



Benutzerhandbuch Workshops (Auszug)

Sicherheits- und Administrations-Workshops

Copyright© Version 08/2020 bintec elmeg GmbH

Rechtlicher Hinweis

Gewährleistung

Änderungen in dieser Veröffentlichung sind vorbehalten.

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

Copyright © bintec elmeg GmbH

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

Inhaltsverzeichnis

Kapitel 1	Sicherheit - IPSec mit Zertifikaten	1
1.1	Einleitung	1
1.2	Konfiguration.	1
1.2.1	IPSec-Peer erstellen	2
1.2.2	Anpassen des Phase-1-Profiles	3
1.2.3	Anpassen des Phase-2-Profiles	5
1.2.4	DynDNS konfigurieren.	7
1.2.5	Zertifikate anfordern und importieren	8
1.2.6	IPSec-Verbindung anpassen	11
1.3	Ergebnis	13
1.4	Kontrolle.	13
1.5	Konfigurationsschritte im Überblick	14
Kapitel 2	Sicherheit - IPSec mit dynamischen IP-Adressen und DynDNS.	18
2.1	Einleitung	18
2.2	Konfiguration	19
2.2.1	Konfiguration am ersten Router (Standort A)	19
2.2.2	Konfiguration am zweiten Router (Standort B)	25
2.3	Kontrolle	32
2.4	Konfigurationsschritte im Überblick	33
Kapitel 3	Sicherheit - Bridging über eine IPSec-Verbindung	38
3.1	Einleitung	38
3.2	Konfiguration am Standort A (bintec be.IP_plus-1)	39

3.3	Konfiguration am Standort B (bintec be.IP_plus-2)	46
3.4	Konfigurationsschritte im Überblick	53
Kapitel 4	Sicherheit - Stateful Inspection Firewall (SIF)	58
4.1	Einleitung	58
4.2	Konfiguration der Firewall	59
4.2.1	Konfiguration der Aliasnamen für IP-Adressen und Netzadresse	59
4.2.2	Konfiguration von Dienstgruppen	63
4.2.3	Konfiguration der Filterregeln	65
4.3	Ergebnis	67
4.4	Überprüfen der Konfiguration	67
4.5	Konfigurationsschritte im Überblick	69
Kapitel 5	Sicherheit - VPN-Anbindung über einen SMS PASSCODE-Server	72
5.1	Einleitung	72
5.2	Konfiguration	73
5.2.1	Hinweise während der Installation und Konfiguration des SMS PASSCODE-Servers	73
5.2.2	Vorbereitungen zur Installation des SMS PASSCODE-Servers	73
5.2.3	Installation des SMS PASSCODE-Servers	73
5.2.4	Konfiguration des Web-Administration-Tools	74
5.2.5	Konfiguration des RADIUS-Server zur Anbindung des VPN-Gateways	76
5.2.6	Konfiguration des VPN-Gateways	77
5.2.7	Konfiguration des bintec Secure IPSec Clients	82
5.3	Test der VPN-Verbindung / Debug-Meldungen des VPN-Gateways	87
5.4	Konfigurationsschritte im Überblick	90
Kapitel 6	Sicherheit - bintec elmeg Webfilter	92

6.1	Einleitung	92
6.2	Webfilter-Assistent	94
6.2.1	Konfiguration auf dem Router	95
6.3	Einrichtung des Webfilters	97
6.3.1	Einrichtung des Webfilters mit dynamischer WAN-IP-Adresse	97
6.4	Ein zusätzliches Filterprofil einrichten	99
6.4.1	Webfilter konfigurieren	100
6.4.2	Router konfigurieren	101
6.5	Konfigurationsschritte im Überblick	104
Kapitel 7	Webfilter Benutzeroberfläche	107
Kapitel 8	Sicherheit - Webfilter mit zwei Internetzugängen	115
8.1	Neues Netzwerk einrichten.	115
8.2	Profile dem neuen Netzwerk zuordnen	119
8.3	Neuen DynDNS-Provider anlegen	120
8.4	Statische Routen zum DynDNS-Server anlegen	124
8.5	Neuen DynDNS-Client anlegen.	126
8.6	DNS Domänenweiterleitung einrichten.	129
8.7	Firewall - Schnittstellengruppe anlegen	130
8.8	Firewall-Regeln anlegen.	132
8.9	Konfigurationsschritte im Überblick	133

Kapitel 1 Sicherheit - IPSec mit Zertifikaten

1.1 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.

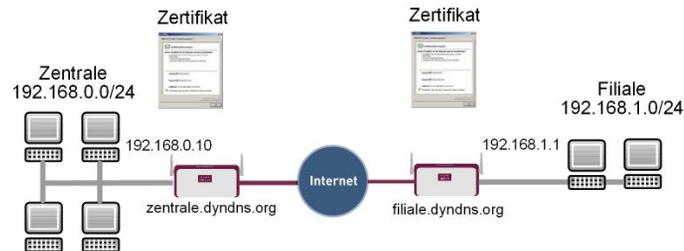


Abb. 1: Beispielszenario IPSec mit Zertifikaten

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.

1.2 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.

1.2.1 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**.

The screenshot shows two configuration panels for an IPSec peer:

- Peer-Parameter:**
 - Administrativer Status: Aktiv Inaktiv
 - Beschreibung:
 - Peer-Adresse: IP-Version ;
 - Peer-ID: ;
 - IKE (Internet Key Exchange):
 - Preshared Key:
 - IP-Version des Tunnelnetzwerks:
- IPv4-Schnittstellenrouten:**
 - Sicherheitsrichtlinie: Nicht Vertrauenswürdig Vertrauenswürdig
 - IPv4-Adressvergabe:
 - Standardroute: Deaktiviert
 - Lokale IP-Adresse:
 - Routeneinträge:

Entfernte IP-Adresse	Netzmaske	Metrik
<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="1"/>
 - HINZUFÜGEN

Abb. 2: 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.

1.2.2 Anpassen des Phase-1-Profiles

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 ▼	<input type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>
Blowfish ▼	MD5 ▼	<input checked="" type="checkbox"/>

DH-Gruppe 2(1024 Bit) ▼

Lebensdauer Sekunden kBytes

Authentifizierungsmethode Preshared Keys ▼

Modus Main Modus (ID Protect) Aggressiv Strikt

Lokaler ID-Typ Fully Qualified Domain Name (FQDN) ▼

Lokaler ID-Wert
zentrale

Erweiterte Einstellungen

Erweiterte Einstellung

Erreichbarkeitsprüfung	Inaktiv ▼
Blockzeit 30	Sekunden
NAT-Traversal	Aktiviert ▼

Abb. 4: VPN -> IPSec -> Phase-1-Profil -> <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**.

1.2.3 Anpassen des Phase-2-Profiles

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

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

Phase-2-Parameter (IPSEC)

Beschreibung
Filiale

Proposals

Verschlüsselung	Authentifizierung	Aktiviert
AES-128 ▼	SHA1 ▼	<input type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>

PFS-Gruppe verwenden

Aktiviert
2(1024 Bit) ▼

Lebensdauer

7200 Sekunden 0 kBytes Schlüssel erneut

erstellen nach 80 % Lebensdauer

Erweiterte Einstellungen

Erweiterte Einstellung	
IP-Komprimierung	<input type="checkbox"/> Deaktiviert
Erreichbarkeitsprüfung	Inaktiv
PMTU propagieren	<input checked="" type="checkbox"/> Aktiviert

Abb. 6: VPN -> IPSec -> Phase-2-Profil -> <Multi-Proposal> -> ✎

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

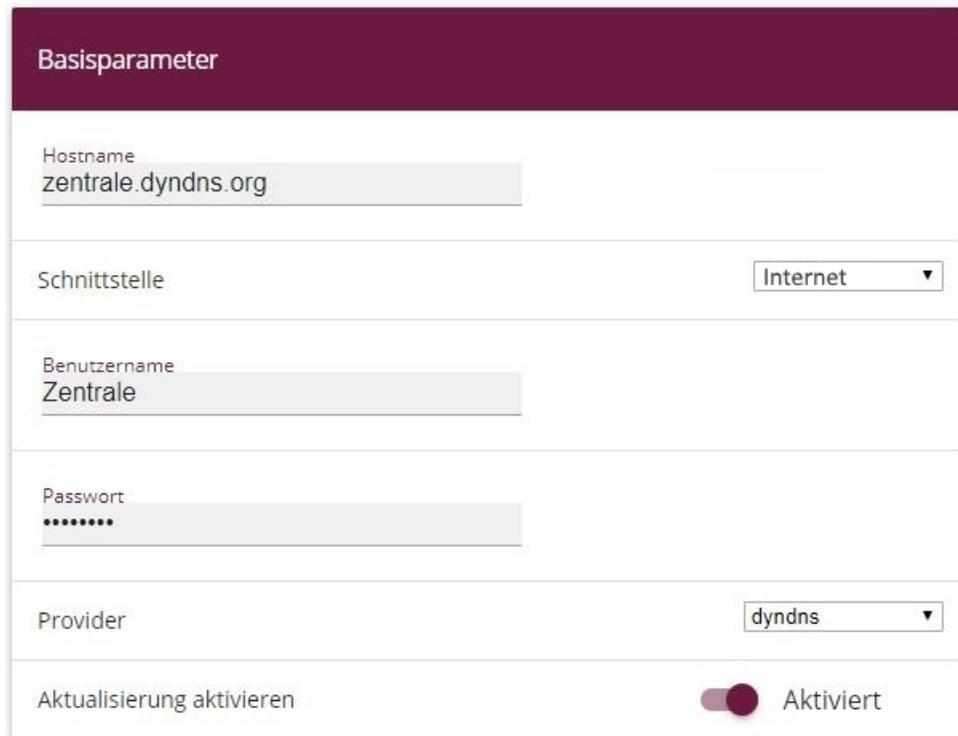
- (1) Bei **Beschreibung** geben Sie einen Namen für das Profil ein, z. B. *Filiale* .
- (2) Wählen Sie bei **Proposals Verschlüsselung** *AES-128*, bei **Authentifizierung** *MD5*.
Da immer mindestens ein Proposal konfiguriert sein muss, ist der erste Eintrag der Liste standardmäßig aktiviert.
- (3) Klicken Sie auf **Erweiterte Einstellungen**.
- (4) **Erreichbarkeitsprüfung** setzen Sie auf *Inaktiv*.
- (5) Bestätigen Sie mit **OK**.

1.2.4 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**.



The screenshot shows a configuration window titled 'Basisparameter' with a dark red header. It contains several input fields and dropdown menus:

- Hostname:** zentrale.dyndns.org
- Schnittstelle:** Internet (dropdown menu)
- Benutzername:** Zentrale
- Passwort:** [Redacted with dots]
- Provider:** dyndns (dropdown menu)
- Aktualisierung aktivieren:** A toggle switch is turned on, labeled 'Aktiviert'.

Abb. 7: 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. *password* 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.

1.2.5 Zertifikate anfordern und importieren

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

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

Abb. 8: **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**.

Zertifikate				
Beschreibung	Subjektname	Typ	Verwendet	Status
Zentrale	CN=Zentrale.	Manuelle Registrierung		Wird ausgeführt

Abb. 9: 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:

Parameter bearbeiten	Details anzeigen				
<table border="1"> <thead> <tr> <th>Beschreibung</th> <th>Zentrale</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Beschreibung	Zentrale			<pre> Certificate Request = SerialNumber = 0 SubjectName = (CN=Zentrale) Signature algorithm = rsa-pkcs1-md5 PublicKeyInfo = Algorithm name (X.509) : rsaEncryption Modulus n (1024 bits) : 157325460928857022853826636132139025432934977768397189050563769368461999 9180857930271379168562084188865727733210892368690142921504560511005643372 228761888435828253917266522732058173685486783181075031069316033321187963 3744008961617951094769878796101397524110110767020532237032646871566036561 140935003389318692079 Exponent e (17 bits) : 65537 Extensions = Available = subject alternative names SubjectAlternativeNames = </pre>
Beschreibung	Zentrale				

Abb. 10: 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**.

Importieren

Externer Dateiname Zentrale.crt

Lokale Zertifikatsbeschreibung
Zentrale

Dateikodierung

Passwort

Abb. 11: 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**.

1.2.6 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> ->** .

Phase-1-Parameter (IKE)

Beschreibung
Filiale

Proposals

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

DH-Gruppe 2(1024 Bit)

Lebensdauer 14400 Sekunden 0 kBytes

Authentifizierungsmethode RSA-Signatur

Lokales Zertifikat Zentrale

Modus Main Modus (ID Protect) Aggressiv Strikt

Lokaler ID-Wert Subjektnamen aus Zertifikat verwenden

Abb. 12: VPN -> IPSec -> Phase-1 -Profile -> <Filiale> -> 

Gehen Sie folgendermaßen vor, um den Eintrag zu verändern:

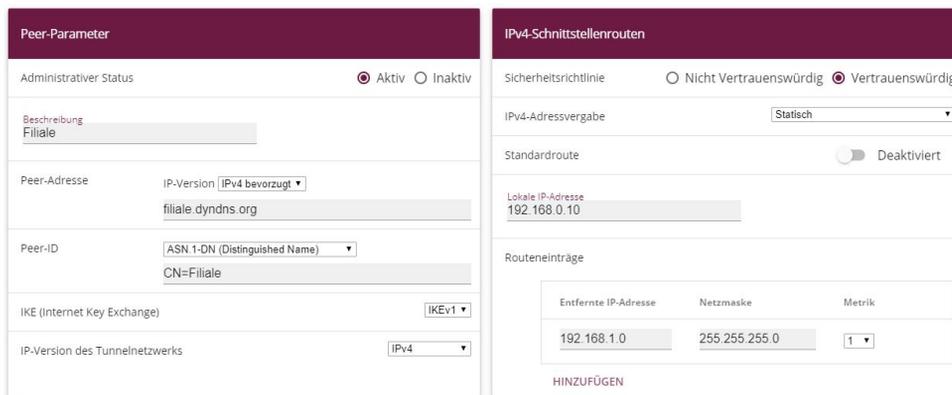
- (1) Unter **Authentifizierungsmethode** wählen Sie *RSA-Signatur*.
- (2) Als **Lokales Zertifikat** wählen Sie das eigene Zertifikat aus, hier *Zentrale*.
- (3) Den **Modus** stellen Sie auf *Main Modus (ID Protect)*.
- (4) Unter **Lokaler ID-Wert** setzen Sie den Haken auf *Subjektnamen aus Zertifikat verwenden*

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> ->** .



The screenshot shows two configuration panels. The left panel, titled 'Peer-Parameter', includes fields for 'Administrativer Status' (Aktiv selected), 'Beschreibung Filiale', 'Peer-Adresse' (IP-Version: IPv4 bevorzugt, filiale.dyndns.org), 'Peer-ID' (ASN 1-DN (Distinguished Name), CN=Filiale), 'IKE (Internet Key Exchange)' (IKEv1 selected), and 'IP-Version des Tunnelnetzwerks' (IPv4 selected). The right panel, titled 'IPv4-Schnittstellenrouten', includes 'Sicherheitsrichtlinie' (Vertrauenswürdig selected), 'IPv4-Adressvergabe' (Statisch selected), 'Standardroute' (Deaktiviert), 'Lokale IP-Adresse' (192.168.0.10), and a table for 'Routeneinträge' with columns for 'Entfernte IP-Adresse', 'Netzmaske', and 'Metrik'. The table contains one entry: 192.168.1.0, 255.255.255.0, 1. A 'HINZUFÜGEN' button is at the bottom.

Abb. 13: **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**.

1.3 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.

1.4 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:

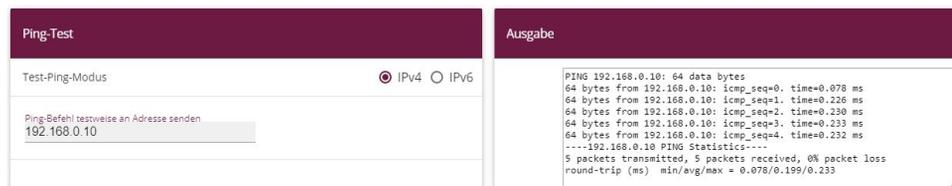


Abb. 14: Wartung -> Diagnose -> Ping-Test



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.

1.5 Konfigurationsschritte im Überblick

IPSec-Peer anlegen

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

Phase-1-Profil anpassen

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

Phase-2-Profile anpassen

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

DynDNS

Feld	Menü	Wert
Hostname	Lokale Dienste -> DynDNS-	z. B. <i>zentra-</i>

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

Zertifikate anfordern und importieren

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

IPSec-Verbindung anpassen

Feld	Menü	Wert
Authentifizierungsmethode	VPN -> IPSec -> Phase-	<i>RSA-Signatur</i>

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 2 Sicherheit - IPSec mit dynamischen IP-Adressen und DynDNS

2.1 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.

