor** aufgerufen. Die Konfiguration des **bintec Secure IPSec Clients** wird über den Assistenten durchgeführt. Beim ersten Start des **bintec Secure IPSec Clients** wird der **Assistent für neues Profil** automatisch gestartet. Wählen Sie die Auswahl **Verbindung zum Firmennetz über IPSec** aus.

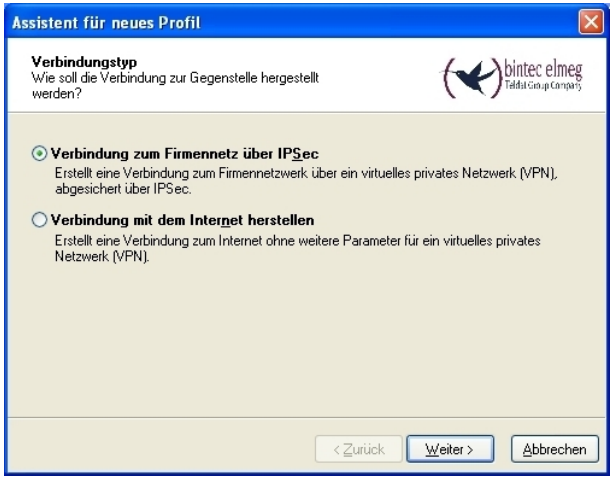


Abb. 176: Verbindungstyp

Geben Sie einen Namen für das Profil ein z. B. `Zentrale`.

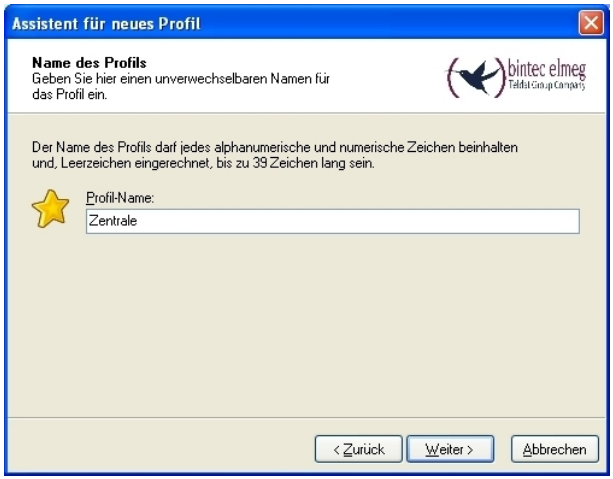


Abb. 177: Profil-Name

Im nächsten Schritt des Assistenten muss ein **Verbindungsmedium** ausgewählt werden über welches eine Verbindung zum Internet aufgebaut wird. In unserem Beispiel wird die Auswahl *LAN (over IP)* verwendet da der VPN-Client keinen direkten Zugang zum Internet herstellt sondern einen Internetzugangsrouter verwendet.

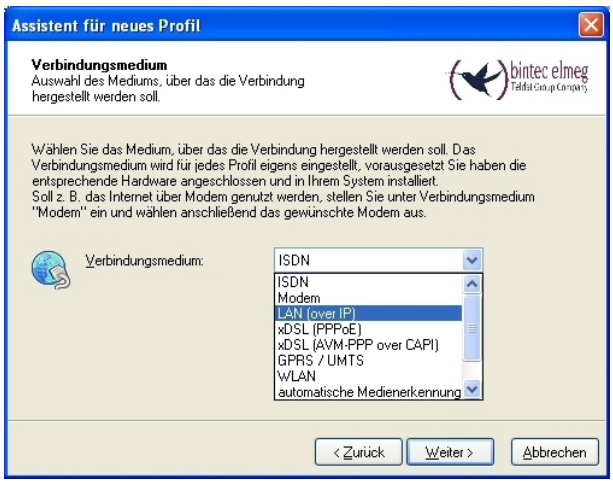


Abb. 178: Verbindungsmedium

Bei der Option **Gateway (Tunnel-Endpunkt)** wird die Adresse hinterlegt über die das VPN-Gateway aus dem Internet erreichbar ist. Aktivieren Sie die Option *Erweiterte Authentifizierung (XAUTH)*.

Hinweis

Bei XAUTH **Benutzername** und **Passwort** können die Windows Active Directory Anmelde-Daten des jeweiligen Benutzers hinterlegt werden.

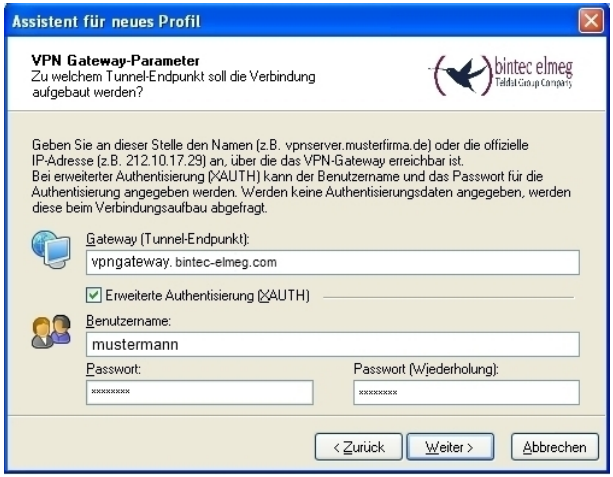


Abb. 179: VPN Gateway-Parameter

Anschließend wird als **Austausch-Modus** der `Aggressive Mode` verwendet, da dem **bintec be.IP** Router und dem **bintec Secure IPSec Client** dynamische IP-Adresse vom Provider zugewiesen werden. Die **PFS-Gruppe** setzen Sie z. B. auf `DH-Gruppe 2 (1024 Bit)`. Die Option `Benutze IP-Kompression` wird in dieser Konfiguration nicht eingesetzt.

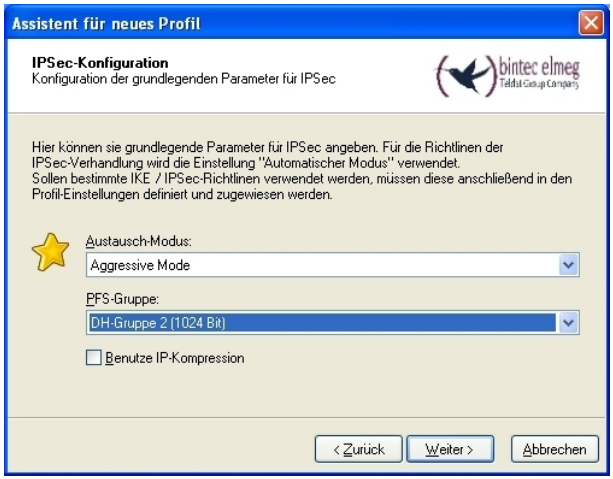


Abb. 180: IPSec-Konfiguration

Im nächsten Schritt des Assistenten wird der am VPN-Gateway hinterlegte **Preshared Key** sowie die IPSec **ID** des VPN-Clients hinterlegt.

Die Auswahl im Feld **Type** muss passend zur eigentlichen IPSec ID gewählt werden (z. B. `Fully Qualified Username` bei Verwendung einer ID in Form einer E-Mail-Adresse).

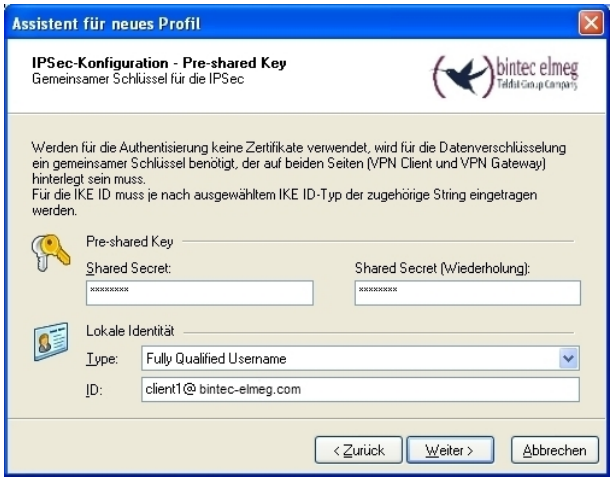


Abb. 181: Pre-shared Key

In diesem Beispiel wird dem VPN IPSec-Client eine dynamische VPN IP-Adresse zugewiesen. Dazu muss die Option `IKE Config Mode verwenden` ausgewählt werden.