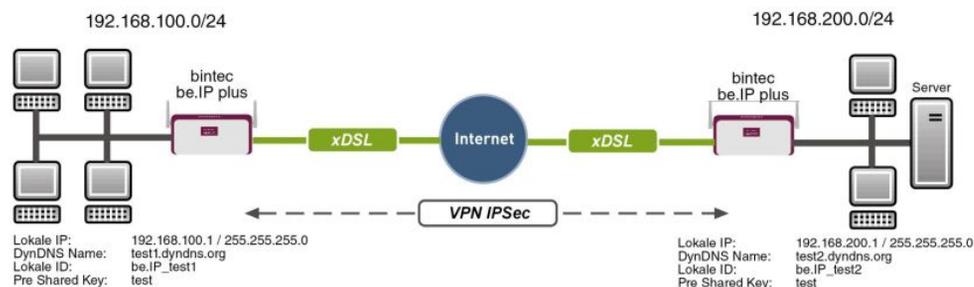


Abb. 15: Beispielszenario

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

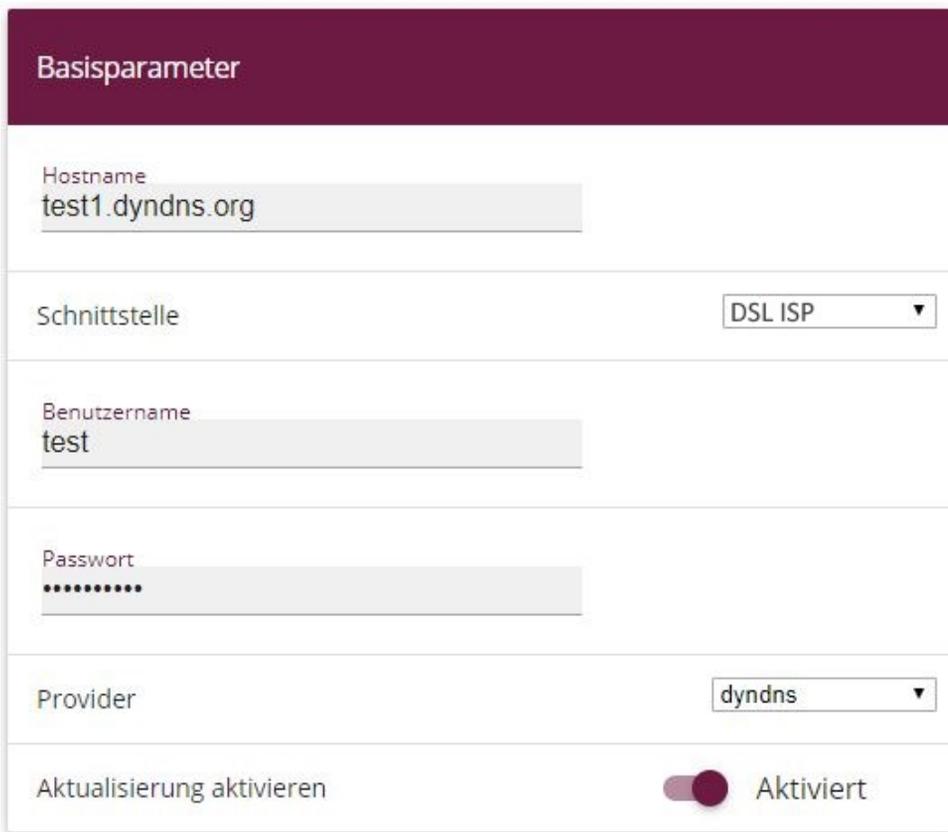
2.2 Konfiguration

2.2.1 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**.



The screenshot shows a configuration form titled "Basisparameter" with the following fields:

- Hostname: test1.dyndns.org
- Schnittstelle: DSL ISP (dropdown menu)
- Benutzername: test
- Passwort: [masked with dots]
- Provider: dyndns (dropdown menu)
- Aktualisierung aktivieren: [toggle switch] Aktiviert

Abb. 16: 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 neuen IPSec-Peer einzurichten.

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

The screenshot displays two configuration panels for an IPSec peer. The left panel, titled "Peer-Parameter", includes fields for "Administrativer Status" (set to "Aktiv"), "Beschreibung" (filled with "be_IP_test2"), "Peer-Adresse" (with "test2.dyndns.org" and "IP-Version" set to "IPv4 bevorzugt"), "Peer-ID" (with "Fully Qualified Domain Name (FQDN)" and "be_IP_test2"), "IKE (Internet Key Exchange)" (set to "IKEv1"), "Preshared Key" (masked with asterisks), and "IP-Version des Tunnelnetzwerks" (set to "IPv4"). The right panel, titled "IPv4-Schnittstellenrouten", includes "Sicherheitsrichtlinie" (set to "Vertrauenswürdig"), "IPv4-Adressvergabe" (set to "Statisch"), "Standardroute" (set to "Deaktiviert"), "Lokale IP-Adresse" (filled with "192.168.100.1"), and a "Routeneinträge" table with columns for "Entfernte IP-Adresse", "Netzmaske", and "Metrik". The table contains one entry: "192.168.200.0", "255.255.255.0", and "1". A "HINZUFÜGEN" button is located below the table.

Abb. 17: 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 vorhandenen 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
autogenerated

Proposals

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

DH-Gruppe 2(1024 Bit) ▼

Lebensdauer Sekunden kBytes

Authentifizierungsmethode Preshared Keys ▼

Modus
 Main Modus (ID Protect) Aggressiv Strikt

Lokaler ID-Typ Fully Qualified Domain Name (FQDN) ▼

Lokaler ID-Wert

Erweiterte Einstellungen

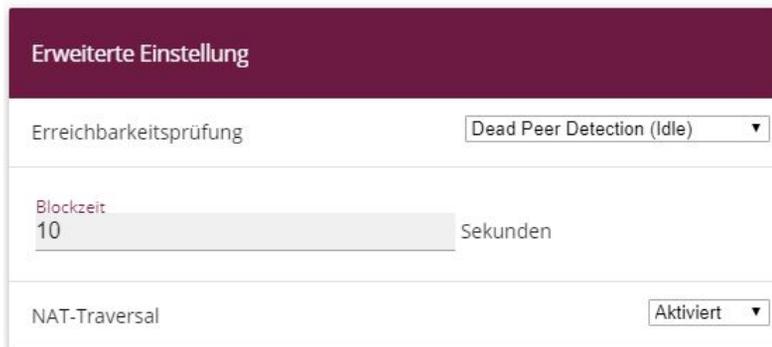


Abb. 19: VPN -> IPsec -> Phase-1-Profil -> Neu

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* KBytes 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-Profil

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-Profil** -> **Neu**.

Phase-2-Parameter (IPSEC)

Beschreibung
autogenerated

Proposals

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

PFS-Gruppe verwenden Aktiviert
2(1024 Bit) ▼

Lebensdauer

900 Sekunden 0 kBytes Schlüssel erneuert

erstellen nach 80 % Lebensdauer

Erweiterte Einstellungen

Erweiterte Einstellung	
IP-Komprimierung	<input type="checkbox"/> Deaktiviert
Erreichbarkeitsprüfung	Heartbeats (Senden & Erwarten) ▼
PMTU propagieren	<input checked="" type="checkbox"/> Aktiviert

Abb. 21: VPN -> IPsec -> Phase-2-Profil -> 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* KBytes 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**.

2.2.2 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**.

Basisparameter

Hostname

Schnittstelle

Benutzername

Passwort

Provider

Aktualisierung aktivieren Aktiviert

Abb. 22: 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. 23: **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
autogenerated

Proposals

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

DH-Gruppe 2(1024 Bit) ▼

Lebensdauer Sekunden kBytes

Authentifizierungsmethode Preshared Keys ▼

Modus
 Main Modus (ID Protect) Aggressiv Strikt

Lokaler ID-Typ Fully Qualified Domain Name (FQDN) ▼

Lokaler ID-Wert

Erweiterte Einstellungen

Abb. 25: VPN -> IPSec -> Phase-1-Profil -> 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* KBytes 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-Profil

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

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

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

Phase-2-Parameter (IPSEC)

Beschreibung
autogenerated

Proposals

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

PFS-Gruppe verwenden Aktiviert
2(1024 Bit) ▼

Lebensdauer

900 Sekunden 0 kBytes Schlüssel erneuert

erstellen nach 80 % Lebensdauer

Erweiterte Einstellungen

Erweiterte Einstellung	
IP-Komprimierung	<input type="checkbox"/> Deaktiviert
Erreichbarkeitsprüfung	Heartbeats (Senden & Erwarten) ▾
PMTU propagieren	<input checked="" type="checkbox"/> Aktiviert

Abb. 27: VPN -> IPsec -> Phase-2-Profil -> 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**.

2.3 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**.

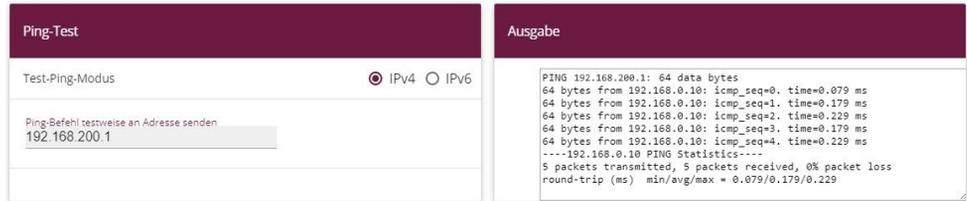


Abb. 28: Wartung -> Diagnose -> Ping-Test

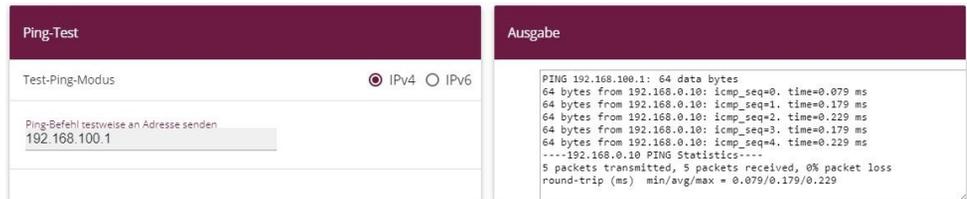


Abb. 29: Wartung -> Diagnose -> Ping-Test

2.4 Konfigurationsschritte im Überblick

DynDNS Account am ersten Router einrichten (Standort A)

Feld	Menü	Wert
Hostname	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	z. B. <i>test1.dyndns.org</i>
Schnittstelle	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	<i>DSL ISP</i>
Benutzername	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	z. B. <i>test</i>
Passwort	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	z. B. <i>test</i>
Provider	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	<i>dyndns</i>
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. <i>be.IP_test2</i>
Peer-Adresse	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. <i>test2.dyndns.org</i>
Peer-ID	VPN -> IPsec -> IPsec-Peers -> Neu	<i>Fully Qualified Domain Name (FQDN) / be.IP_test2</i>
Preshared Key	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. <i>test</i>
IP-Adressenvergabe	VPN -> IPsec -> IPsec-Peers -> Neu	Statisch
Standardroute	VPN -> IPsec -> IPsec-Peers -> Neu	Deaktiviert
Lokale IP-Adresse	VPN -> IPsec -> IPsec-Peers -> Neu	<i>192.168.100.1</i>
Routeneinträge	VPN -> IPsec -> IPsec-Peers -> Neu	<i>192.168.200.0 / 255.255.255.0</i>

IPsec-Konfiguration - Phase-1

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

IPsec-Konfiguration - Phase-2

Feld	Menü	Wert
Beschreibung	VPN -> IPsec -> Phase-2-Profil -> Neu	z. B. <i>*autogenerated*</i>
Proposals	VPN -> IPsec -> Phase-2-Profil -> Neu	<i>Blowfish, MD5</i>
PFS-Gruppe verwenden	VPN -> IPsec -> Phase-2-Profil -> Neu	<i>2 (1024 Bit)</i>
Lebensdauer	VPN -> IPsec -> Phase-2-Profil -> Neu	<i>900 Sekunden, 0 kBytes</i>
IP-Komprimierung	VPN -> IPsec -> Phase-2-Profil -> Neu -> Erweiterte Einstellungen	<i>Deaktiviert</i>
Erreichbarkeitsprüfung	VPN -> IPsec -> Phase-2-Profil -> Neu -> Erweiterte Einstellungen	<i>Heartbeats (Senden & Erwarten)</i>
PMTU propagieren	VPN -> IPsec -> Phase-2-Profil -> 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. <i>test2.dyndns.org</i>
Schnittstelle	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	<i>DSL ISP</i>
Benutzername	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	z. B. <i>test</i>
Passwort	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	z. B. <i>test</i>
Provider	Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu	<i>dyndns</i>
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. <i>be.IP_test1</i>
Peer-Adresse	VPN -> IPsec -> IPsec-Peers -> Neu	z. B. <i>test1.dyndns.org</i>
Peer-ID	VPN -> IPsec -> IPsec-Peers -> Neu	<i>Fully Qualified Domain Name (FQDN)</i>

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

IPSec-Konfiguration - Phase-1

Feld	Menü	Wert
Beschreibung	VPN -> IPSec -> Phase-1-Profile -> Neu	z. B. <i>*autogenerated*</i>
Proposals	VPN -> IPSec -> Phase-1-Profile -> Neu	<i>Blowfish, MD5</i>
DH-Gruppe	VPN -> IPSec -> Phase-1-Profile -> Neu	<i>2 (1024 Bit)</i>
Lebensdauer	VPN -> IPSec -> Phase-1-Profile -> Neu	<i>900 Sekunden, 0 kBytes</i>
Authentifizierungsmethode	VPN -> IPSec -> Phase-1-Profile -> Neu	<i>Preshared Keys</i>
Modus	VPN -> IPSec -> Phase-1-Profile -> Neu	<i>Aggressiv</i>
Lokaler ID-Typ	VPN -> IPSec -> Phase-1-Profile -> Neu	<i>Fully Qualified Domain Name (FQDN)</i>
Lokaler ID-Wert	VPN -> IPSec -> Phase-1-Profile -> Neu	<i>be.IP_test2</i>
Erreichbarkeitsprüfung	VPN -> IPSec -> Phase-1-Profile -> Neu -> Erweiterte Einstellungen	<i>Dead Peer Detection (Idle)</i>
Blockzeit	VPN -> IPSec -> Phase-1-Profile -> Neu -> Erweiterte Einstellungen	<i>10 Sekunden</i>
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. <i>*autogenerated*</i>
Proposals	VPN -> IPSec -> Phase-2-Profile -> Neu	<i>Blowfish, MD5</i>
PFS-Gruppe verwenden	VPN -> IPSec -> Phase-2-Profile -> Neu	<i>2 (1024 Bit)</i>
Lebensdauer	VPN -> IPSec -> Phase-2-Profile -> Neu	<i>900 Sekunden, 0 kBy-</i>

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

Kapitel 3 Sicherheit - Bridging über eine IPSec-Verbindung

3.1 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.

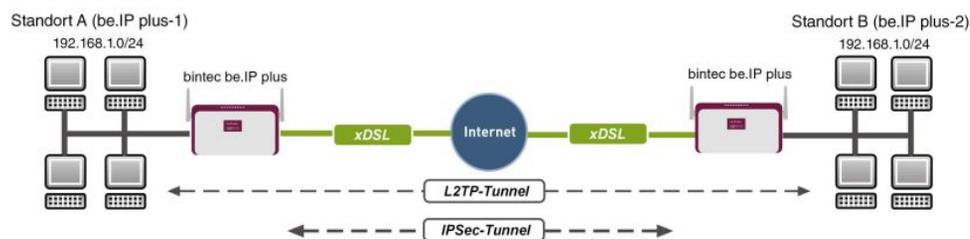


Abb. 30: Beispielszenario

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

3.2 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**.

Wählen Sie das VPN-Szenario aus: ?

VPN-Szenario IPSec - LAN-zu-LAN-Verbindung ▼

Abb. 31: 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.

Ausgewähltes Szenario: LAN-zu-LAN-Verbindung

Verbindungsdetails	IP-Einstellungen eingeben:
Beschreibung IPSec-Peer1	IPSec Peer IPv4-Adresse 10.1.1.4
Lokale IPSec ID be.ip_plus-1	Entferntes IPv4-Netzwerk 1.1.1.2
Entfernte IPSec ID be.ip_plus-2	255.255.255.0
Preshared Key *****	
IP-Version des Tunnelnetzwerks IPv4	
Lokale IP-Adresse 192.168.1.253	
Diese Verbindung als Standardroute definieren <input type="checkbox"/>	Deaktiviert

Abb. 32: 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 -> **.