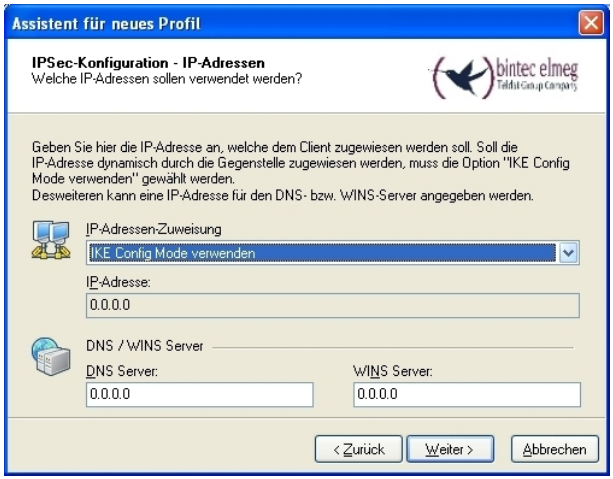


Abb. 182: IKE Config Mode

Im letzten Schritt wird die **Firewall** des **bintec Secure IPSec Clients** konfiguriert. Wenn der Client direkt mit dem Internet verbunden ist, sollte die Firewall aktiviert sein.

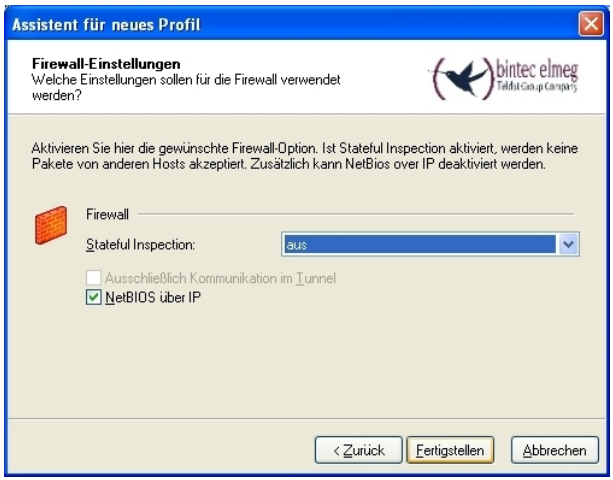


Abb. 183: Firewall

10.3 Test der VPN-Verbinduing / Debug-Meldungen des VPN-Gateways

Zu Beginn des Verbindungsaufbaus wird der **bintec Secure IPSec Clients** mit Hilfe des Pre-Shared-Keys authentifiziert. Anschließend erfolgt eine zweifache Benutzer/Passwort Abfrage welche über den Windows- und dem **SMS PASSCODE**-Server authentifiziert wird. Hierbei wird zuerst die Anmeldung mit dem jeweiligen Windows Active Directory Benutzer und Passwort durchgeführt wodurch der **SMS PASSCODE**-Server einen Benutzer und dessen Mobilfunkrufnummer zuordnen kann. Daraufhin wird ein Einmal-Passwort per SMS versendet. Nach Eingabe des per SMS erhaltenen Passworts wird der VPN-Tunnel vollständig aufgebaut.

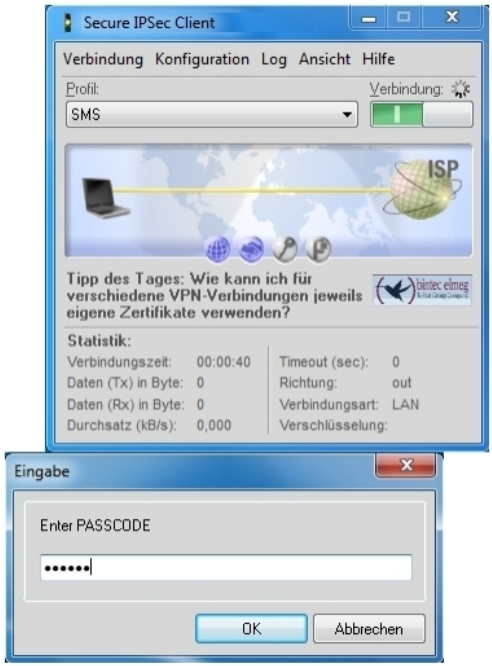


Abb. 184: Secure IP Sec Client

Debug Meldungen des VPN-Gateways beim Verbindungsaufbau

```
P1: peer 0 () sa 3 (R): new ip 172.16.105.141 <- ip 172.16.105.130
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'da8e937880010000'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'draft-ietf-ipsra-isakmp-xauth-06'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'draft-ietf-ipsec-nat-t-ike-03'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'draft-ietf-ipsec-nat-t-ike-02'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'draft-ietf-ipsec-nat-t-ike-00'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is '4a131c81070358455c5728f20e95452f'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'Dead Peer Detection (DPD, RFC 3706)'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'cb1ed48b6d68269bb411b61a07bc9e07'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'c61baca1f1a60cc108000000000000000'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is '4048b7d56ebce88525e7de7f00d6c2d3c0000000'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is '12f5f28c457168a9702d9fe274cc0100'
P1: peer 1 (SMS-user1) sa 3 (R): identified ip 172.16.105.141 <- ip 172.16.105.130
P1: peer 1 (SMS-user1) sa 3 (R): notify id fqdn(any:0,[0..5]=rt3002) <- id usr@fqdn(any:0,[0..15]=mustermann@teldat.de ):
Initial contact notification proto 1 spi(16) = [ba868f6b b0d5e4e3 : dcf124bb fa22f6bc]
Dynamic Client: Created Child Peer SMS-user1-2 (30002) IP 172.16.105.130 ID mustermann@bintec-elmeg.com for Parent SMS-user1 (1)
P1: peer 30002 (SMS-user1-2) sa 3 (R): identified ip 172.16.105.141 <- ip 172.16.105.130
P1: peer 30002 (SMS-user1-2) sa 3 (R): done id fqdn(any:0,[0..5]=rt3002) <- id usr@fqdn(any:0,[0..15]=mustermann@teldat.de )
AG[ba868f6b b0d5e4e3 : dcf124bb fa22f6bc]
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): request client for extended authentication
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): reply for extended authentication received
RADIUS: requested user mustermann
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): request client for extended authentication
CFG: peer 30002 (SMS-user1-2) sa 3 (R): request for ip address received
CFG: peer 30002 (SMS-user1-2) sa 3 (R): ip address 100.100.100.2 assigned
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): created 0.0.0.0/0:0 < any > 100.100.100.2/32:0 rekeyed 0
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): SA 5 established ESP[5e154fc4] in[0] Mode tunnel enc aes-cbc (128 bit)
auth md5 (128 bit)
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): SA 6 established ESP[8b23d731] out[0] Mode tunnel enc aes-cbc (128 bit)
auth md5 (128 bit)
Activate Bundle 3 (Peer 30002 Traffic -1)
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): established  (172.16.105.141<->172.16.105.130) with 2 SAs life 28800 Sec/0
Kb rekey 25920 Sec/0 Kb Hb none PMTU
P1: peer 30002 (SMS-user1-2) sa 3 (R): DPD: received request sequence 2079799787
P1: peer 30002 (SMS-user1-2) sa 3 (R): DPD: sent response sequence 2079799787
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): reply for extended authentication received
RADIUS: requested user mustermann
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): reply for extended authentication received
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): extended authentication for user 'mustermann' succeeded
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): created 0.0.0.0/0:0 < any > 100.100.100.2/32:0 rekeyed 3
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): SA 7 established ESP[3b8c19bc] in[0] Mode tunnel enc aes-cbc (128 bit)
auth md5 (128 bit)
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): SA 8 established ESP[ddc2f16b] out[0] Mode tunnel enc aes-cbc (128 bit)
auth md5 (128 bit)
Activate Bundle 4 (Peer 30002 Traffic -1)
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): established  (172.16.105.141<->172.16.105.130) with 2 SAs life 28800 Sec/0
Kb rekey 25920 Sec/0 Kb Hb none PMTU
```

10.4 Konfigurationsschritte im Überblick

Installation des SMS PASSCODE-Servers

Feld	Menü	Wert
RADIUS client protection	**SMS PASSCODE -> InstallShield Wizard**	*Aktiviert*

Konfiguration des Web-Administration Tools

Feld	Menü	Wert
Enable AD Integration	**Settings -> General**	*Enabled (single domain mode)*
Mobile number required	**Policies -> User Integration Policies**	*Aktiviert*
AD Credentials	**Policies -> User Integration Policies**	Login / Password
Group Name	**Policies -> User Integration Policies**	z. B. *SMS PASSCODE Users*

Konfiguration des RADIUS-Server

Feld	Menü	Wert
Enable this RADIUS client	**Network Policy Server -> RADIUS Clients**	*Aktiviert*
Friendy name	**Network Policy Server -> RADIUS Clients**	z. B. *SMA-Passcode-GW*
Address (IP or DNS)	**Network Policy Server -> RADIUS Clients**	z. B. *172.16.105.141*
Shared secret	**Network Policy Server -> RADIUS Clients**	z. B. *supersecret*