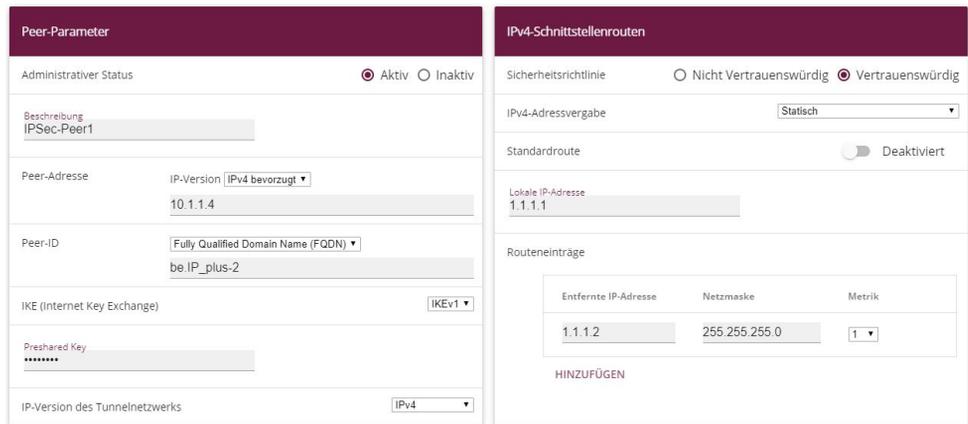


Abb. 33: **VPN -> IPSec -> IPSec-Peers -> **

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**.

Basisparameter	Parameter des LAC-Modus
Beschreibung L2TP-LAC	Entfernte IP-Adresse 1.1.1.2
Lokaler Hostname be.IP_plus-1	UDP-Quellport <input type="checkbox"/> Dynamisch
Entfernter Hostname be.IP_plus-2	UDP-Zielport 1701
Passwort *****	

- (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**.

Basisparameter	IP-Modus und Routen						
Beschreibung L2TP-LAC	IP-Adressmodus <input checked="" type="radio"/> Statisch <input type="radio"/> IP-Adresse abrufen						
Verbindungstyp <input type="radio"/> LNS <input checked="" type="radio"/> LAC	Standardroute <input type="checkbox"/> Deaktiviert						
Tunnelprofil L2TP-LAC	NAT-Eintrag erstellen <input type="checkbox"/>						
Benutzername L2TP-User	Lokale IP-Adresse 1.1.1.3						
Passwort *****	Routeneinträge						
Immer aktiv <input type="checkbox"/> Deaktiviert	<table border="1"> <thead> <tr> <th>Entfernte IP-Adresse</th> <th>Netzmaske</th> <th>Metrik</th> </tr> </thead> <tbody> <tr> <td>1.1.1.4</td> <td>255.255.255.255</td> <td>1</td> </tr> </tbody> </table>	Entfernte IP-Adresse	Netzmaske	Metrik	1.1.1.4	255.255.255.255	1
Entfernte IP-Adresse	Netzmaske	Metrik					
1.1.1.4	255.255.255.255	1					
Timeout bei Inaktivität 300 Sekunden	HINZUFÜGEN						

Erweiterte Einstellungen

Erweiterte Einstellung	IP-Optionen
Blockieren nach Verbindungsfehler für 300 Sekunden	OSPF-Modus <input checked="" type="radio"/> Passiv <input type="radio"/> Aktiv <input type="radio"/> Inaktiv
Authentifizierung MS-CHAPv2	Proxy-ARP-Modus <input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv
Verschlüsselung <input checked="" type="radio"/> Keiner <input type="radio"/> Aktiviert <input type="radio"/> Windows-kompatibel	DNS-Aushandlung <input checked="" type="checkbox"/> Aktiviert
LCP-Erreichbarkeitsprüfung <input checked="" type="checkbox"/> Aktiviert	
TCP-ACK-Pakete priorisieren <input type="checkbox"/> Deaktiviert	

Abb. 37: 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**.

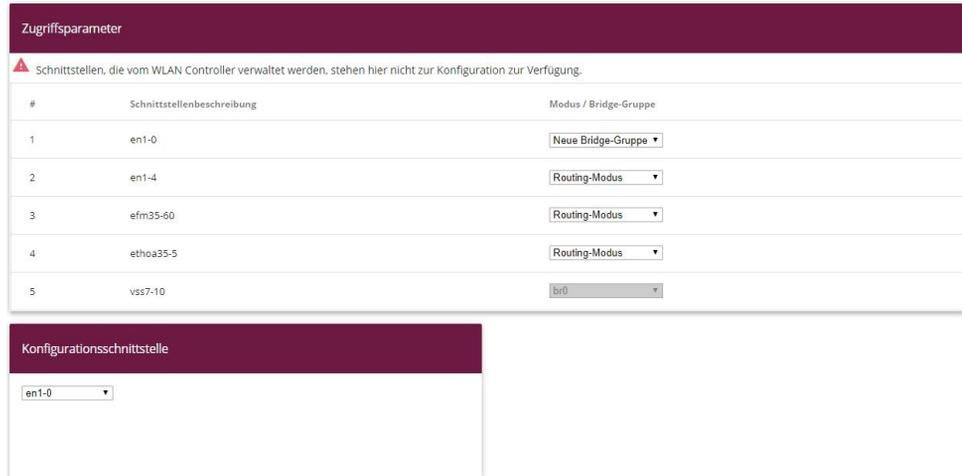


Abb. 38: Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen

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:

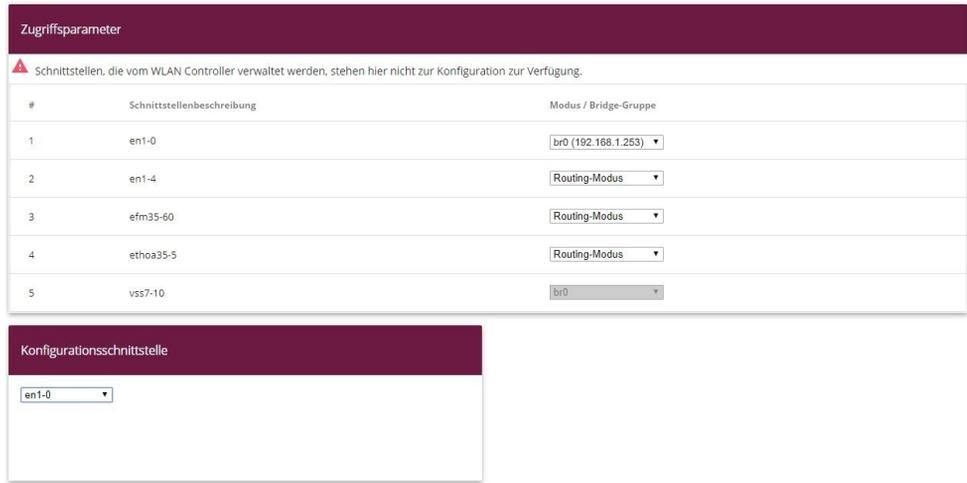


Abb. 39: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**

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

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



Abb. 40: **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.

Zugriffparameter

⚠ Schnittstellen, die vom WLAN Controller verwaltet werden, stehen hier nicht zur Konfiguration zur Verfügung.

#	Schnittstellenbeschreibung	Modus / Bridge-Gruppe
1	en1-0	br0 (192.168.1.253)
2	en1-4	Routing-Modus
3	efm35-60	Routing-Modus
4	ethoa35-5	Routing-Modus
5	vss7-10	br0
6	L2TP-LAC	br0 (192.168.1.253)

Konfigurationsschnittstelle

en1-0

Abb. 41: 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.

3.3 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**.

Wählen Sie das VPN-Szenario aus: ?

VPN-Szenario IPSec - LAN-zu-LAN-Verbindung ▼

Abb. 42: 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.

Ausgewähltes Szenario: LAN-zu-LAN-Verbindung

Verbindungsdetails	IP-Einstellungen eingeben:
Beschreibung IPSec-Peer1	IPSec Peer IPv4-Adresse 10.1.1.1
Lokale IPSec ID be.ip_plus-2	Entferntes IPv4-Netzwerk 1.1.1.1
Entfernte IPSec ID be.ip_plus-1	255.255.255.255
Preshared Key *****	
IP-Version des Tunnelnetzwerks IPv4	
Lokale IP-Adresse 192.168.1.254	
Diese Verbindung als Standardroute definieren <input type="checkbox"/> Deaktiviert	

Abb. 43: 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 -> **.

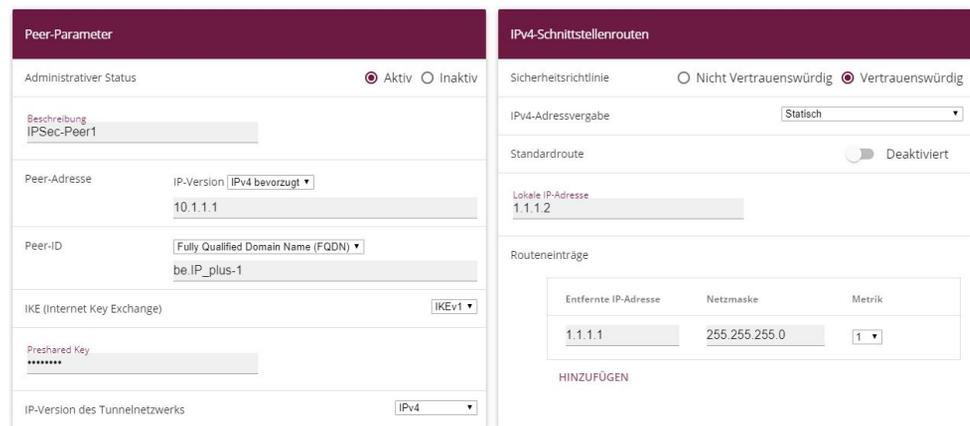


Abb. 44: **VPN -> IPSec -> IPSec-Peers -> **

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**.

Basisparameter	Parameter des LAC-Modus
Beschreibung L2TP-LAS	Entfernte IP-Adresse 1.1.1.1
Lokaler Hostname be.IP_plus-2	UDP-Quellport <input type="checkbox"/> Dynamisch
Entfernter Hostname be.IP_plus-1	UDP-Zielport 1701
Passwort *****	

Erweiterte Einstellungen

Erweiterte Einstellung	
Lokale IP-Adresse 1.1.1.2	
Hello-Intervall 30	Sekunden
Minimale Zeit zwischen Versuchen 1	Sekunden
Maximale Zeit zwischen Versuchen 16	Sekunden
Maximale Anzahl Wiederholungen 5	
Sequenznummern der Datenpakete	<input type="checkbox"/> Deaktivieren

Abb. 46: 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**.

The screenshot shows two configuration panels for a VPN user. The left panel, titled 'Basisparameter', contains the following fields and options:

- Beschreibung:** L2TP-LAS
- Verbindungstyp:** LNS (selected), LAC
- Benutzername:** L2TP-User
- Passwort:** [Redacted]
- Immer aktiv:** Deaktiviert
- Timeout bei Inaktivität:** 300 Sekunden

The right panel, titled 'IP-Modus und Routen', contains the following fields and options:

- IP-Adressmodus:** Statisch (selected), IP-Adresse bereitstellen
- Standardroute:** Deaktiviert
- NAT-Eintrag erstellen:** Deaktiviert
- Lokale IP-Adresse:** 1.1.1.4
- Routeneinträge:** A table with columns 'Entfernte IP-Adresse', 'Netzmaske', and 'Metrik'. The first row contains '1.1.1.3', '255.255.255.255', and '1'. A 'HINZUFÜGEN' button is located below the table.

Below these panels is the 'Erweiterte Einstellungen' section, which is divided into two sub-panels:

Erweiterte Einstellung:

- Blokkieren nach Verbindungsfehler für:** 300 Sekunden
- Authentifizierung:** MS-CHAPv2
- Verschlüsselung:** Keiner (selected), Aktiviert, Windows-kompatibel
- LCP-Erreichbarkeitsprüfung:** Aktiviert
- TCP-ACK-Pakete priorisieren:** Deaktiviert

IP-Optionen:

- OSPF-Modus:** Passiv (selected), Aktiv, Inaktiv
- Proxy-ARP-Modus:** Inaktiv (selected), Aktiv oder Ruhend, Nur aktiv
- DNS-Aushandlung:** Aktiviert

Abb. 48: 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**.

The screenshot shows a web interface with a dark purple header. Below the header, there is a warning icon and a message: "Schnittstellen, die vom WLAN Controller verwaltet werden, stehen hier nicht zur Konfiguration zur Verfügung." Below this is a table with the following data:

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

Below the table, there is a section titled "Konfigurationsschnittstelle" with a dropdown menu showing "en1-0".

Abb. 49: **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:

The screenshot shows two parts of the configuration interface. The top part, titled 'Zugriffsparameter', displays a table of interfaces and their assigned bridge groups. The bottom part, titled 'Konfigurationsschnittstelle', shows the configuration for the selected interface 'en1-0'.

#	Schnittstellenbeschreibung	Modus / Bridge-Gruppe
1	en1-0	br0 (192.168.1.254)
2	en1-4	Routing-Modus
3	efm35-60	Routing-Modus
4	ethoa35-5	Routing-Modus
5	vss7-10	br0

The 'Konfigurationsschnittstelle' section shows a dropdown menu with 'en1-0' selected.

Abb. 50: **Systemverwaltung** -> **Schnittstellenmodus / Bridge-Gruppen** -> **Schnittstellen**

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

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

The screenshot shows the 'Schnittstellen' configuration screen. It features a header 'Schnittstellen' and a main area with a label 'Schnittstelle' and a dropdown menu showing 'L2TP-LAS'.

Abb. 51: **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 da-

zu in folgendes Menü:

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

The screenshot shows a web-based configuration interface. At the top, there is a dark red header with the text 'Zugriffsparmeter'. Below it, a warning icon and text state: 'Schnittstellen, die vom WLAN Controller verwaltet werden, stehen hier nicht zur Konfiguration zur Verfügung.' Below this is a table with the following columns: '#', 'Schnittstellenbeschreibung', and 'Modus / Bridge-Gruppe'. The table contains six rows of interface data. Below the table is a section titled 'Konfigurationsschnittstelle' with a dropdown menu currently showing 'en1-0'.

#	Schnittstellenbeschreibung	Modus / Bridge-Gruppe
1	en1-0	br0 (192.168.1.254)
2	en1-4	Routing-Modus
3	efm35-60	Routing-Modus
4	ethoa35-5	Routing-Modus
5	vss7-10	br0
6	L2TP-LAS	br0 (192.168.1.254)

Abb. 52: **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.

3.4 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-	z. B. IPSec-Peer1

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

Ändern der lokalen IP-Adresse

Feld	Menü	Wert
Lokale IP-Adresse	VPN -> IPSec -> IPSec-Peers -> 	z. B. <i>1.1.1.1</i>

Tunnelprofile konfigurieren

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

Neuen Benutzer konfigurieren

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

Bridge-Gruppe konfigurieren

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

L2TP-Schnittstelle zuweisen

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

Konfiguration Standort B

Feld	Menü	Wert
VPN-Szenario	Assistenten -> VPN -> VPN-Verbindungen -> Neu	<i>IPSec-LAN-zu-LAN-Verbindung</i>

VPN-Assistenten konfiguration

Feld	Menü	Wert
Beschreibung	Assistenten -> VPN -> VPN-	z. B. <i>IPSec-Peer1</i>

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

Ändern der lokalen IP-Adresse

Feld	Menü	Wert
Lokale IP-Adresse	VPN -> IPSec -> IPSec-Peers -> 	z. B. <i>1.1.1.2</i>

Tunnelprofile konfigurieren

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

Neuen Benutzer konfigurieren

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

Bridge-Gruppe konfigurieren

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

L2TP-Schnittstelle zuweisen

Feld	Menü	Wert
Schnittstelle	Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen -> Hinzufügen	<i>L2TP-LAS</i>
Modus / Bridge-Gruppe	Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen	<i>br0 (192.168.1.254)</i>

Kapitel 4 Sicherheit - Stateful Inspection Firewall (SIF)

4.1 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.

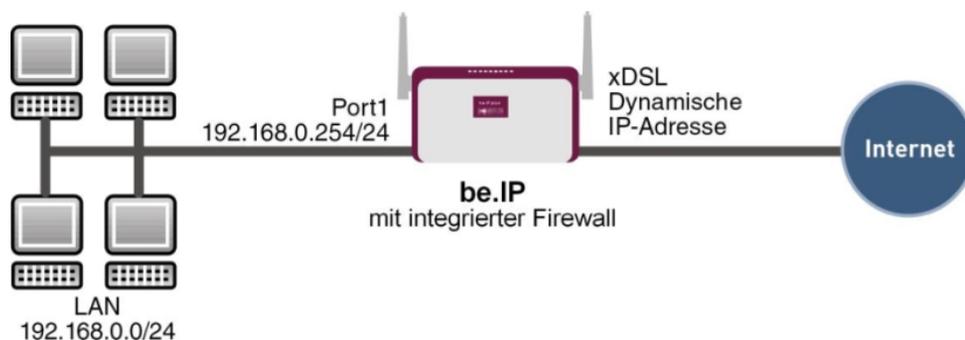


Abb. 53: Beispielszenario SIF

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

4.2 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.