Konfiguration des VPN-Gateways

Feld	Menü	Wert
Authentifizierungstyp	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	*XAUTH*
Server-IP-Adresse	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	z. B. *172.16.105.131*
RADIUS-Passwort	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	z. B. *supersecret*

IP-Adresspool anlegen

Feld	Menü	Wert
IP-Poolname	**VPN -> IPSec -> IP Pools -> Neu**	z. B. *IPSec-Pool*

Feld	Menü	Wert
IP-Adressbereich	**VPN -> IPSec -> IP Pools -> Neu**	z. B. *10.10.10.1 - 10.10.10.100*

XAUTH-Profil anlegen

Feld	Menü	Wert
Beschreibung	**VPN -> IPSec -> XAUTH-Profile -> Neu**	z. B. *SMS-Passcode*
Rolle	**VPN -> IPSec -> XAUTH-Profile -> Neu**	*Server*
Modus	**VPN -> IPSec -> XAUTH-Profile -> Neu**	*RADIUS*

IPSec-Peers konfigurieren

Feld	Menü	Wert
Beschreibung	**VPN -> IPSec -> IPSec-Peers -> Neu**	z. B. *SMS-Passcode-Users*
Preshared Key	**VPN -> IPSec -> IPSec-Peers -> Neu**	z. B. *supersecret*
IPv4-Adressvergabe	**VPN -> IPSec -> IPSec-Peers -> Neu**	*Server im IKE-Konfigurationsmodus*
IPv4-Zuordnungs-Pool	**VPN -> IPSec -> IPSec-Peers -> Neu**	*IPSec-Pool*
Lokale IPv4-Adresse	**VPN -> IPSec -> IPSec-Peers -> Neu**	z. B. *172.16.105.141*
Phase-1-Profil	**VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen**	*Keines (Standardprofil verwenden)*
Phase-2-Profil	**VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen**	*Keines (Standardprofil verwenden)*
XAUTH-Profil	**VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen**	*SMS-Passcode*
Anzahl erlaubter Verbindungen	**VPN -> IPSec -> IPSec-Peers -> Neu -> Erweiterte Einstellungen**	*Mehrere Benutzer*

Konfiguration des bintec Secure IPSec Clients

Feld	Menü	Wert
Verbindungstyp	**Assistent für neues Profil**	*Verbindung zum Firmennetz über IPSec*
Profil-Name	**Assistent für neues Profil**	*Zentrale*
Verbindungsmedi-	**Assistent für neues Profil**	*LAN (over IP)*

Feld	Menü	Wert
um		
Gateway (Tunnel-Endpunkt)	**Assistent für neues Profil**	z. B. *vpngateway.bintec-elmeg.com*
Erweiterte Authentifizierung (XAUTH)	**Assistent für neues Profil**	Aktiviert
Benutzername	**Assistent für neues Profil**	z. B. *mustermann*
Passwort	**Assistent für neues Profil**	z. B. *supersecret*
Austausch-Modus	**Assistent für neues Profil**	Aggressive Mode
PFS-Gruppe	**Assistent für neues Profil**	DH-Gruppe 2 (1024 Bit)
Shared Secret	**Assistent für neues Profil**	z. B. *bintec elmeg*
Shared Secret (Wiederholung)	**Assistent für neues Profil**	z. B. *bintec elmeg*
Typ	**Assistent für neues Profil**	z. B. *Fully Qualified Username*
ID	**Assistent für neues Profil**	z. B. *client1@bintec-elmeg.com*
IP-Adressen-Zuweisung	**Assistent für neues Profil**	*IKE Config Mode verwenden*
Stateful Inspection	**Assistent für neues Profil**	*aus*
NetBIOS über IP	**Assistent für neues Profil**	Aktiviert

Kapitel 11 Sicherheit - bintec elmeg Webfilter

Der bintec elmeg Webfilter ist eine Cloud-basierte Anwendung, mittels derer Sie den Zugriff aus Ihrem Netzwerk auf bestimmte Inhalte im Internet steuern und Aufrufe schädlicher Webseiten unterbinden können. Dazu konfigurieren Sie ihr Gerät so, dass DNS-Anfragen nicht mehr an den ungefilterten DNS-Server Ihres Internetanbieters gesendet werden, sondern an den DNS-Server des Webfilters. Dieser teilt dem Client in seiner Antwort dann entweder die IP-Adresse der gewünschten Seite mit - oder sendet eine Meldung, dass die Seite nicht angezeigt werden darf. Weitere Informationen über den Webfilter finden Sie hier: *http://www.bintec-elmeg.com/produkte/software/software/webfilter/* .

11.1 Einleitung

Der bintec elmeg Webfilter-Server bietet folgende Möglichkeiten der Filterung an:

- Sperrlisten (Blacklists): vordefinierte Kategorien bzw. private Kategorie für selbst erstellte Sperrlisten
- Integration von Google SafeSearch: Beschränkung der Google-Suchergebnisse
- Geolocation: Datenverkehr anhand geographischer Standorte erlauben oder blockieren
- Reporting: Echtzeitberichte und Auswertung der aufgerufenen Webseiten-Kategorien
- Benachrichtigungen bei Client-Anfragen zur Freigabe einer Webseite
- Zeitplaner: Aktiviert bzw. deaktiviert Sperrlisten zu bestimmten Zeiten

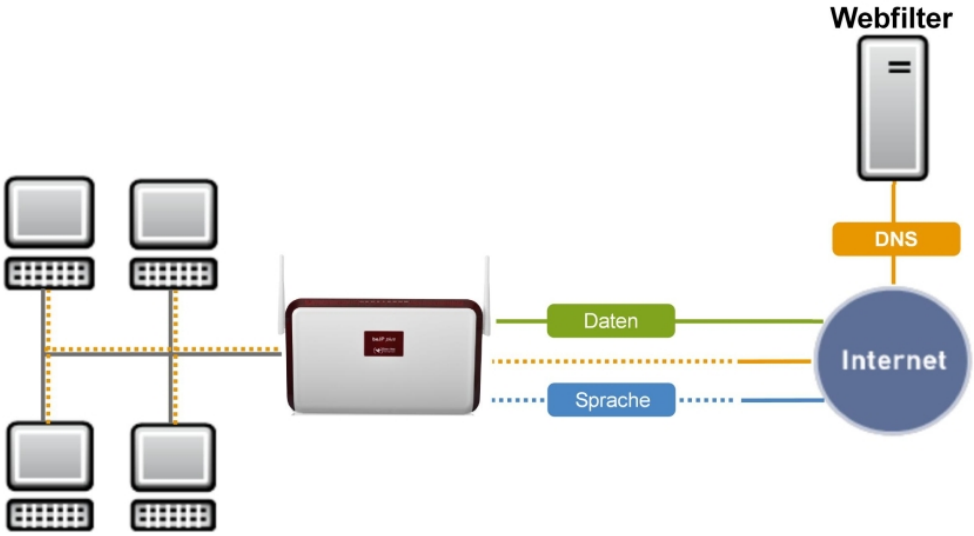


Abb. 185: Scenario

Voraussetzungen

- be.IP wird als DHCP-Server für angeschlossene Clients eingesetzt.
- be.IP hat die öffentliche IP-Adresse des Internetzugangs.
- Wichtig: Clients in Ihrem lokalen Netzwerk (LAN) verwenden für DNS-Anfragen die be.IP.

Allgemeine Funktionsweise des Webfilters

Die grundsätzliche Funktionsweise der Lösung ist wie folgt:

Die be.IP weist einem anfragenden DHCP-Client neben der IP-Adresse und dem Gateway auch die eigene Adresse als DNS-Server zu.

Alle DNS-Anfragen werden von der be.IP an einen der bintec elmeg Webfilter-DNS-Server weitergeleitet (185.236.104.104 bzw. 185.236.105.105). Sobald der Client eine Internetseite in seinem Browser aufruft, geschieht Folgendes:

(1) Die DNS-Anfrage des Clients wird an den Webfilter-DNS-Server gesendet.

(2) Der DNS-Server identifiziert das eingerichtete Profil auf der bintec elmeg Webfilter-Plattform anhand der Quell-IP-Adresse der DNS-Anfrage. Dies ist die öffentliche IP-Adresse Ihres Internetzugangs.

(3) Der DNS-Server prüft anhand der von Ihnen eingerichteten Richtlinien, ob die angefragte URL aufgelöst werden darf oder nicht.

- Darf die URL aufgelöst werden, teilt der DNS-Server die IP-Adresse per DNS-Antwort

mit.

- Darf die URL nicht aufgelöst werden, teilt der DNS-Server die IP-Adresse der bintec elmeg Webfilter-Plattform mit. Der Client ruft somit per HTTP(S) die bintec elmeg Webfilter-Webseite auf, die ihm mitteilt, dass der Aufruf der gewünschten Seite nicht erlaubt ist.