4.2.1 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**.

Basisparameter

Beschreibung
Administrator

IPv4 Aktiviert

Adresstyp Adresse/Subnetz Adressbereich

Adresse/Subnetz
192.168.0.2 / 255.255.255.255

IPv6

Abb. 54: Firewall -> Adressen -> Adressliste -> Neu

Gehen Sie folgendermaßen vor, um einen Aliasnamen für den Administrator zu erstellen:

- (1) Tragen Sie bei **Beschreibung** den Namen des Alias 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 Alias 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 Alias 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 Alias 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**.

Basisparameter

Beschreibung

IP-Version IPv4 IPv6

Auswahl

Adressen	Auswahl
Administrator	<input checked="" type="checkbox"/>
Geschäftsführer	<input checked="" type="checkbox"/>
be.IP	<input type="checkbox"/>
Netzwerk-Intern	<input type="checkbox"/>
ANY	<input type="checkbox"/>

Abb. 55: 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**.

4.2.2 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**.

Basisparameter

Beschreibung
Internetports

Mitglieder

Dienst	Auswahl
activity	<input type="checkbox"/>
ah	<input type="checkbox"/>
any	<input type="checkbox"/>
ftp	<input checked="" type="checkbox"/>
gopher	<input type="checkbox"/>
http	<input checked="" type="checkbox"/>
http (SSL)	<input checked="" type="checkbox"/>
imap	<input type="checkbox"/>

Abb. 56: 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. *Internetports*.
- (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.

4.2.3 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.

Filterregeln					
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv
1	Administration_be.IP	be.IP	Administrationsport	Zugriff	<input checked="" type="checkbox"/> Aktiviert
2	LAN_LOCAL	ANY	dns	Zugriff	<input checked="" type="checkbox"/> Aktiviert
3	Netzwerk-Intern	be.IP	dns	Zugriff	<input checked="" type="checkbox"/> Aktiviert
4	ANY	be.IP	any	Verweigern	<input checked="" type="checkbox"/> Aktiviert
5	Geschäftsführer	ANY	any	Zugriff	<input checked="" type="checkbox"/> Aktiviert
6	Netzwerk-Intern	ANY	Internetports	Zugriff	<input checked="" type="checkbox"/> Aktiviert

Abb. 57: 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.

4.3 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.

4.4 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.

```
bc.IP:> debug all
01:43:23 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.2:1396] -> bc.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] -> bc.IP [1:192.168.0.1:23] telnet:6
01:44:31 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.50:1396] -> bc.IP [1:192.168.0.1:53] dns:17
01:44:34 DEBUG/INET: SIF: Accept Geschaefsfuehrer[1000:192.168.0.50:137] -> ANY[1000:192.168.0.255:137] any:17
01:44:34 DEBUG/INET: SIF: Accept Geschaefsfuehrer[1000:192.168.0.50:123] -> ANY[10001:207.46.232.189:123] any:17
01:44:41 DEBUG/INET: SIF: Accept Geschaefsfuehrer[1000:192.168.0.50:8] -> ANY[10001:62.146.2.103:0] any:1
01:44:43 DEBUG/INET: SIF: Accept Geschaefsfuehrer[1000:192.168.0.50:138] -> ANY[1000:192.168.0.255:138] any:17
bc.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.

4.5 Konfigurationsschritte im Überblick

Aliasnamen für IP-Adressen und Netzadressen

Feld	Menü	Wert
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>Administrator</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.0.2</i> mit <i>255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>Geschäftsführer</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.0.3</i> mit <i>255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>be.IP</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.0.254</i> mit <i>255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>Netzwerk-Intern</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.0.0</i> mit <i>255.255.255.0</i>

Adressgruppen

Feld	Menü	Wert
Beschreibung	Firewall -> Adressen -> Gruppen -> Neu	z. B. <i>Administrati- on_be.IP</i>
Auswahl	Firewall -> Adressen -> Gruppen -> Neu	z. B. <i>Administrator</i> und <i>Geschäftsführer</i>

Dienstgruppen

Feld	Menü	Wert
Beschreibung	Firewall -> Dienste -> Gruppen -> Neu	z. B. <i>Internetports</i>
Mitglieder	Firewall -> Dienste -> Gruppen -> Neu	z. B. <i>http, http (SSL)</i> und <i>ftp</i>
Beschreibung	Firewall -> Dienste -> Gruppen -> Neu	z. B. <i>Administrationsports</i>
Mitglieder	Firewall -> Dienste -> Gruppen -> Neu	z. B. <i>http</i> und <i>telnet</i>

Filterregeln

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Administration_be.IP</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>be.IP</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Administrationsports</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LOCAL</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>ANY</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>dns</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Netzwerk_Intern</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>be.IP</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>dns</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>ANY</i>

Feld	Menü	Wert
	Filterregeln -> Neu	
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>be.IP</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Verweigern</i>
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Geschäftsführer</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>ANY</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Netzwerk_Intern</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>ANY</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Internetports</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Zugriff</i>

Kapitel 5 Sicherheit - VPN-Anbindung über einen SMS PASSCODE-Server

5.1 Einleitung

Dieser Workshop beschreibt die VPN IPSec-Client-Anbindung des **bintec Secure IPSec Clients** 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 Mobilfunknummern 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.

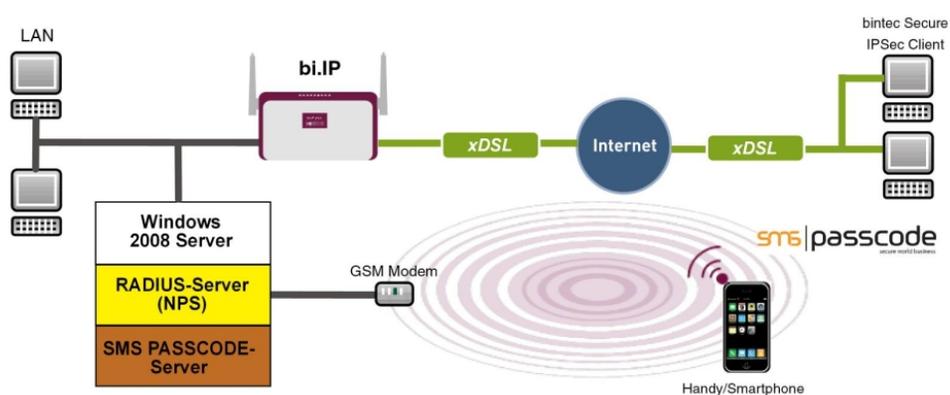


Abb. 58: Beispielszenario

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 kompatibelem GSM-Modem / SIM-Karte (siehe dazu <http://www.smspsscode.com>)
- Mindestens ein **bintec Secure IPSec Client**

5.2 Konfiguration

5.2.1 Hinweise während der Installation und Konfiguration des SMS PASSCODE-Servers

Dieser Abschnitt 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.smspsscode.com>).

5.2.2 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.

5.2.3 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-Assistenten 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. 59: SMS PASSCODE

5.2.4 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 Microsoft 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 Mobilfunknummer 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.

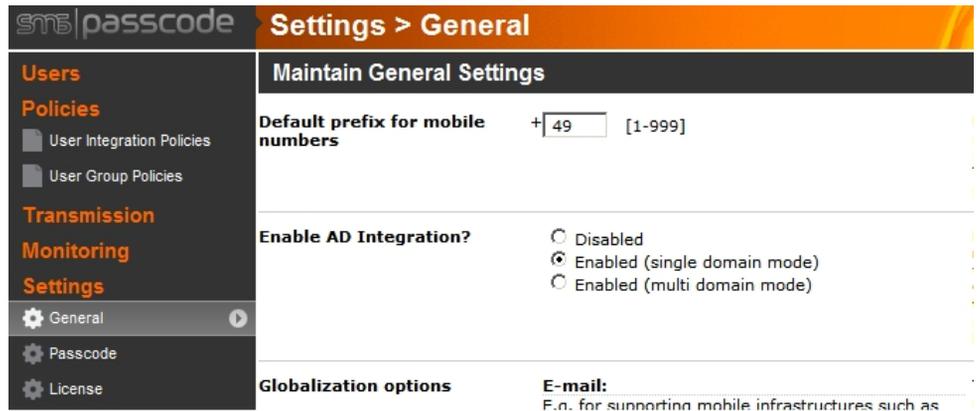


Abb. 60: **Settings -> General**

Anschließend können im Menü **Policies -> User Integration Policies** weitere Einstellungen zum Zugriff auf die Benutzer des **Active Directory** festgelegt werden.

Abb. 61: 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.

5.2.5 Konfiguration des RADIUS-Server zur Anbindung des VPN-Gateways

Die Anbindung des bintec VPN-Gateways erfolgt mit Hilfe des bereits installierten 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.

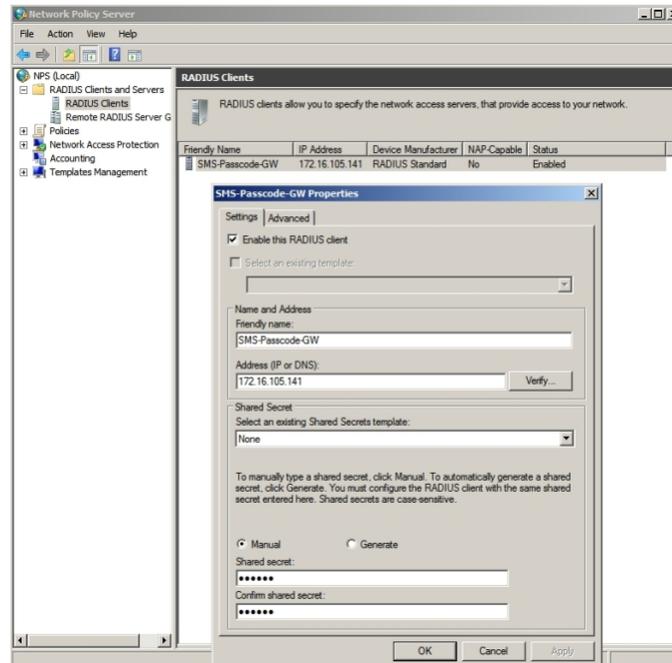


Abb. 62: Network Policy Server (NPS)

- (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**.

5.2.6 Konfiguration des VPN-Gateways

In diesem Szenario 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-Konfiguration** besteht auch die Möglichkeit 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 RADIUS-Server am bintec VPN-Gateway gehen Sie in folgendes Menü:

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

Basisparameter

Authentifizierungstyp

Server-IP-Adresse

RADIUS-Passwort

Standard-Benutzerpasswort

Priorität

Eintrag aktiv Aktiviert

Gruppenbeschreibung

Abb. 63: 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**.

Basisparameter

IP-Poolname
IPSec-Pool

IP-Adressbereich
10.10.10.1 - 10.10.10.100

DNS-Server
Primär
Sekundär

Abb. 64: **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**.

The screenshot shows a configuration window titled 'Basisparameter' with a dark red header. It contains four rows of configuration options:

- Beschreibung:** A text input field containing 'SMS-Passcode'.
- Rolle:** A dropdown menu with 'Server' selected.
- Modus:** A dropdown menu with 'RADIUS' selected.
- RADIUS-Server Gruppen-ID:** A dropdown menu with 'STR_defaultGroup0' selected.

Abb. 65: **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**.

Peer-Parameter	IPv4-Schnittstellenrouten
Administrativer Status <input checked="" type="radio"/> Aktiv <input type="radio"/> Inaktiv	Sicherheitsrichtlinie <input type="radio"/> Nicht Vertrauenswürdig <input checked="" type="radio"/> Vertrauenswürdig
Beschreibung SMS-Passcode-User	IPv4-Adressvergabe <input type="text" value="Server im IKE-Konfigurationsmodus"/>
Peer-Adresse IP-Version <input type="text" value="IPv4 bevorzugt"/>	Konfigurationsmodus <input checked="" type="radio"/> Pull <input type="radio"/> Push
Peer-ID <input type="text" value="Fully Qualified Domain Name (FQDN)"/>	IPv4-Zuordnungs-Pool <input type="text" value="IPSec-Pool"/>
IKE (Internet Key Exchange) <input type="text" value="IKEv1"/>	Lokale IPv4-Adresse <input type="text" value="172.16.105.141"/>
Preshared Key <input type="text" value="*****"/>	
IP-Version des Tunnelnetzwerks <input type="text" value="IPv4"/>	

Abb. 66: 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 Szenario 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**.

Erweiterte Einstellungen

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

Abb. 67: 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**.

5.2.7 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. 68: Verbindungstyp

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



Abb. 69: 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 Internetzugangsrouten verwendet.

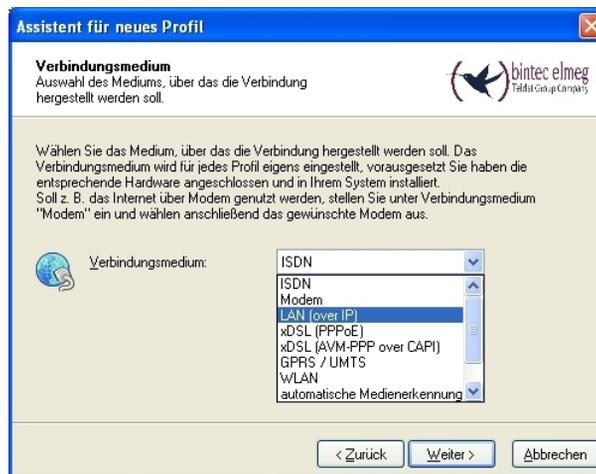


Abb. 70: Verbindungsmedium

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.

Assistent für neues Profil

VPN Gateway-Parameter
Zu welchem Tunnel-Endpunkt soll die Verbindung aufgebaut werden?

Geben Sie an dieser Stelle den Namen (z.B. vpnserver.musterfirma.de) oder die offizielle IP-Adresse (z.B. 212.10.17.29) an, über die das VPN-Gateway erreichbar ist.
Bei erweiterter Authentisierung (XAUTH) kann der Benutzername und das Passwort für die Authentisierung angegeben werden. Werden keine Authentisierungsdaten angegeben, werden diese beim Verbindungsaufbau abgefragt.

Gateway (Tunnel-Endpunkt):
vpngateway.bintec-elmeg.com

Erweiterte Authentisierung (XAUTH)

Benutzername:
mustermann

Passwort:
XXXXXXXX

Passwort (Wiederholung):
XXXXXXXX

< Zurück Weiter > Abbrechen

Abb. 71: 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.

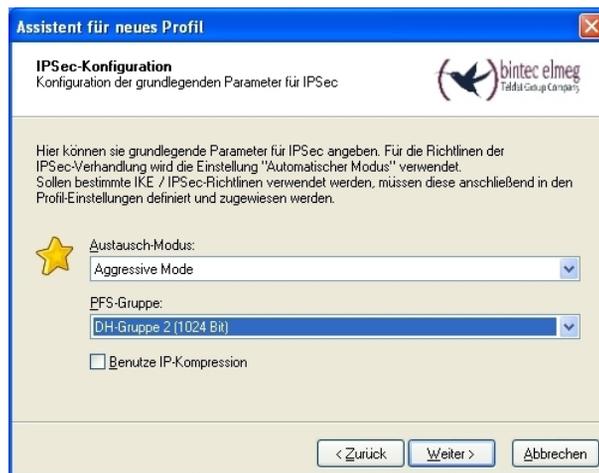


Abb. 72: IPSec-Konfiguration

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. 73: 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. 74: 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. 75: Firewall

5.3 Test der VPN-Verbindung / 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. 76: Secure IP Sec Client

Debug Meldungen des VPN-Gateways beim Verbindungsaufbau

```

P1: peer 0 0 sa 3 (R): new ip 172.16.105.141 <- ip 172.16.105.130
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'da8e937880010000'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'draft-ietf-ipsra-1sakmp-xauth-06'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'draft-ietf-ipsecc-nat-t-ike-03'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'draft-ietf-ipsecc-nat-t-ike-02'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'draft-ietf-ipsecc-nat-t-ike-00'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is '4a131c81070358459c5728f20e95452f'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'dead Peer detection (DPD, RFC 3706)'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'cbleed48b6d8269bb411b61a07bc9e07'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'c61bacaf1a60cc108000000000000000'
P1: peer 0 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is '4048b7d56ebce88525e7de7f00d6c2d3c0000000'
P1: peer 0 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 user@fqdn(any:0,[0..15])=musermann@ldat.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 musermann@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 user@fqdn(any:0,[0..15])=musermann@ldat.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 musermann
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 < any > 100.100.100.2/32:0 rekeyed 0
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): SA 5 established ESP[3e134fc4] 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 musermann
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 musermann succeeded
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): created 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[ddc2f16c] 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

```

5.4 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
Friendly 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. <i>vpngate- way.bintec-elmeg.c om</i>
Erweiterte Authentifizierung (XAUTH)	Assistent für neues Profil	Aktiviert
Benutzername	Assistent für neues Profil	z. B. <i>mustermann</i>
Passwort	Assistent für neues Profil	z. B. <i>supersecret</i>
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. <i>bintec elmeg</i>
Shared Secret (Wiederholung)	Assistent für neues Profil	z. B. <i>bintec elmeg</i>
Typ	Assistent für neues Profil	z. B. <i>Fully Qualified Username</i>
ID	Assistent für neues Profil	z. B. <i>cli- ent1@bintec-elmeg. com</i>
IP-Adres- sen-Zuweisung	Assistent für neues Profil	<i>IKE Config Mode verwenden</i>
Stateful Inspection	Assistent für neues Profil	<i>aus</i>
NetBIOS über IP	Assistent für neues Profil	Aktiviert

Kapitel 6 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/> .

6.1 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

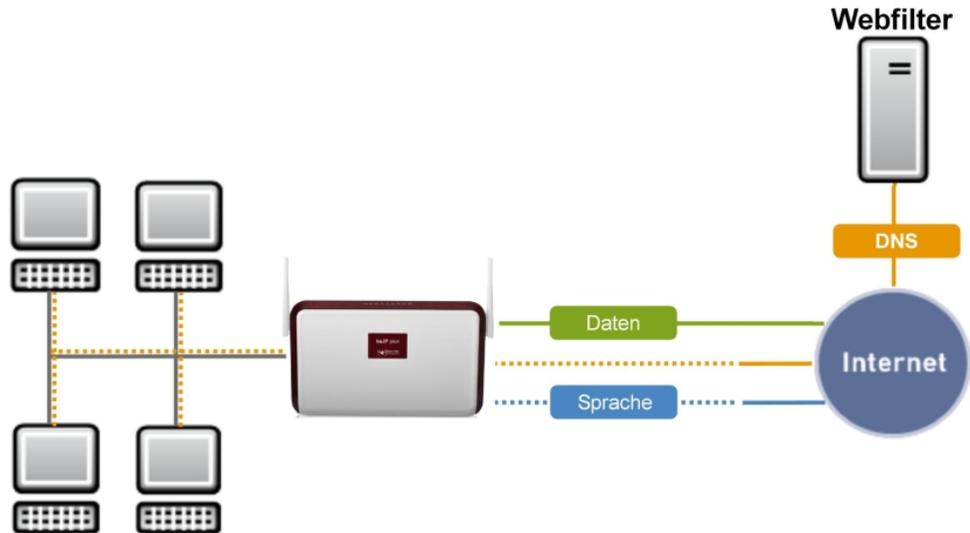


Abb. 77: Scenario

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

6.2 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/>

6.2.1 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.

Webfilter

Webfilter aktivieren Aktiviert

LAN-Schnittstelle BRIDGE_BR0 ▾

IP-Adressbereich der gefilterten Clients 192.168.0.10 - 192.168.0.30

Benutzername
user.name@company.net

Passwort

Filtermodus Standard L2TP

Abb. 78: **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.

6.2.1.1 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:

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

Im Menü **Lokale Dienste** -> **DNS**-> **Domänenweiterleitung** ist die Weiterleitung aller DNS-Anfragen an die DNS-Server des Webfilters angelegt:

Domänenweiterleitung:	
Host/Domäne	Weiterleiten an
*	185.236.104.104 / 185.236.105.105

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:

Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv				
1	BRIDGE_BR0	LOCAL	dns	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↓	☰	🗑️	✎
2	BRIDGE_BR0	WAN_GERMANY - TELEKOM ENTERTAIN	dns	Verweigern	<input checked="" type="checkbox"/> Aktiviert	↓	☰	🗑️	✎

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.

DynDNS-Aktualisierung:					
Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden ÜBERNEHMEN					
Hostname	Schnittstelle	Status	Aktualisierung aktiv	Aktualisierung	
ddns.flashstart.com	Germany - Telekom Entertain	Fehlgeschlagen	<input checked="" type="checkbox"/>	↻	🗑️ ✎

6.3 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.

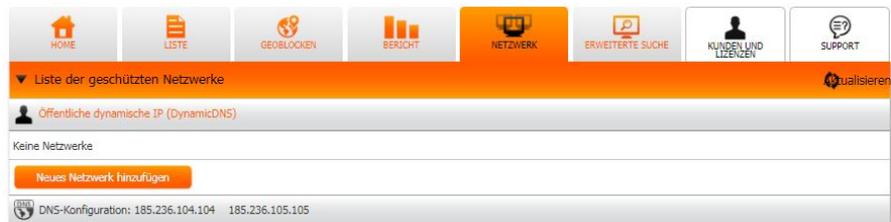
6.3.1 Einrichtung des Webfilters mit dynamischer WAN-IP-Adresse

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.

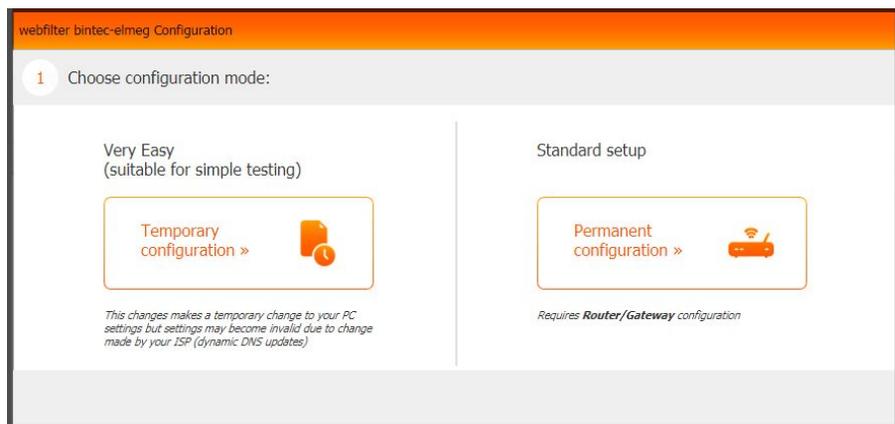
Das Problem hierbei ist, dass sich diese öffentliche IP-Adresse u. a. bei Zwangstrennungen, Neustart des Routers oder administrativer Neueinwahl ändern kann. Um dem bintec elmeg Webfilter-Server die aktuell verwendete IP-Adresse bekannt zu geben, wird ein

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**.

webfilter bintec-elmeg Configuration

3 Do you have a static or a dynamic IP?

I have a Static Ip

I have a Dynamic Ip

« back Continue »

step 3 of 6

- (5) Im darauffolgenden Fenster können Sie eingeben welches Gerät Sie verwenden.

webfilter bintec-elmeg Configuration

4 Confirm your device

Generic device

Help us improve: what router / firewall / device do you use?

bintec be.IP Continue »

« back Continue »

step 4 of 5

- (6) Die Einrichtung des Webfilters mit dynamischer WAN-IP-Adresse ist damit abgeschlossen. Klicken Sie auf **Device connection test** um den Geräteverbindungstest zu starten.

webfilter bintec-elmeg Configuration

Configure the following DNS servers on your router:

- 185.236.104.104
- 185.236.105.105

Configure Dynamic DNS on your router with the data

- Host: ddns.flashstart.com (Can not customize the host?)
- Username: [redacted]
- Password: M*****

View the guide » Device connection test

6.4 Ein zusätzliches Filterprofil einrichten

Ein zusätzliches Filterprofil soll für eine weitere interne Schnittstelle (z. B. Gast-WLAN / vss7-10) mit individuellen Regeln verwendet werden.

6.4.1 Webfilter konfigurieren

Melden Sie sich mit Ihren Anmeldedaten am bintec elmeg Webfilter an (siehe [Einrichtung des Webfilters](#) auf Seite 97). Wählen Sie **Profil->Neues Profil anlegen** auf der Benutzeroberfläche des Webfilters aus (siehe [Webfilter Benutzeroberfläche](#) auf Seite 107) .

The screenshot shows the 'Select profile' configuration window. At the top, there is a 'Help' icon. Below it, a '+ Neues Profil anlegen' button is visible. The current profile is 'Default - Normal'. The configuration form includes the following fields:

- Name:** GastWLAN
- Timezone:** (GMT+01:00) Berlino
- Modus:** Normal
- DNS:** 185.236.104.114 - 185.236.105.115 (highlighted with a red box)
- Netzwerke:** [selected] @bintec-elmeg.com

At the bottom of the form, there are two buttons: 'Einfügen' (orange) and 'Absagen' (grey).

Abb. 79: **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 individuelle DNS-Server gebunden.

Benutzer	Profil	DNS	IP
@bintec-elmeg.com	Default	185.236.104.104 185.236.105.105	80.147.2
	GastWLAN	185.236.104.114 185.236.105.115	

Abb. 80: **Liste der geschützten Netzwerke**

Im nächsten Schritt legen Sie neue Regeln für die zusätzliche Client-Schnittstelle fest.

6.4.2 Router konfigurieren

Gehen Sie auf der Benutzeroberfläche der be.IP in das Menü **Firewall->Richtlinien->IPv4-Filterregeln->Neu**.

Basisparameter	
Quelle	vss7-10
Ziel	LAN_LOCAL
Dienst	dns
Aktion	Zugriff

Abb. 81: **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:

Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv				
1	vss7-10	LAN_LOCAL	dns	Zugriff	Aktiviert				
2	vss7-10	WAN_GERMANY-TELEKOM ENTERTAIN	dns	Verweigern	Aktiviert				
3	vss7-10	LAN_LOCAL	dns	Zugriff	Aktiviert				
4	vss7-10	WAN_GERMANY-TELEKOM ENTERTAIN	dns	Verweigern	Aktiviert				

Abb. 82: 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 ENTER-TAIN* 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**.

Weiterleitungsparameter

Weiterleiten Host Domäne

Host
*

Weiterleiten an Schnittstelle DNS-Server

Quellschnittstelle vss7-10 ▼

Primärer DNS-Server (IPv4/IPv6)
185.236.104.114

Sekundärer DNS-Server (IPv4/IPv6)
182.236.105.115

Abb. 83: **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:

Domänenweiterleitung:	
Host/Domäne	Weiterleiten an
*	185.236.104.104 / 185.236.105.105
*	185.236.104.114 / 182.236.105.115

Abb. 84: Lokale Dienste->DNS->Domänenweiterleitung

Damit ist die Konfiguration eines zusätzlichen Filterprofils abgeschlossen.

6.5 Konfigurationsschritte im Überblick

Webfilter-Konfiguration

Feld	Menü	Wert
Webfilter aktivieren	Assistenten ->Webfilter	Aktiviert
LAN-Schnittstelle	Assistenten ->Webfilter	z. B. <i>BRIDGE_BR0</i>
IP-Adressbereich der gefilterten Clients	Assistenten ->Webfilter	z. B. <i>192.168.0.10 - 192.168.0.30</i>
Benutzername	Assistenten ->Webfilter	z. B. <i>user.name@company.net</i> (Zugangsdaten vom Provider)
Passwort	Assistenten ->Webfilter	Passwort (Zugangsdaten vom Provider)
Filtermodus	Assistenten ->Webfilter	<i>Standard</i>

Zusätzliches Filterprofil einrichten (Webfilter)

Feld	Menü	Wert
Name	Neues Profil anlegen	z. B. <i>GastWLAN</i>
DNS	Neues Profil anlegen	z. B. <i>185.236.104.114 - 185.236.105.115</i>

Zusätzliches Filterprofil einrichten (be.IP)

Feld	Menü	Wert
Quelle	Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu	z. B. <i>vss7-10</i>
Ziel	Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu	z. B. <i>LAN_LOCAL</i>