Hinweise zur Konfigurationsanleitung

- Die LAN-Schnittstelle in dieser Konfigurationsanleitung ist br0, die Schnittstelle für den Internetzugang heißt “WAN - Internet”.
- Die Firewall ist aktiv. Die LAN-Schnittstelle ist der vertrauenswürdigen Zone und die WAN-Schnittstelle der nicht vertrauenswürdigen Zone zugeordnet.
- Für das interne Netzwerk ist eine DHCP-Server-Konfiguration erforderlich.
- In Abhängigkeit von der Art der IP-Adresszuweisung an der Internet-Schnittstelle (statisch oder dynamisch) sind unterschiedliche Konfigurationen des Filters notwendig.
- Beachten Sie, dass die DNS-Auflösung für Clients im LAN ab dem Zeitpunkt des Einrichtens des DNS-Servers fehlschlagen kann, wenn der bintec elmeg Webfilter-Server noch nicht konfiguriert ist.
- Die be.IP wird über den Assistenten so konfiguriert, dass Anfragen an andere DNS-Server nicht zugelassen sind.

Aktuelle Einschränkungen

(1) IPv6 darf an der Schnittstelle, an der die LAN-Clients angeschlossen sind, nicht aktiv sein.

Software-Mindestversion

be.IP-Serie, RSxx3-Serie, R1202, RT1202, RXL12x00 mit Version 10.2.3 oder höher

11.2 Webfilter-Assistent

Zur Filterung unerwünschten Datenverkehrs und zum Schutz vor schädlichen Webseiten kann der bintec elmeg Webfilter über einen einfachen Konfigurationsassistenten eingerichtet werden.

Hinweis

Beachten Sie, dass Sie für den Betrieb des Webfilters eine Lizenz erwerben müssen. Informationen finden Sie unter
http://www.bintec-elmeg.com/produkte/software/software/webfilter/

11.2.1 Konfiguration auf dem Router

Mit dem Webfilter-Assistenten können Sie DNS-Server und Firewall sowie DynDNS-Einstellungen in einem einzigen Menü konfigurieren.

(1) Gehen Sie dazu in das Menü **Assistenten**->**Webfilter**.

(2) Aktivieren Sie die Funktion **Webfilter aktivieren**, um den Webfilter zu konfigurieren.

Abb. 186: **Assistenten**->**Webfilter**

Gehen Sie folgendermaßen vor:

(1) **LAN-Schnittstelle**
Wählen Sie aus, für welche der vorhandenen Ethernet- bzw. WLAN-Schnittstellen die Webfilterung aktiviert werden soll. Sie können hier lediglich eine Schnittstelle auswählen. Wählen Sie daher die Schnittstelle, in deren Netz sich die Clients befinden, deren Webanfragen gefiltert werden sollen, z.B. die Schnittstelle Ihres Gäste-WLANs.

(2) **IP-Adressbereich der gefilterten Clients**
Wenn Sie eine Schnittstelle ausgewählt haben, für die noch kein DHCP-Server eingerichtet ist, können Sie den zu filternden Bereich an IP-Adressen hier selbst einge-

ben.

(3) **Benutzername**
Geben Sie den Benutzernamen ein, unter dem Sie sich beim bintec elmeg Webfilter registriert haben.

(4) **Passwort**
Geben Sie das entsprechende Passwort ein.

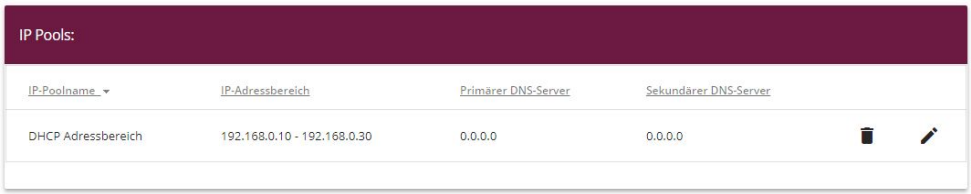
(5) **Filtermodus**
Wählen Sie den Filtermodus aus.
Standard: In dieser Betriebsart sendet Ihr Gerät Anfragen über die (statische oder dynamische) öffentliche IP-Adresse Ihres Routers an den Webfilter.
L2TP: Diese Betriebsart ermöglicht es, den Webfilter auch dann zu betreiben, wenn Ihr Router über keine eigene öffentliche Adresse verfügt, also z. B. wenn Ihr Internetanbieter sogenanntes Carrier Grade NAT durchführt, bei dem sich mehrere Router im Netz des Anbieters eine öffentliche Netzadresse teilen. In diesem Fall wird eine sog. Tunnelverbindung von Ihrem Gateway zum DNS-Server des Webfilters eingerichtet. Auch die dazu erforderlichen Einstellungen werden automatisch vorgenommen, hier aber nicht weiter abgebildet, da sie erweiterte Kenntnisse der Netzwerkkonfiguration erfordern.

(6) Sobald Sie die Einstellungen mit **OK** bestätigen, wird die Filterung aktiv.

11.2.1.1 Konfigurationsübersicht

Der Webfilter-Assistent nimmt Einstellungen in unterschiedlichen Menüs vor. Wenn Sie die Einstellungen überprüfen wollen, finden Sie diese in den folgenden Menüs:

Im Menü **Lokale Dienste** ->**DHCP-Server** ->**IP-Pool-Konfiguration** wird der vom Webfilter abgedeckte IP-Pool angezeigt:



Im Menü **Lokale Dienste** ->**DNS**->**Domänenweiterleitung** ist die Weiterleitung aller DNS-Anfragen an die DNS-Server des Webfilters angelegt:

Die Übersicht der Firewall-Richtlinien im Menü **Firewall**->**Richtlinien**->**IPv4-Filterregeln** enthält die Einträge, die Anfragen an andere DNS-Server unterbinden. Beachten Sie die Reihenfolge:

Im Menü **Lokale Dienste** ->**DynDNS-Client** ->**DynDNS-Aktualisierung** wird in der Liste die DynDNS-Registrierung angezeigt. Diese ist notwendig, wenn dem Webfilter eine dynamisch vergebene öffentlichen IP-Adresse als Adresse Ihres Netzwerks mitzuteilen ist.

11.3 Einrichtung des Webfilters

Die Konfiguration der Filterung selbst erfolgt in einer Web-Applikation. Benutzername und Passwort erhalten Sie bei der Registrierung.

Öffnen Sie einen Browser und geben Sie *http://webfilter.bintec-elmeg.com* ein. Registrieren Sie sich über den Button **Nicht registriert?**. Geben Sie die erforderlichen Daten ein. Nach erfolgter Registrierung erhalten Sie eine E-Mail mit Ihren Anmeldedaten.

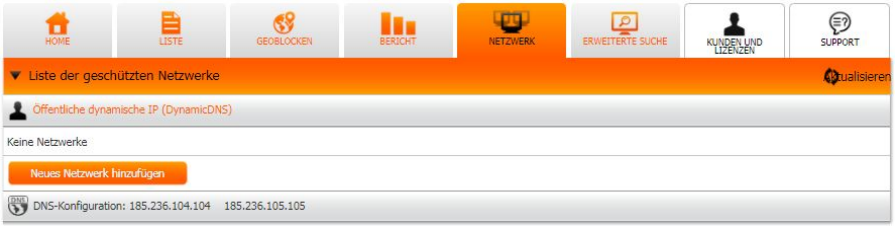
11.3.1 Einrichtung des Webfilters mit dynamischer WAN-IP-Adresse

In den meisten Fällen vergeben Internet Service Provider an sich einwählende Router dynamische öffentliche IP-Adressen. Da die Verknüpfung Ihres Anschlusses mit dem DNS-Server des bintec elmeg Webfilters über diese öffentliche IP-Adresse hergestellt wird, muss diese im DNS-Server hinterlegt werden.