Dienst	Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu	<i>dns</i>
Aktion	Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu	<i>Zugriff</i>
Quelle	Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu	z. B. <i>vss7-10</i>
Ziel	Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu	z. B. <i>WAN_GERMANY - TELEKOM ENTERTAIN</i>
Dienst	Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu	<i>dns</i>
Aktion	Firewall ->Richtlinien ->IPv4_Filterregeln ->Neu	<i>Verweigern</i>
Quelle	Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu	z. B. <i>vss7-10 (optional)</i>
Ziel	Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu	z. B. <i>LAN_LOCAL (optional)</i>
Dienst	Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu	<i>dns (optional)</i>
Aktion	Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu	<i>Zugriff (optional)</i>
Quelle	Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu	z. B. <i>vss7-10 (optional)</i>
Ziel	Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu	z. B. <i>WAN_GERMANY - TELEKOM ENTERTAIN (optional)</i>
Dienst	Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu	<i>dns (optional)</i>
Aktion	Firewall ->Richtlinien ->IPv6_Filterregeln ->Neu	<i>Verweigern (optional)</i>
Weiterleiten	Lokale Dienste ->DNS ->Domänenwei- terleitung ->Neu	<i>Host</i>

Feld	Menü	Wert
Host	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	*
Weiterleiten an	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	<i>DNS-Server</i>
Quellschnittstelle	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	<i>vss7-10</i>
Primär DNS-Server (IPv4/IPv6)	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	<i>185.236.104.114</i>
Sekundär DNS-Server (IPv4/IPv6)	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	<i>182.236.105.115</i>

Kapitel 7 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



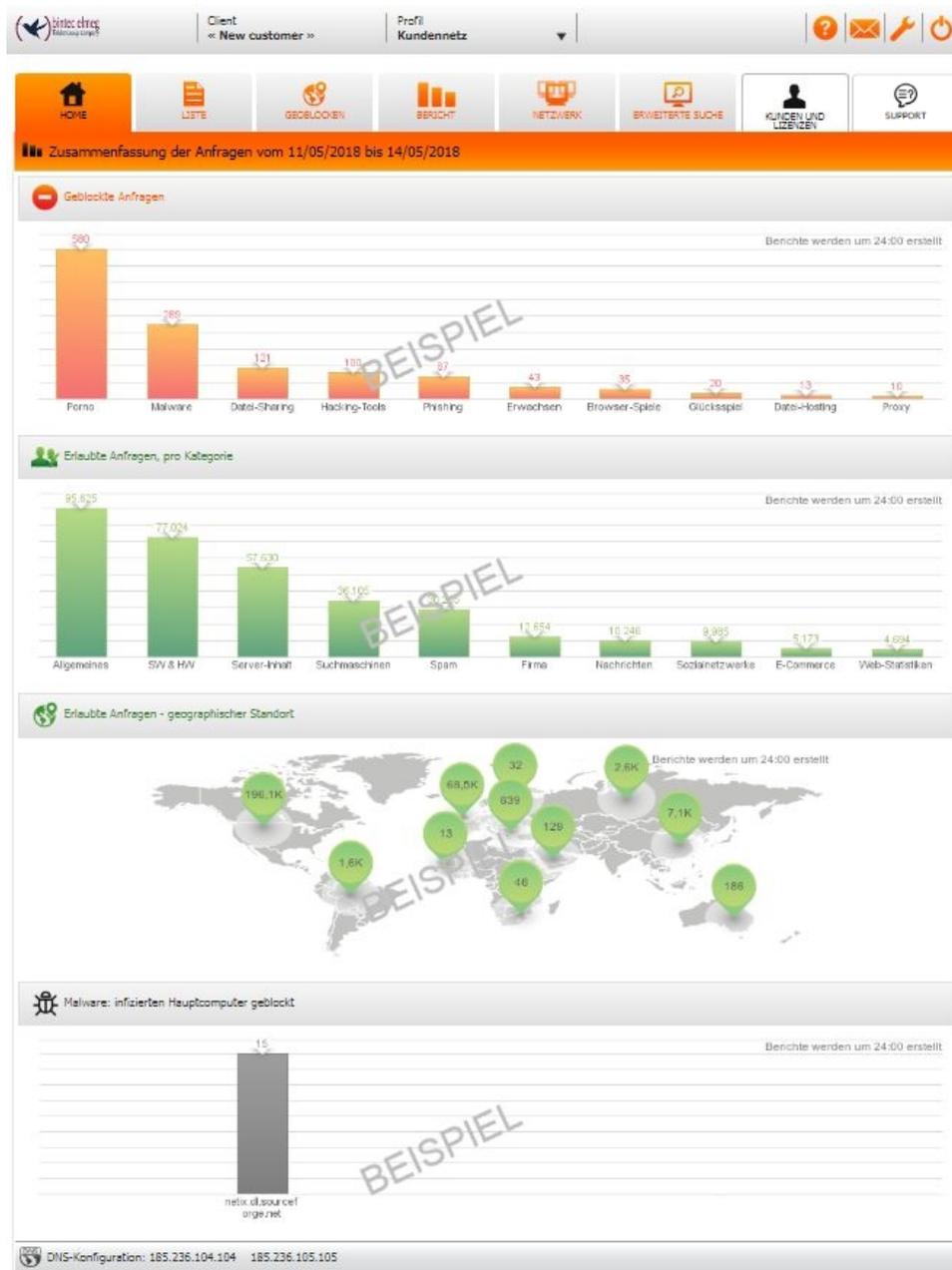
Über das Symbol  können Sie die Online-Hilfe abrufen, mit  die Freigabeanfragen ansehen und verwalten.

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.

Liste

▼ Blacklist des Systems || Echtzeitfilterung anzeigen || In Listen suchen || einen technischen Fehler melden

Kategorienliste	Freigeben	Sperren	zeitliche Sperren
▶ Allgemeines	<input checked="" type="radio"/>	<input type="radio"/>	
▶ Anzeigen, Spam & Webstatistik	<input checked="" type="radio"/>	<input type="radio"/>	
▶ Arbeit	<input checked="" type="radio"/>	<input type="radio"/>	
▶ Freizeit	<input checked="" type="radio"/>	<input type="radio"/>	
▶ kritische Anwendungen	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
▶ Nachrichten	<input checked="" type="radio"/>	<input type="radio"/>	
▶ Social Network	<input checked="" type="radio"/>	<input type="radio"/>	
▶ Suchmaschinen	<input checked="" type="radio"/>	<input type="radio"/>	
▶ Tech & Instant-Messaging	<input checked="" type="radio"/>	<input type="radio"/>	
▶ Unerwünscht	<input checked="" type="radio"/>	<input checked="" type="radio"/>	

Go to easy configuration >

▶ Private Blacklist

▶ Private Whitelist

▶ Erweiterte Einstellungen

DNS-Konfiguration: 185.236.104.104 185.236.105.105

Hier können Sie Kategorien erlauben oder blockieren . In einer Kategorienliste können Sie die Unterkategorien auch einzeln erlauben oder blockieren .

▼ kritische Anwendungen	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
▶ Datei-Sharing	<input checked="" type="radio"/>	<input type="radio"/>	
▶ Glücksspiel	<input type="radio"/>	<input checked="" type="radio"/>	
▶ Hacking-Tools	<input type="radio"/>	<input checked="" type="radio"/>	
▶ Malware	<input type="radio"/>	<input checked="" type="radio"/>	
▶ Phishing	<input type="radio"/>	<input checked="" type="radio"/>	
▶ Proxy	<input type="radio"/>	<input checked="" type="radio"/>	

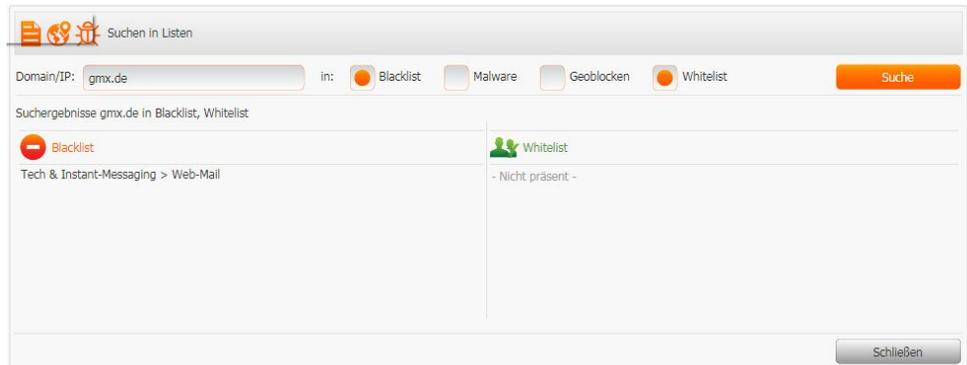
Ebenso können Sie hier eine geplante Blockierung konfigurieren. Wählen Sie dazu eine Kategorie aus und klicken Sie auf das Zeichen in der Spalte **Geplante Blockierung**.

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.

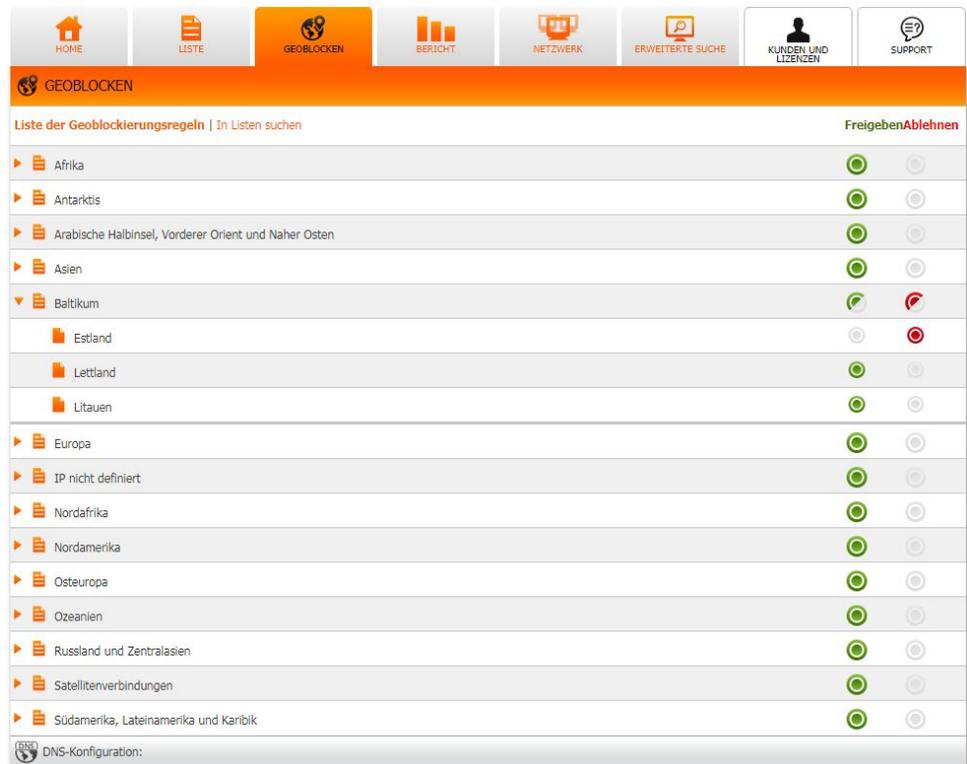
Mit einem Klick auf **Echtzeitfilterung anzeigen** wird angezeigt, welche Kategorien Ihr Webfilter gerade blockiert.

Mit der Option **In Listen suchen** können Sie nach einer bestimmten Domain oder IP-Adresse suchen.



Übersicht Geoblocken

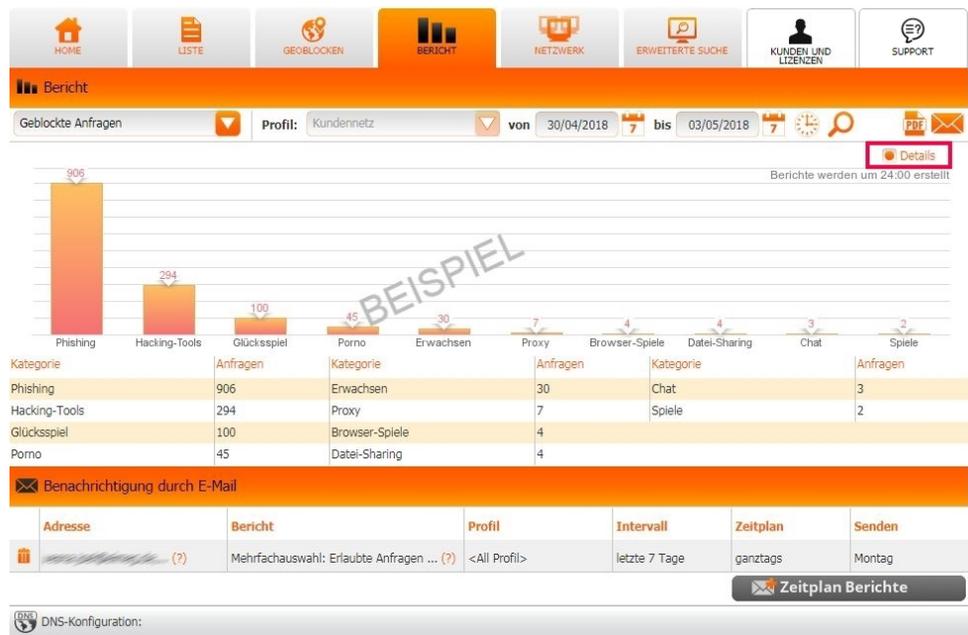
In der Übersicht **Geoblocken** können Sie Länder oder Landbereiche sperren. Klicken Sie dazu in der Spalte **Ablehnen** auf das Symbol .



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.



Bericht

Geblockte Anfragen  Profil: Kundennetz  von 30/04/2018  bis 03/05/2018     [Details](#)

Berichte werden um 24:00 erstellt

BEISPIEL

Kategorie	Anfragen	Kategorie	Anfragen	Kategorie	Anfragen
Phishing	906	Erwachsen	30	Chat	3
Hacking-Tools	294	Proxy	7	Spiele	2
Glücksspiel	100	Browser-Spiele	4		
Porno	45	Datei-Sharing	4		

 Benachrichtigung durch E-Mail

Adresse	Bericht	Profil	Intervall	Zeitplan	Senden
  (?)	Mehrfachauswahl: Erlaubte Anfragen ... (?)	<All Profil>	letzte 7 Tage	ganztags	Montag

 Zeitplan Berichte

 DNS-Konfiguration:

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.

Müssen Sie Ihren Router konfigurieren? Lesen Sie die Anleitungen hier

HOME LISTE GEOBLOCKEN BERICHT NETZWERK ERWEITERTE SUCHE KUNDEN UND LIZENZEN SUPPORT

▼ Liste der geschützten Netzwerke aktualisieren

Öffentliche statische IP

IP-Adresse	Profil	Status	Letzte Registrierung
192.168.4.251	Default - Anschluss 53	●	heute, 09:15:38

Neues Netzwerk hinzufügen

DNS-Konfiguration: 185.236.104.104 185.236.105.105

Erweiterte Suche

In **Erweiterte Suche** können Sie Profile nach Datum, Uhrzeit und nach Kategorie filtern.

AUFMERKSAMKEIT: Die ersten Ergebnisse werden nach etwa drei Stunden gefiltertem Surfen bereitgestellt.

HOME LISTE GEOBLOCKEN BERICHT NETZWERK ERWEITERTE SUCHE KUNDEN UND LIZENZEN SUPPORT

Erweiterte Suche

Profil: Kundennetz | Datum: 03/05/2018 | Zeitplan: 07:00 -> 10:00 | Aktion: Alle | Kategorie: <Alle> | Objekte pro Seite: 30

Suche

Keine Daten für die gewählte Zeitperiode.

- Profil: Kundennetz
- Datum: 03/05/2018 von 07:00 bis 10:00
- Aktion: Alle
- Kategorie: <Alle>

DNS-Konfiguration:

Kunden und Lizenzen

Über **Kunden und Lizenzen** können Sie einen weiteren Kunden anlegen.

Configure filter, select blacklists and manage reports

Filter Management

Try the filter for free and let your customers try it

Activate a demo

Do you have a PIN code? Insert it here to activate

es. XXXXXXXXXX

CUSTOMER

LICENSES »

Cloud single license

New licenses

SUPPORT

LISTS

TRIAL LANDING PAGE LINK

MY PROFILE

▼ ACTIVE TRIALS (1)

Customer	License/User	Expiration	Filter status
▶ WBT	Demo 10000	21/11/2018	

Unterstützung

Über das Menü **Support** gelangen Sie zu der Hilfeseite.

Configure filter, select blacklists and manage reports

Filter Management

Try the filter for free and let your customers try it

Activate a demo

Do you have a PIN code? Insert it here to activate

es. XXXXXXXXXX

CUSTOMER

LICENSES

SUPPORT

Customers and Licenses

Filter Management

Manual

FAQ »

Submit a ticket

LISTS

TRIAL LANDING PAGE LINK

MY PROFILE

» SUPPORT » FILTER MANAGEMENT » FAQ

- ▶ How to run scripts with multi-WAN scenarios
- ▶ Avast Antivirus: Real Site - Resolution compatibility problems
- ▶ How to register my dynamic IP on the Cloud service from a Linux system?
- ▶ How to assign Bulk licenses to end customers?
- ▶ How can I enable access to a domain blocked by Geoblocking?
- ▶ Can we block applications such as Peer to Peer or Torrent?
- ▶ Blacklists/Whitelists modifications appear not to be effective?
- ▶ Why does a blacklisted website remain open for navigation?
- ▶ DNS configuration for computer using
- ▶ How to permit to a specific computer being excepted from traffic filtering?
- ▶ How can I monitor Internet navigation?
- ▶ How to setup automatic emailing of a navigation report?
- ▶ How to block other DNS servers?
- ▶ How to activate traffic filtering with dynamic IP?

Can't find the answer to your problem? ASK FOR SUPPORT

Kapitel 8 Sicherheit - Webfilter mit zwei Internetzugängen

Der zuvor beschriebene Assistent zur Einrichtung des bintec elmeg Webfilters geht nur von einem einzelnen Internetzugang aus. Werden zwei Internetzugänge zur Erhöhung der nutzbaren Internetbandbreite oder zur Absicherung eines Ausfalles konfiguriert, zeigt der Assistent eine Warnung an und kann nicht verwendet werden.



Abb. 85: Assistenten->Webfilter

Im folgenden wird davon ausgegangen, dass beide Internetzugänge ohne ein zusätzliches NAT auf der Providerseite (CGN - Carrier Grade NAT) bereitgestellt werden und in Betrieb sind. Die gleichzeitige Verwendung von zwei Internetzugängen ist in den IP-Workshops https://archive.bintec-elmeg.com/Files/Weitere_Downloads/Documentation/workshops/current_de/ws_ip_pdf_de.PDF bzw. https://archive.bintec-elmeg.com/Files/Weitere_Downloads/Documentation/workshops/current_de/ws_ip_html_de_HTML/start.html beschrieben. Da der Webfilter die anfragende IP-Adresse dazu verwendet, eine DNS-Anfrage einem konfiguriertem Filterprofil zuzuordnen, muss der Webfilter die IP-Adressen beider Internetzugänge kennen. Um die dynamischen IP-Adressen der Internetzugänge zu lernen, erwartet der Webfilter Updates über das DynDNS-Protokoll vom bintec elmeg Router. Die Quell-IP-Adressen dieser Anfragen werden dann gespeichert.

8.1 Neues Netzwerk einrichten