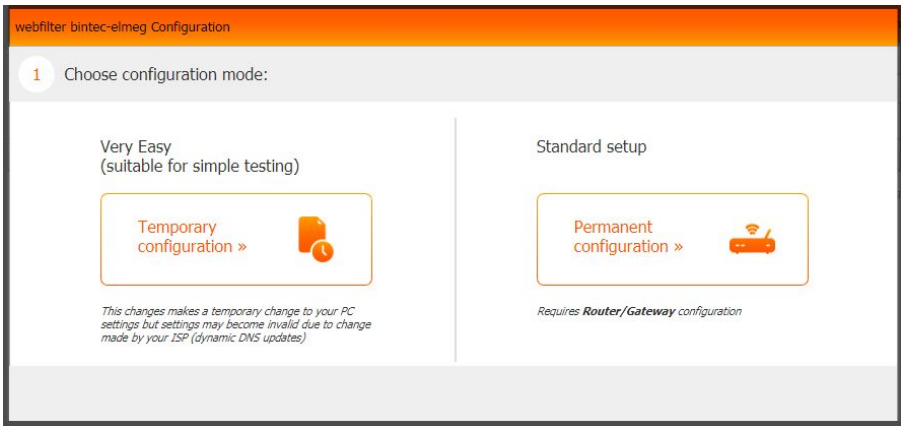
Das Problem hierbei ist, dass sich diese öffentliche IP-Adresse u. a. bei Zwangstrennungen, Neustart des Routers oder administrativer Neueinwahl ändern kann. Um dem bintec elmeg Webfilter-Server die aktuell verwendete IP-Adresse bekannt zu geben, wird ein

DynDNS-Client verwendet.

(1) Nachdem Sie sich am Portal angemeldet haben, gehen Sie in das Menü **Netzwerk Neues Netzwerk hinzufügen**.



(2) Wählen Sie im ersten Schritt die Option **Permanent configuration**.

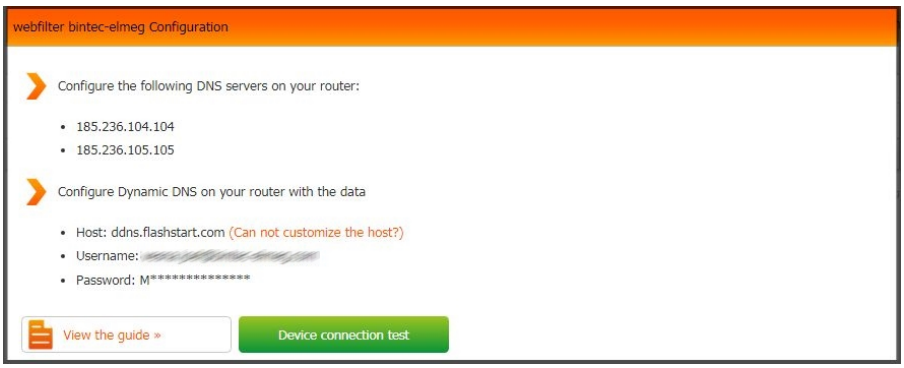


(3) Klicken Sie auf **Can not find your device? Switch to manual configuration**.

(4) Markieren Sie die Option **I have a Dynamic IP**.

(5) Im darauffolgenden Fenster können Sie eingeben welches Gerät Sie verwenden.

(6) Die Einrichtung des Webfilters mit dynamischer WAN-IP-Adresse ist damit abgeschlossen. Klicken Sie auf **Device connection test** um den Geräteverbindungstest zu starten.



11.4 Ein zusätzliches Filterprofil einrichten

Ein zusätzliches Filterprofil soll für eine weitere interne Schnittstelle (z. B. Gast-WLAN / vss7-10) mit individuellen Regeln verwendet werden.

11.4.1 Webfilter konfigurieren

Melden Sie sich mit Ihren Anmeldedaten am bintec elmeg Webfilter an (siehe *Einrichtung des Webfilters* auf Seite 206). Wählen Sie **Profil**->**Neues Profil anlegen** auf der Benutzeroberfläche des Webfilters aus (siehe *Webfilter Benutzeroberfläche* auf Seite 216) .

Abb. 187: **Profil**->**Neues Profil anlegen**

Gehen Sie folgendermaßen vor:

(1) Geben Sie einen **Namen** für das Profil ein, hier z. B. `GastWLAN`.

(2) Wählen Sie alternative IP-Adressen für den **DNS-Server** aus, hier z. B. `185.236.104.114 - 185.236.105.115`.

(3) Klicken Sie auf **Einfügen**.

(4) Klicken Sie auf die Registerkarte **Netzwerk**.

In der Übersicht **Liste der geschützten Netzwerke** sind nun die beiden Profile an invidiuelle DNS-Server gebunden.

Abb. 188: **Liste der geschützten Netzwerke**

Im nächsten Schritt legen Sie neue Regeln für die zusätzliche Client-Schnittstelle fest.

11.4.2 Router konfigurieren

Gehen Sie auf der Benutzeroberfläche der be.IP in das Menü **Firewall**->**Richtlinien**->**IPv4-Filterregeln**->**Neu**.

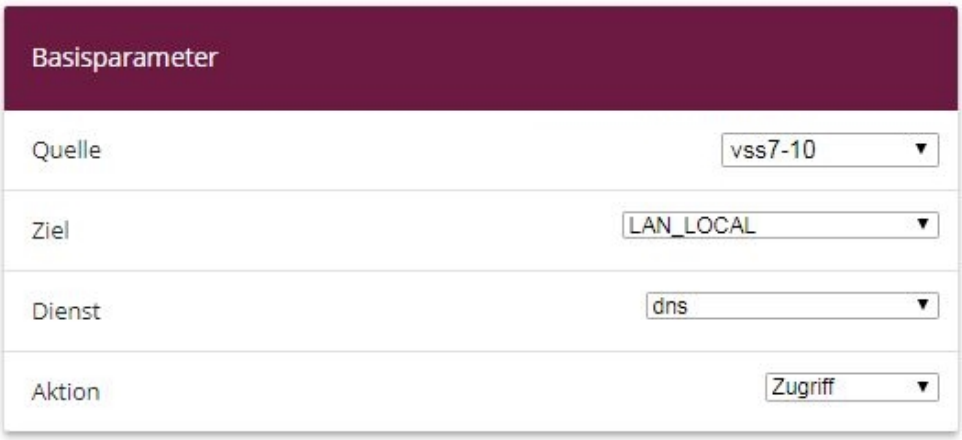


Abb. 189: **Firewall**->**Richtlinien**->**IPv4-Filterregeln**->**Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie als **Quelle** die interne Schnittstelle *vss7-10* aus.

(2) Als **Ziel** wählen Sie *LAN_LOCAL* aus.

(3) Wählen Sie als **Dienst** *dns*.

(4) Wählen Sie bei **Aktion** *Zugriff*.

(5) Bestätigen Sie Ihre Einstellungen mit **OK**.

Konfigurieren Sie nun eine Regel, die Anfragen an andere DNS-Server abweist.

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

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Quelle** die interne Schnittstelle *vss7-10* aus.

(2) Als **Ziel** wählen Sie eine Internetschnittstelle, z. B. *WAN_GERMANY-TELEKOM ENTERTAIN* aus.

(3) Wählen Sie bei **Dienst** *dns*.

(4) Wählen Sie bei **Aktion** *Verweigern*.

(5) Bestätigen Sie Ihre Einstellungen mit **OK**.

Ergebnis:

Abb. 190: **Firewall**->**Richtlinien**->**IPv4-Filterregeln**

Erstellen Sie weitere Firewallregeln, wenn IPv6 auf der zusätzlichen Schnittstelle aktiv ist.

Gehen Sie in das Menü **Firewall**->**Richtlinien**->**IPv6-Filterregeln**->**Neu**.

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Quelle** die interne Internetschnittstelle *vss7-10* aus.

(2) Als **Ziel** wählen Sie *LAN_LOCAL* aus.

(3) Wählen Sie bei **Dienst** *dns*.

(4) Wählen Sie bei **Aktion** *Zugriff*.

(5) Bestätigen Sie Ihre Einstellungen mit **OK**.

Konfigurieren Sie nun eine Regel, die Anfragen an andere DNS-Server abweist.

Gehen Sie in das Menü **Firewall**->**Richtlinien**->**IPv6-Filterregeln**->**Neu**.

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Quelle** die interne Internetschnittstelle . *vss7-10* aus.

(2) Als **Ziel** wählen Sie eine Internetschnittstelle, z. B *WAN_GERMANY-TELEKOM ENTERTAIN* aus.

(3) Wählen Sie bei **Dienst** *dns*.

(4) Wählen Sie bei **Aktion** *Verweigern*.

(5) Bestätigen Sie Ihre Einstellungen mit **OK**.

Im letzten Schritt legen Sie eine neue Domänenweiterleitung für die zusätzliche Client-Schnittstelle fest.

Gehen Sie dazu in das Menü **Lokale Dienste**->**DNS**->**Domänenweiterleitung**->**Neu**.

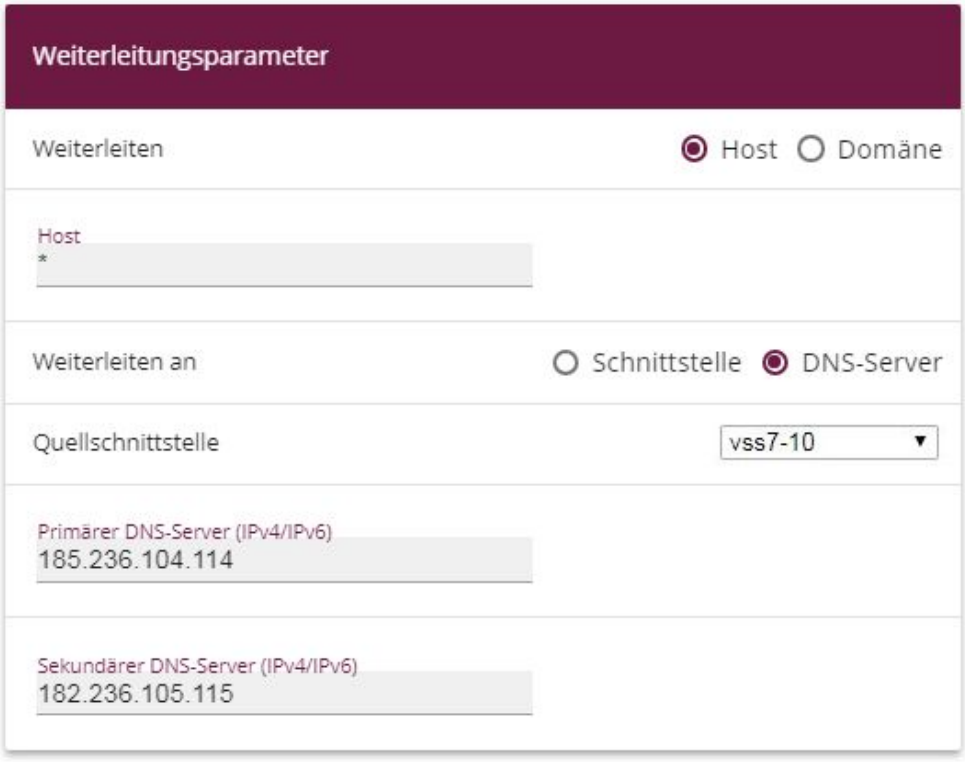


Abb. 191: **Lokale Dienste**->**DNS**->**Domänenweiterleitung**->**Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Weiterleiten** *Host* aus.

(2) Bei **Host** geben Sie *** ein.

(3) Wählen Sie bei **Weiterleiten an** *DNS-Server* aus.

(4) Legen Sie die **Quellschnittstelle** der DNS-Anfragen fest, hier *vss7-10*.

(5) Geben Sie die **IPv4/IPv6-Adresse des primären DNS-Servers** ein, hier *185.236.104.114*.

(6) Geben Sie die **IPv4/IPv6-Adresse des sekundären DNS-Servers** ein, hier *182.236.105.115*.

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

Ergebnis:

Abb. 192: **Lokale Dienste->DNS->Domänenweiterleitung**

Damit ist die Konfiguration eines zusätzlichen Filterprofils abgeschlossen.

11.5 Konfigurationsschritte im Überblick

Webfilter-Konfiguration

Feld	Menü	Wert
Webfilter aktivieren	**Assistenten ->Webfilter**	Aktiviert
LAN-Schnittstelle	**Assistenten ->Webfilter**	z. B. *BRIDGE_BR0*
IP-Adressbereich der gefilterten Clients	**Assistenten ->Webfilter**	z. B. *192.168.0.10* - *192.168.0.30*
Benutzername	**Assistenten ->Webfilter**	z. B. *user.name@company.net* (Zugangsdaten vom Provider)
Passwort	**Assistenten ->Webfilter**	Passwort (Zugangsdaten vom Provider)
Filtermodus	**Assistenten ->Webfilter**	*Standard*

Zusätzliches Filterprofil einrichten (Webfilter)

Feld	Menü	Wert
Name	**Neues Profil anlegen**	z. B. *GastWLAN*
DNS	**Neues Profil anlegen**	z. B. *185.236.104.114* - *185.236.105.115*

Zusätzliches Filterprofil einrichten (be.IP)

Feld	Menü	Wert
Quelle	**Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu**	z. B. *vss7-10*
Ziel	**Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu**	z. B. *LAN_LOCAL*
Dienst	**Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu**	*dns*
Aktion	**Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu**	*Zugriff*
Quelle	**Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu**	z. B. *vss7-10*
Ziel	**Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu**	z. B. *WAN_GERMANY - TELEKOM ENTERTAIN*
Dienst	**Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu**	*dns*
Aktion	**Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu**	*Verweigern*
Quelle	**Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu**	z. B. *vss7-10* (optional)
Ziel	**Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu**	z. B. *LAN_LOCAL* (optional)
Dienst	**Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu**	*dns* (optional)
Aktion	**Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu**	*Zugriff* (optional)
Quelle	**Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu**	z. B. *vss7-10* (optional)
Ziel	**Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu**	z. B. *WAN_GERMANY - TELEKOM ENTERTAIN* (optional)
Dienst	**Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu**	*dns* (optional)
Aktion	**Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu**	*Verweigern* (optional)
Weiterleiten	**Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu**	*Host*

Feld	Menü	Wert
Host	**Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu**	***
Weiterleiten an	**Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu**	*DNS-Server*
Quellschnittstelle	**Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu**	*vss7-10*
Primär DNS-Server (IPv4/IPv6)	**Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu**	*185.236.104.114*
Sekundär DNS-Server (IPv4/IPv6)	**Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu**	*182.236.105.115*

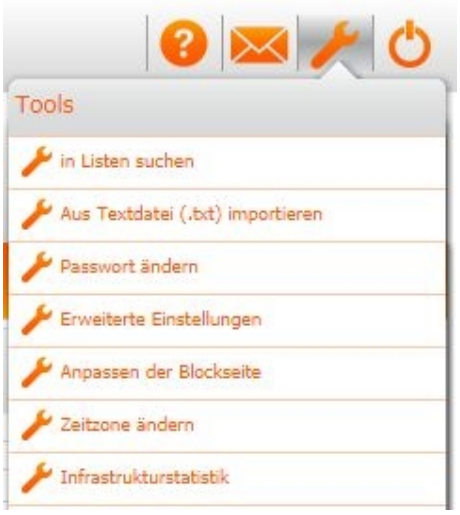
Kapitel 12 Webfilter Benutzeroberfläche

Mit der grafischen Benutzeroberfläche des Webfilters können Sie Netzwerke und Profile verwalten, den Zugriff auf unerwünschte Webseiten unterbinden sowie Sperrlisten zu bestimmten Zeiten aktivieren bzw. deaktivieren.

Übersicht Kopfzeile

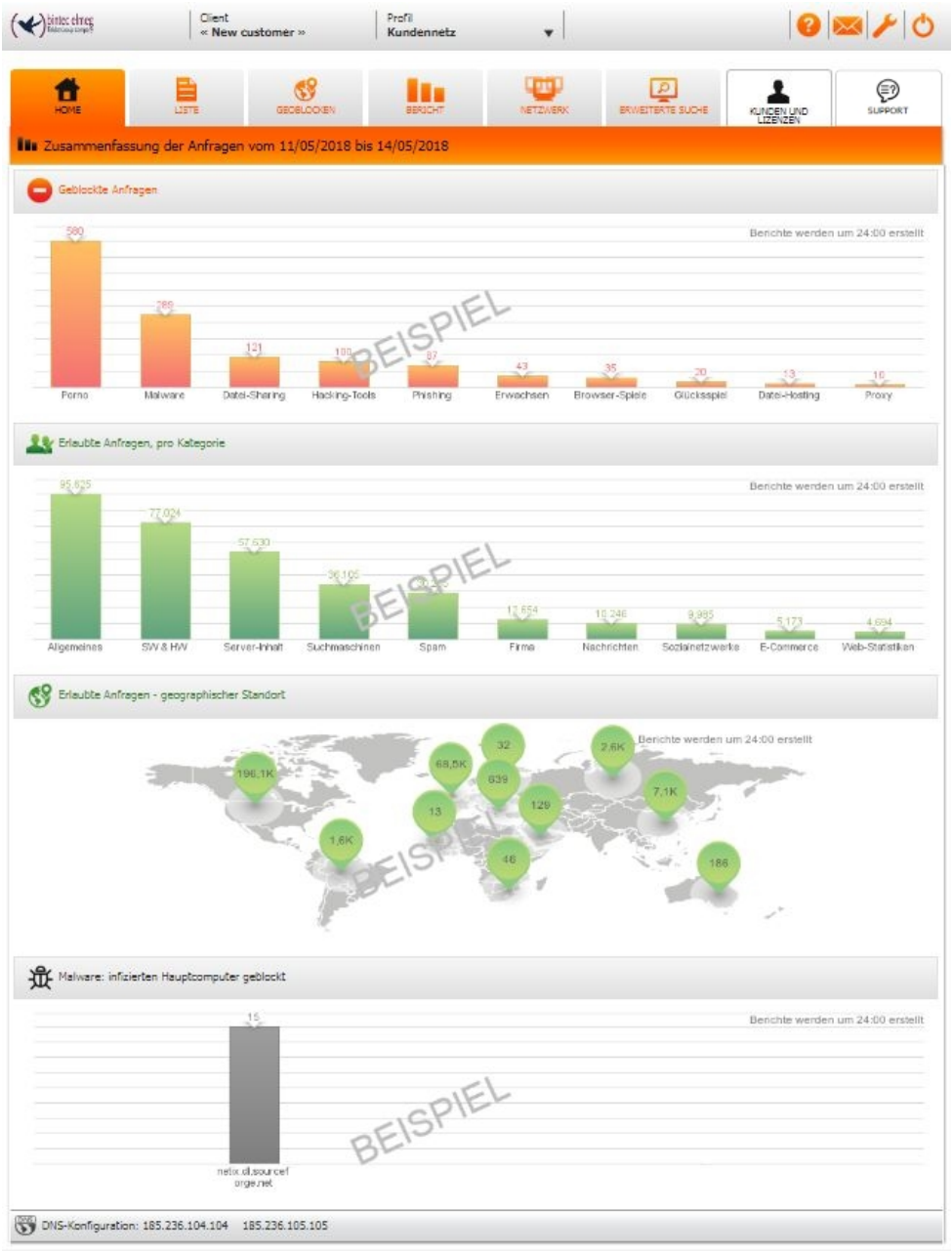
Über das Symbol können Sie die Online-Hilfe abrufen, mit die Freigabeanfragen ansehen und verwalten.