Jedes **Netzwerk** im bintec elmeg Webfilter speichert eine öffentliche IP-Adresse. In einem Szenario mit zwei Internetzugängen müssen daher auch zwei Netzwerke angelegt sein. Nach dem Anlegen des Accounts und dem ersten Login ist schon ein Netzwerk eingerichtet.

▼ Liste der geschützten Netzwerke

Öffentliche dynamische IP (DynamicDNS)

Benutzer	Profil	DNS	IP	Status	Letzte Synchronisation
@bintec-elmeg.com	Default	→ { 185.236.104.104 185.236.105.105	87. .225	●	heute, 13:47:08
	GastWLAN	→ { 185.236.104.114 185.236.105.115			

Neues Netzwerk hinzufügen

Einzigartiger DNS zum Einrichten in Ihrem Netzwerk: 185.236.104.104 185.236.105.105

Impressum | Datenschutzerklärung © 2020 von Collini Consulting

Um ein neues Netzwerk anzulegen, klicken Sie auf **Neues Netzwerk hinzufügen**. In dem sich öffnenden Dialog wählen Sie das vorhandene Filterprofil zur weiteren Verwendung aus.

webfilter bintec-elmeg Configuration

You already have a network enabled, do you want to use an existing profile for the new network?

Yes, use profile: Default

No, create a new profile

Continue >

Klicken Sie anschließend auf **Fortfahren**.

Wählen Sie nun **Schließen Sie einen Router an (für dynamische IP-Verbindungen)**.

 .26' (unselected) and 'Schließen Sie einen Router an (für dynamische IP-Verbindungen)' (selected). A 'Fortfahren >' button is at the bottom right, and a '< back' button is at the bottom left."/>

webfilter bintec-elmeg Configuration

Jetzt müssen Sie Ihren Standort definieren

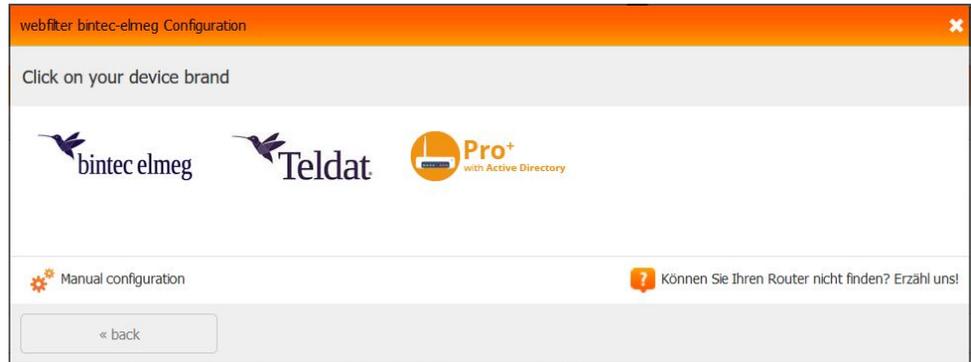
Gewähren Sie eine statische IP 93. .26

Schließen Sie einen Router an (für dynamische IP-Verbindungen)

Fortfahren >

< back

Nach einem erneuten Klick auf **Fortfahren** werden Sie nach dem Routerhersteller gefragt. Wählen Sie hier **bintec elmeg** und im nächsten Schritt auf **bintec elmeg** (ohne Cloud-Filter Integration) .



The screenshot shows a configuration window titled "webfilter bintec-elmeg Configuration". The main heading is "Click on your device brand". Below this, there are three logos: "bintec elmeg", "Teldat", and "Pro+ with Active Directory". At the bottom left, there is a gear icon and the text "Manual configuration". At the bottom right, there is a question mark icon and the text "Können Sie Ihren Router nicht finden? Erzähl uns!". A "« back" button is located at the bottom left.



The screenshot shows the same configuration window, now at the "Choose model:" step. The "bintec elmeg" logo is selected. Below it, there are two router models: "Bintec Elmeg" and "Bintec Elmeg - Integration mit dem Cloud-Filter". A "« back" button is located at the bottom left.

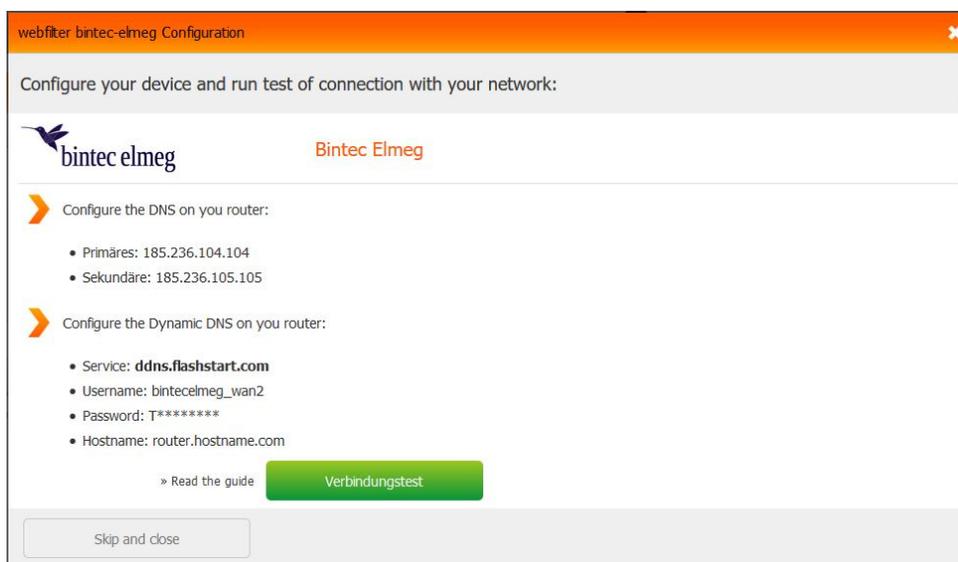
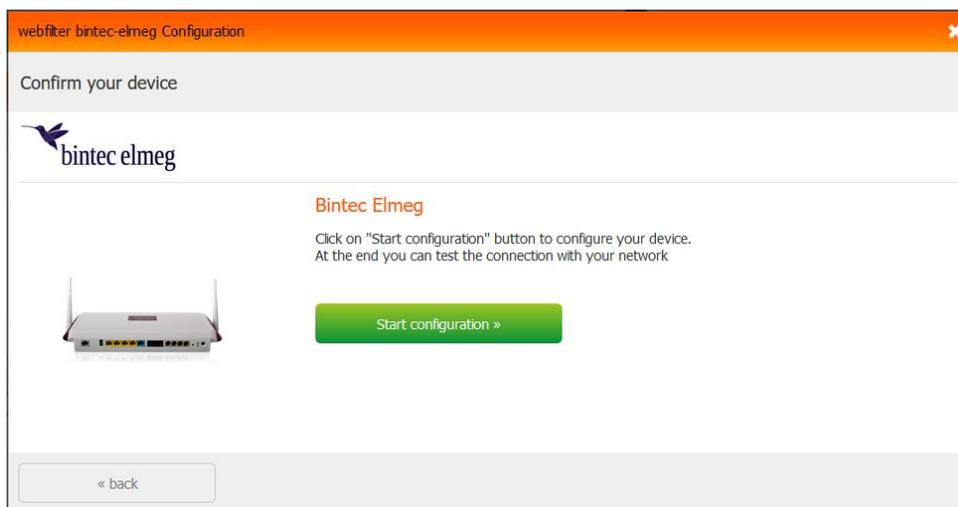
Im letzten Schritt werden Sie aufgefordert, einen **Benutzernamen** und ein **Kennwort** zur Aktualisierung der IP-Adresse des neuen Netzwerks anzulegen. Diese Kombination aus Benutzername und Kennwort wird später in der Konfiguration des bintec elmeg Routers benötigt.



The screenshot shows the configuration window at the "Register new user:" step. It contains three input fields: "Email/Username:" with the value "bintecelmeg_wan2", "Password:" with masked characters "*****", and "Passwort bestätigen:" with masked characters "*****". At the bottom left is a "« back" button, and at the bottom right is a green "Continue »" button.

Nachdem Sie den **Benutzernamen** und das **Kennwort** eingerichtet haben, werden Sie zu-

erst aufgefordert, die Routerkonfiguration zu starten und bekommen anschließend die Informationen zur Einrichtung des DynDNS-Clients angezeigt.



Schließen Sie dieses Fenster mit **Skip and close**.

Sie sehen nun, das neu eingerichtete **Netzwerk** in der Übersicht.

Benutzer	Profil	DNS	IP	Status	Letzte Synchronisation
bintecelmeg_wan2	Default	→ { 185.236.104.104 185.236.105.105		●	nie
@bintec-elmeg.com	Default	→ { 185.236.104.104 185.236.105.105	87.225	●	heute, 13:47:08
	GastWLAN	→ { 185.236.104.114 185.236.105.115			

Einzigartiger DNS zum Einrichten in Ihrem Netzwerk: 185.236.104.104 185.236.105.105

8.2 Profile dem neuen Netzwerk zuordnen

Um dem neu angelegten Netzwerk schon vorhandene Filterprofile zuzuweisen, klicken Sie oben in die Profilauswahl und neben dem gewünschten Profile auf das Symbol .

Benutzer	Profil	DNS	IP	Status	Letzte Synchronisation
bintecelmeg_wan2	Default	→ { 185.236.104.104 185.236.105.105		●	nie
@bintec-elmeg.com	Default	→ { 185.236.104.104 185.236.105.105	87.225	●	heute, 13:47:08
	GastWLAN	→ { 185.236.104.114 185.236.105.115			

Einzigartiger DNS zum Einrichten in Ihrem Netzwerk: 185.236.104.104 185.236.105.105

Anschließend aktivieren Sie für dieses Profil das neu angelegte Netzwerk.

Profil auswählen

Name: GastWLAN

Zeitzone: (GMT+01:00) Berlino

Modus: Normal

DNS zugewiesen: 185.236.104.114 - 185.236.105.115

Quellennetze: bintecelmeg_wan2

Bestätigen Abbrechen

Benutzer	Profil
bintecelmeg_wan2	Default
@bintec-elmeg.com	Default
	GastWLAN

Einzigartiger DNS zum Einrichten in Ihrem Netzwerk: 185.236.104.104 185.236.105.105

In der Übersicht sehen Sie nun, dass dem neuen Netzwerk zwei Filterprofile zugeordnet sind.

Liste der geschützten Netzwerke

Öffentliche dynamische IP (DynamicDNS)

Benutzer	Profil	DNS	IP	Status	Letzte Synchronisation
bintecelmeg_wan2	Default	→ 185.236.104.104 185.236.105.105		●	nie
	GastWLAN	→ 185.236.104.114 185.236.105.115		●	
@bintec-elmeg.com	Default	→ 185.236.104.104 185.236.105.105	87.225	●	heute, 05:49:39
	GastWLAN	→ 185.236.104.114 185.236.105.115		●	

Einzigartiger DNS zum Einrichten in Ihrem Netzwerk: 185.236.104.104 185.236.105.105

8.3 Neuen DynDNS-Provider anlegen

Um später die Updates der zweiten IP-Adresse sicher über den zweiten Internetzugang durchführen zu können, legen Sie einen neuen DynDNS-Provider an.

Gehen Sie auf der Benutzeroberfläche des Routers in das Menü **Lokale**

DynDNS-Client->DynDNS-Provider und klicken Sie auf **Neu**.

Basisparameter

Providername	Webfilter2
Server	ddns2.flashstart.com
Aktualisierungspfad	/nic/update
Port	80
Protokoll	DynDNS
Aktualisierungsintervall	60 Sekunden
IPv6-Server	
Unterstützt SSL	<input type="checkbox"/> Deaktiviert
Homepage	https://webfilter.bintec-elmeg.com

Abb. 86: Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu

Gehen Sie folgendermaßen vor:

- (1) Tragen Sie den **Providernamen** für den Eintrag ein, z. B. *Webfilter2*.
- (2) Bei **Server** geben Sie den Host-Namen oder die IP-Adresse des Servers ein, hier z. B. *ddns2.flashstart.com*.
- (3) Geben Sie den **Aktualisierungspfad** ein, z. B. */nic/update*.
- (4) Geben Sie den **Port** ein, z. B. *80*.
- (5) Bei **Protokoll** wählen Sie *DynDNS* aus.
- (6) Den **Aktualisierungsintervall** stellen Sie auf *60* Sekunden ein.
- (7) Um direkt auf die Seite des Anbieters zu gelangen, können Sie bei **Homepage** eine Web-Adresse eingeben, hier z. B. *https://webfilter.bintec-elmeg.com*.
- (8) Klicken Sie auf **OK**.

Da der DynDNS-Dienst des Webfilters lediglich dazu verwendet wird, IP-Adressen zu ermitteln, nicht aber um Einträge in DNS-Servern anzulegen, wird die Überprüfung des DynDNS-Updates fehlschlagen. Um diese Überprüfung zu deaktivieren und um Updates in kurzen Intervallen zuzulassen, wechseln Sie unter **Ansicht** in den **SNMP-Browser**.



Im Bereich **ip** wählen Sie die **ipDynDnsProviderTable** aus und bearbeiten den neu angelegten Eintrag **Webfilter2**.

ipDynDnsProviderTable	
ipDdnsIndex	100
ipDdnsName (*) Webfilter2	
ipDdnsServer ddns2.flashstart.com	
ipDdnsPath /nic/update	
ipDdnsPort 80	
ipDdnsProtocol	dyn dns ▾
ipDdnsMinWait 60	
ipDdnsVerification	disabled ▾
ipDdnsUpdateInterval 60	
ipDdnsServer6	
ipDdnsSupportsSSL	no ▾

Gehen Sie folgendermaßen vor:

- (1) Setzen Sie den Wert für **ipDdnsMinWait** auf *60* und wählen Sie für **ipDdnsVerification** *disabled* aus.
- (2) Klicken Sie auf **OK** und wechseln zurück in die Standard-Ansicht.

8.4 Statische Routen zum DynDNS-Server anlegen

Um sicherzustellen, dass die DynDNS-Updates über die richtige Schnittstelle ausgeführt werden, müssen Sie im Router statische Routen anlegen.

Wechseln Sie dafür in das Menü **Netzwerk->Routen->Konfiguration von IPv4-Routen** und klicken Sie auf **Neu**.

Basisparameter	Routenparameter
Routentyp Host-Route über Schnittstelle	Ziel-IP-Adresse/Netzmaske 185.236.104.104 / 255.255.255.255
Schnittstelle WAN_GERMANY - TELEKOM BUSINESS	Lokale IP-Adresse 0.0.0.0
Routenklasse <input checked="" type="radio"/> Standard <input type="radio"/> Erweitert	Metrik 1

Abb. 87: Netzwerk->Routen->Konfiguration von IPv4-Routen ->Neu

Gehen Sie folgendermaßen vor:

- (1) Unter **Routentyp** wählen Sie *Host-Route über Schnittstelle* aus.
- (2) Wählen Sie unter **Schnittstelle** den ersten Internetzugang aus, hier *WAN_GERMANY - TELEKOM BUSINESS*.
- (3) Unter **Ziel-IP-Adresse/Netzmaske** tragen Sie die *185.236.104.104* als Adresse des ersten DynDNS-Servers ein.
- (4) Bestätigen Sie die Eingaben mit **OK**.

Wiederholen Sie die Schritte für die zweite Schnittstelle und den zweiten DynDNS-Server.

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

Basisparameter	Routenparameter
Routentyp Host-Route über Schnittstelle	Ziel-IP-Adresse/Netzmaske 185.236.104.114 / 255.255.255.255
Schnittstelle WAN_TELEKOM2	Lokale IP-Adresse 0.0.0.0
Routenklasse <input checked="" type="radio"/> Standard <input type="radio"/> Erweitert	Metrik 1

Abb. 88: Netzwerk->Routen->Konfiguration von IPv4-Routen ->Neu

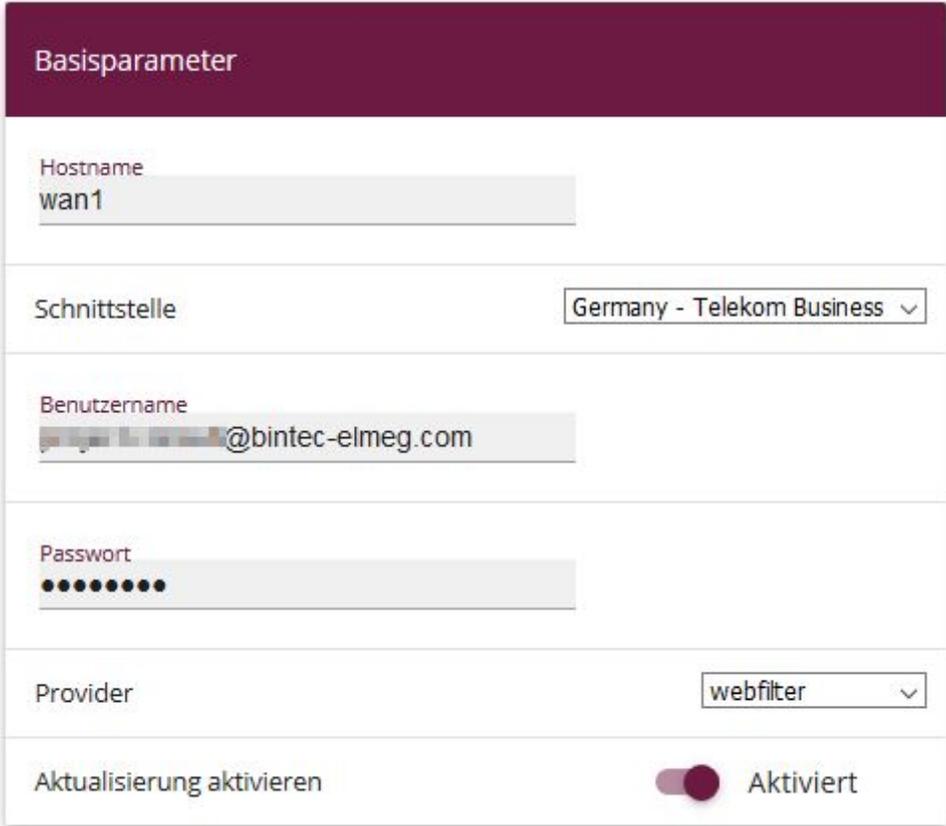
Gehen Sie folgendermaßen vor:

- (1) Unter **Routentyp** wählen Sie *Host-Route über Schnittstelle* aus.