Mit öffnen Sie eine Liste mit verschiedenen Tools.



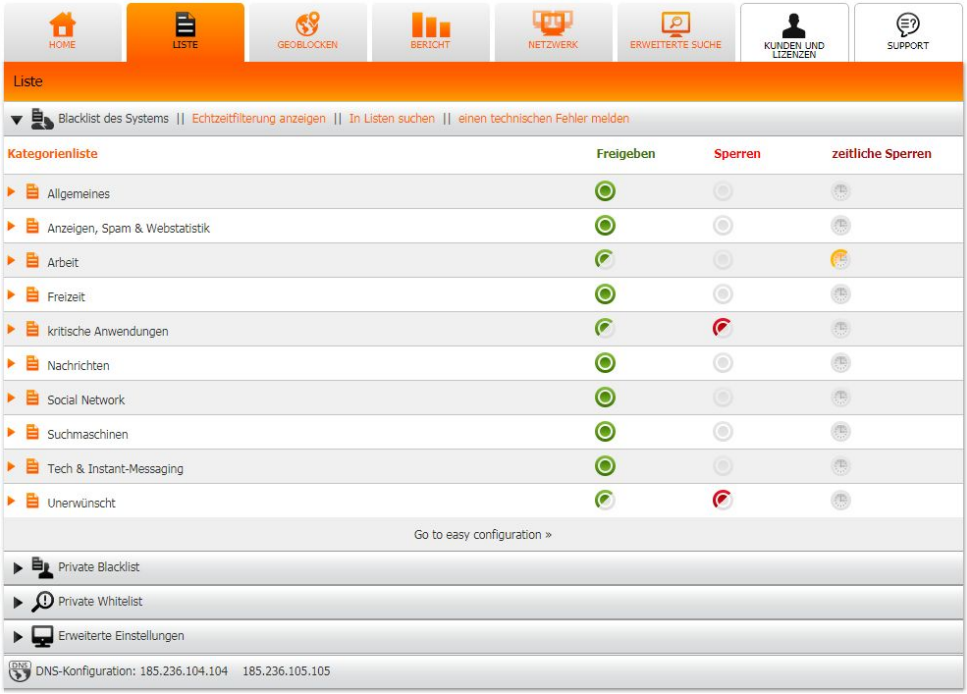
Home

In der Übersicht **Home** sehen Sie in einer grafischen Darstellung die Zusammenfassung der geblockten Anfragen sowie eine grafische und eine geographische Darstellung der erlaubten Anfragen.



Liste

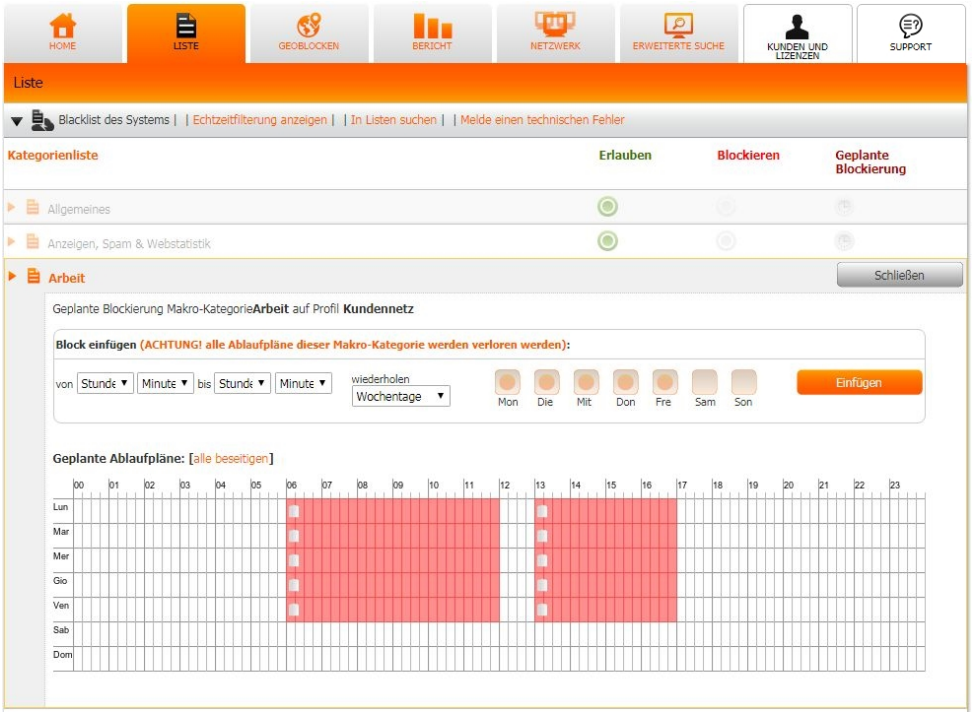
In der Übersicht **Liste** können Sie die Kategorienliste bearbeiten.



Hier können Sie Kategorien erlauben oder blockieren . In einer Kategorienliste können Sie die Unterkategorien auch einzeln erlauben oder blockieren .

Ebenso können Sie hier eine geplante Blockierung konfigurieren. Wählen Sie dazu eine Kategorie aus und klicken Sie auf das Zeichen in der Spalte **Geplante Blockierung**.

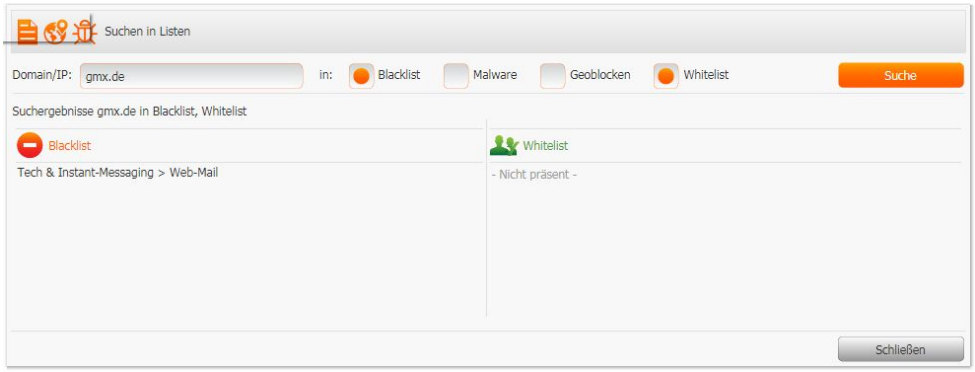
Wählen Sie die Zeit (Stunde und Minute) und den Wochentag für die geplante Blockierung aus.



Unter **Private Whitelist** können Sie einzelne Seiten aus einer gesperrten Kategorie erlauben. Analog dazu können Sie in unter **Private Blacklist** einzelne Seiten aus einer erlaubten Kategorie sperren.

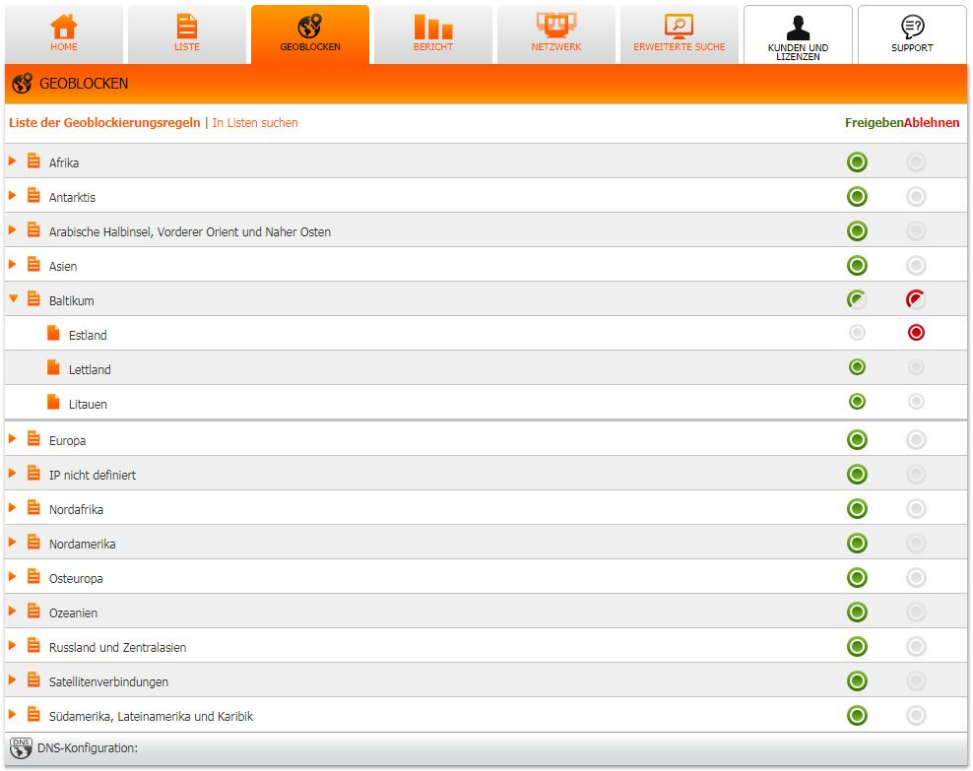
Mit einem Klick auf **Echtzeitfilterung anzeigen** wird angezeigt, welche Kategorien Ihr Webfilter gerade blockiert.

Mit der Option **In Listen suchen** können Sie nach einer bestimmten Domain oder IP-Adresse suchen.



Übersicht Geoblocken

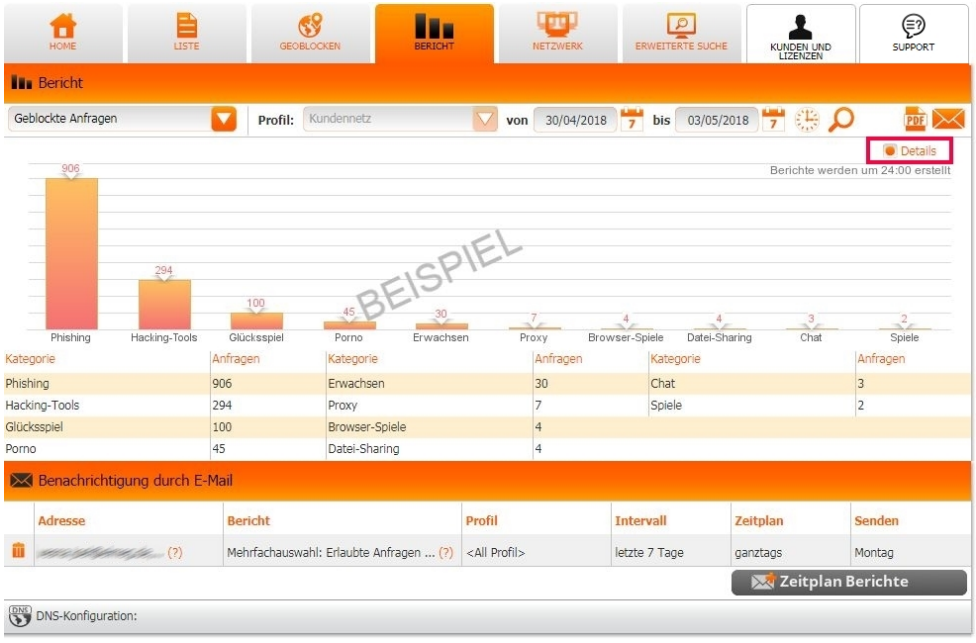
In der Übersicht **Geoblocken** können Sie Länder oder Landbereiche sperren. Klicken Sie dazu in der Spalte **Ablehnen** auf das Symbol .



Übersicht Bericht

In der Übersicht **Bericht** können Sie aus der Liste eine Kategorie, das Profil und einen Zeitraum auswählen und anzeigen lassen (z. B. in welcher Kategorie die Mitarbeiter zu einer bestimmten Zeit im Internet gesurft haben). Aktivieren Sie **Details**, um den Bericht zusätzlich in Listenform anzeigen zu lassen.

Mit können Sie für die Suchberichte einen Zeitplan erstellen und mit die Berichte nach Datum durchsuchen. Außerdem können Sie den Bericht als PDF erstellen oder per E-Mail verschicken.



Netzwerke

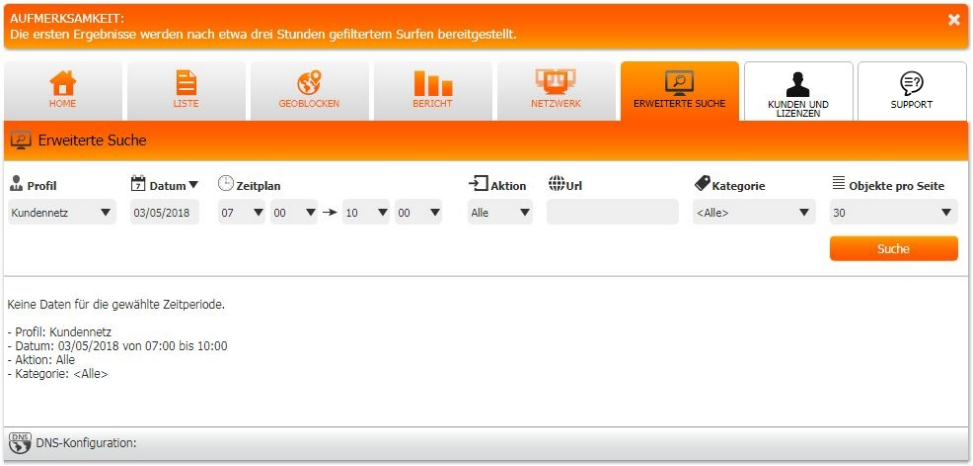
Im Bereich Netzwerk werden die konfigurierten Netzwerke angezeigt. Mit **Neues Netzwerk hinzufügen** fügen Sie ein neues Netzwerk hinzu.

Hinweis

Für jede weitere WAN IP-Adresse, die Sie hinzufügen möchten, benötigen Sie eine Lizenz. Jede Lizenz gilt nur für eine bestimmte WAN IP-Adresse.

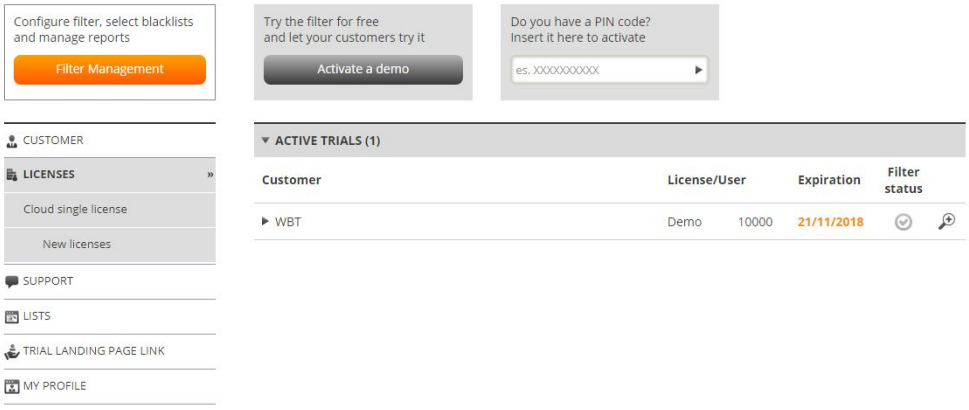
Erweiterte Suche

In **Erweiterte Suche** können Sie Profile nach Datum, Uhrzeit und nach Kategorie filtern.



Kunden und Lizenzen

Über **Kunden und Lizenzen** können Sie einen weiteren Kunden anlegen.



Unterstützung

Über das Menü **Support** gelangen Sie zu der Hilfeseite.