- (2) Wählen Sie unter **Schnittstelle** den ersten Internetzugang aus, hier *WAN_TELEKOM2*.
- (3) Unter **Ziel-IP-Adresse/Netzmaske** tragen Sie die *185.236.104.114* als Adresse des ersten DynDNS-Servers ein.
- (4) Bestätigen Sie die Eingaben mit **OK**.

8.5 Neuen DynDNS-Client anlegen

Im folgenden legen Sie zwei DynDNS-Clients an, um dem Webfilter die IP-Adressen der beiden Internetzugänge bekannt zu machen.

Wechseln Sie hierzu in das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung** und klicken Sie auf **Neu**.



Basisparameter

Hostname
wan1

Schnittstelle
Germany - Telekom Business

Benutzername
[masked]@bintec-elmeg.com

Passwort
[masked]

Provider
webfilter

Aktualisierung aktivieren Aktiviert

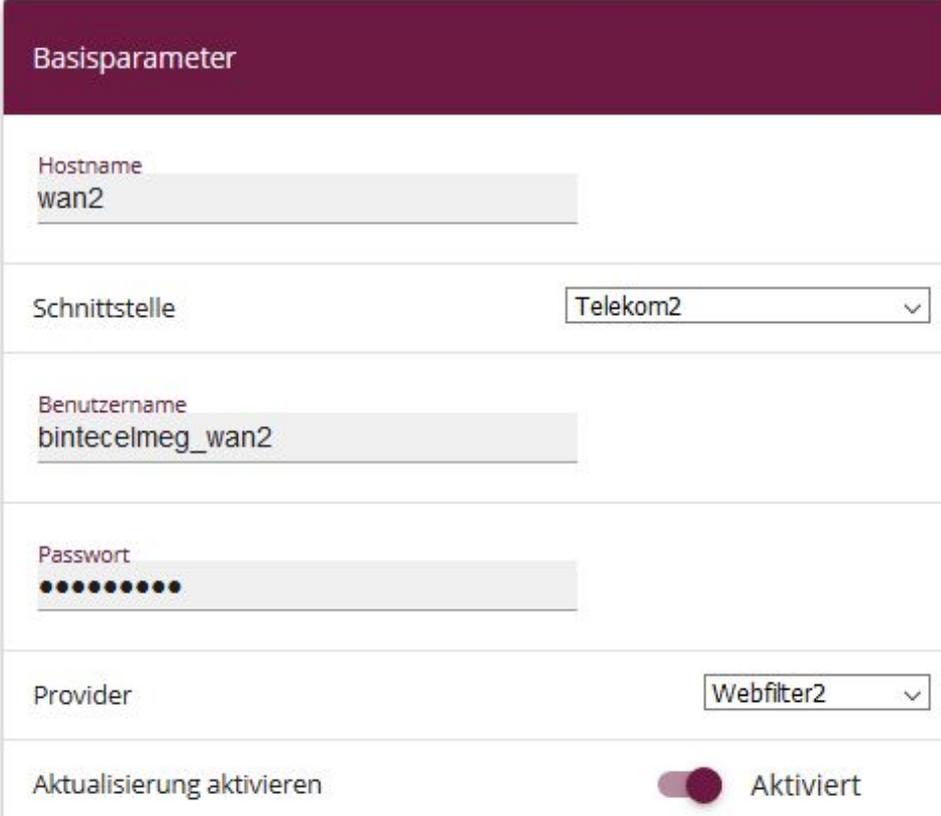
Abb. 89: **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie den **Hostnamen** ein, z. B. *wan1*.
- (2) Bei **Schnittstelle** wählen Sie *Germany - Telekom Business* (der erste Internetzugang).
- (3) Unter **Benutzername** tragen Sie Ihren Anmeldenamen im Webfilter (Ihre E-Mail-Adresse) ein.

- (4) Bei **Passwort** geben Sie Ihr Anmeldepasswort im Webfilter ein.
- (5) Wählen Sie Ihren **Provider** aus, hier z. B. *webfilter*.
- (6) Aktivieren Sie die Option **Aktualisierung aktivieren**.
- (7) Speichern Sie die Eingaben mit **OK** und legen Sie einen weiteren Eintrag an.

Gehen Sie in das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung** und klicken Sie auf **Neu**.



The screenshot shows a configuration window titled "Basisparameter" with a dark red header. Below the header are several input fields and dropdown menus:

- Hostname:** A text input field containing "wan2".
- Schnittstelle:** A dropdown menu with "Telekom2" selected.
- Benutzername:** A text input field containing "bintecelmeg_wan2".
- Passwort:** A text input field with 10 black dots representing a masked password.
- Provider:** A dropdown menu with "Webfilter2" selected.
- Aktualisierung aktivieren:** A toggle switch that is currently turned on, labeled "Aktiviert".

Abb. 90: **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu**

Gehen Sie folgendermaßen vor:

- (1) Geben Sie den **Hostnamen** ein, z. B. *wan2*.
- (2) Bei **Schnittstelle** wählen Sie *Telekom2* (der zweiten Internetzugang).
- (3) Unter **Benutzername** tragen Sie den neu vergebenen Benutzernamen ein, (siehe [Neues Netzwerk einrichten](#) auf Seite 115)

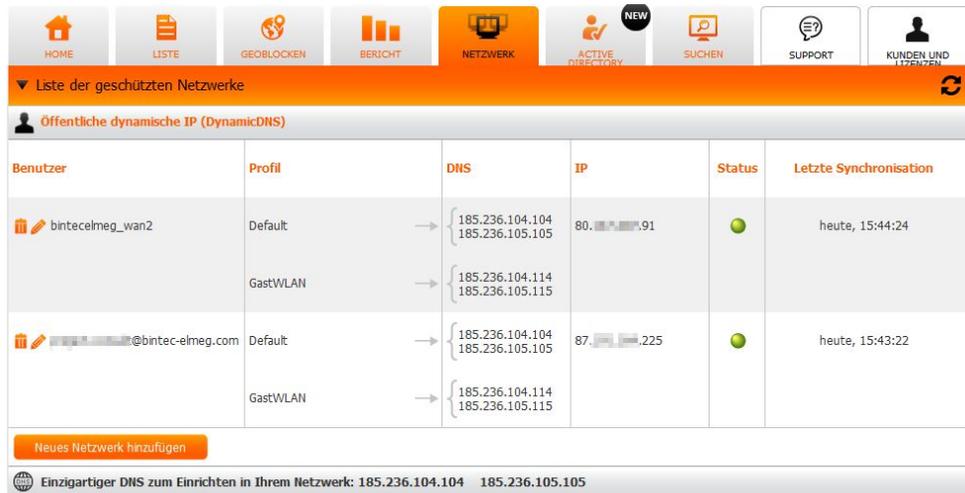
- (4) Bei **Password** geben Sie das neu vergebene Passwort ein, (siehe [Neues Netzwerk einrichten](#) auf Seite 115)
- (5) Wählen Sie Ihren **Provider** aus, hier z. B. *webfilter2*.
- (6) Aktivieren Sie die Option **Aktualisierung aktivieren**.
- (7) Speichern Sie die Eingaben mit **OK**.

Sie sehen nun die beiden eingerichteten Clients.



Abb. 91: Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung

Im Webfilter können Sie nun sehen, dass die beiden IP-Adressen der zwei Internetzugänge bekannt sind.



8.6 DNS Domänenweiterleitung einrichten

Das Konzept des Webfilters basiert darauf, dass alle DNS-Anfragen an den Webfilter weitergeleitet werden. Dort wird anhand der Filterprofile entschieden, ob die richtige Antwort zurückgegeben wird oder ob als Ziel eine Infoseite angezeigt wird, dass der Zugriff auf die gewünschte Adresse gesperrt ist. Dazu ist es erforderlich alle DNS-Anfragen, die am bintec-elmeg Router eingehen an die DNS-Server des Webfilters weiterzuleiten.

Wechseln Sie dazu in das Menü **Lokale Dienste->DNS->Domänenweiterleitung ->Neu** und erstellen sie einen neuen Eintrag.

Weiterleitungsparameter

Weiterleiten Host Domäne

Domäne
*

Weiterleiten an Schnittstelle DNS-Server

Quellschnittstelle BRIDGE_BR0

Primärer DNS-Server (IPv4/IPv6)
185.236.104.104

Sekundärer DNS-Server (IPv4/IPv6)
185.236.105.105

Abb. 93: **Lokale Dienste->DNS->Domänenweiterleitung ->Neu**

Gehen Sie folgendermaßen vor:

- (1) Bei **Weiterleiten** wählen Sie *Domäne* aus.
- (2) Bei **Domäne** geben Sie * ein.

- (3) Unter **Weiterleiten an** wählen Sie *DNS-Server* aus.
- (4) Bei **Quellschnittstelle** wählen Sie die Schnittstelle, an der die Clients verbunden sind aus, hier *BRIDGE_BR0*.
- (5) Geben Sie unter **Primärer DNS-Server (IPv4/IPv6)** den DNS-Server, der in der Webfilter Netzwerkübersicht Ihren Filterprofilen zugeordnet ist, hier *185.236.104.104*.
- (6) Geben Sie unter **Sekundärer DNS-Server (IPv4/IPv6)** den DNS-Server, der in der Webfilter Netzwerkübersicht Ihren Filterprofilen zugeordnet ist, hier *185.236.105.105*.
- (7) Speichern Sie den Eintrag mit **OK**.

8.7 Firewall - Schnittstellengruppe anlegen

Damit der Webfilter nicht umgangen werden kann, muss der Zugriff auf andere DNS-Server durch Firewallregeln verhindert werden. Um die Regeln einfach zu halten, legen Sie eine Schnittstellengruppe an, die die beiden Internetzugänge enthält.

Wechseln Sie dazu in das Menü **Firewall->Schnittstellen->IPv4-Gruppen->Neu** und legen Sie einen neuen Eintrag an.

Basisparameter

Beschreibung
WAN-Schnittstellen

Mitglieder

Schnittstelle	Auswahl
LAN_LOCAL	<input type="checkbox"/>
LAN_EN1-4	<input type="checkbox"/>
WAN_ETHOA35-5	<input type="checkbox"/>
BRIDGE_BR0	<input type="checkbox"/>
LAN_EN1-2	<input type="checkbox"/>
WAN_GERMANY - TELEKOM BUSINESS	<input checked="" type="checkbox"/>
WAN_TELEKOM2	<input checked="" type="checkbox"/>

Abb. 94: Firewall->Schnittstellen->IPv4-Gruppen->Neu

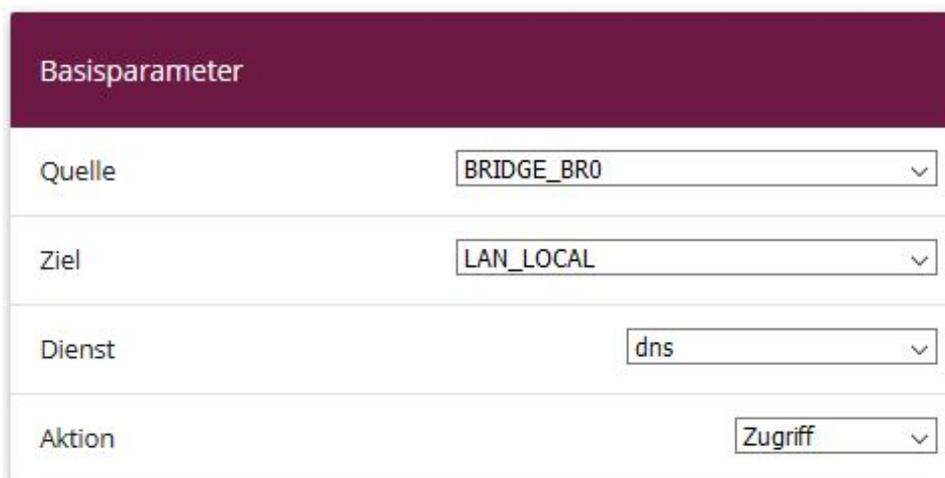
Gehen Sie folgendermaßen vor:

- (1) Geben Sie eine **Beschreibung** ein, die Sie wiedererkennen, z. B. *WAN-Schnittstellen*.
- (2) Unter **Mitglieder** wählen Sie die beiden Internetzugänge aus, hier *WAN_GERMANY - TELEKOM BUSINESS* und *WAN_TELEKOM2*.
- (3) Speichern Sie den Eintrag mit **OK**.

8.8 Firewall-Regeln anlegen

Im letzten Schritt müssen Sie Firewall-Regeln erstellen, die DNS-Anfragen an den bintec-elmeg Router erlauben, Anfragen an DNS-Server im Internet aber verhindern.

Wechseln Sie dazu ins Menü **Firewall->Richtlinien->IPv4-Filterregeln->Neu** und legen einen neuen Eintrag an, der DNS-Anfragen an den bintec-elmeg Router zulässt.



The screenshot shows a configuration window titled 'Basisparameter' with a dark red header. It contains four rows of configuration options, each with a label on the left and a dropdown menu on the right:

Basisparameter	
Quelle	BRIDGE_BR0
Ziel	LAN_LOCAL
Dienst	dns
Aktion	Zugriff

Abb. 95: **Firewall->Richtlinien->IPv4-Filterregeln->Neu**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie als **Quelle** die Schnittstelle aus, über die die zu filternden Endgeräte verbunden sind, hier *BRIDGE_BR0*.
- (2) Wählen Sie als **Ziel** *LAN_LOCAL* aus.
- (3) Unter **Dienst** wählen Sie *dns* aus.
- (4) Als **Aktion** geben Sie *Zugriff* an.
- (5) Speichern Sie Ihre Eingaben mit **OK** und legen eine weitere Regel an, die Zugriffe auf DNS-Server im Internet verhindert.

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

Basisparameter

Quelle	BRIDGE_BRO
Ziel	WAN-Schnittstellen
Dienst	dns
Aktion	Verweigern

Abb. 96: Firewall->Richtlinien->IPv4-Filterregeln->Neu

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie als **Quelle** erneut die Client-Schnittstelle aus, hier *BRIDGE_BRO*.
- (2) Als **Ziel** wählen Sie die Schnittstellengruppe *WAN-Schnittstellen* aus.
- (3) Unter **Dienst** wählen Sie *dns* aus.
- (4) Als **Aktion** tragen Sie *Verweigern* ein.
- (5) Speichern Sie Ihre Eingaben mit **OK**.

Sie sehen die neu eingerichteten Firewall-Regeln.

Filterregeln

Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv				
1	BRIDGE_BRO	LAN_LOCAL	dns (UDP/TCP:53)	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓	≡+	🗑️	✎
2	BRIDGE_BRO	WAN-Schnittstellen	dns (UDP/TCP:53)	Verweigern	<input checked="" type="checkbox"/> Aktiviert	↑↓	≡+	🗑️	✎

Abb. 97: Firewall->Richtlinien->IPv4-Filterregeln

Damit ist die Einrichtung des Webfilters mit zwei Internetzugängen abgeschlossen.

Möchten Sie mehrere unterschiedliche Filterprofile verwenden, so folgen Sie bitte den Anweisungen im Abschnitt [Ein zusätzliches Filterprofil einrichten](#) auf Seite 99.

8.9 Konfigurationsschritte im Überblick

Neuer DynDNS-Provider

Feld	Menü	Wert
Providername	Lokale Dienste ->DynDNS-Client ->DynDNS-Provider ->Neu	z. B. <i>Webfilter2</i>
Server	Lokale Dienste ->DynDNS-Client ->DynDNS-Provider ->Neu	z. B. <i>ddns2.flashstart.com</i>
Aktualisierungspfad	Lokale Dienste ->DynDNS-Client ->DynDNS-Provider ->Neu	z. B. <i>/nic/update</i>
Port	Lokale Dienste ->DynDNS-Client ->DynDNS-Provider ->Neu	z. B. <i>80</i>
Protokoll	Lokale Dienste ->DynDNS-Client ->DynDNS-Provider ->Neu	<i>DynDNS</i>
Aktualisierungsintervall	Lokale Dienste ->DynDNS-Client ->DynDNS-Provider ->Neu	<i>60</i> Sekunden
Homepage	Lokale Dienste ->DynDNS-Client ->DynDNS-Provider ->Neu	z. B. <i>https://webfilter.bintec-elmeg.com</i>

Einstellung im SNMP-Browser

Feld	Menü	Wert
ipDdnsName(*)	ip ->ipDynDnsProviderTable	<i>Webfilter2</i>
ipDdnsMinWait	ip ->ipDynDnsProviderTable	<i>60</i>
ipDdnsVerification	ip ->ipDynDnsProviderTable	<i>disabled</i>

Statische Routen zum DynDNS-Server anlegen

Feld	Menü	Wert
Routentyp	Netzwerk ->Routen ->Konfiguration von IPv4-Routen ->Neu	<i>Host-Route über Schnittstelle</i>
Schnittstelle	Netzwerk ->Routen ->Konfiguration von IPv4-Routen ->Neu	<i>WAN_GERMANY - TELEKOM BUSINESS</i>
Ziel-IP-Adresse/Netzmaske	Netzwerk ->Routen ->Konfiguration von IPv4-Routen ->Neu	<i>185.236.104.104</i>
Routentyp	Netzwerk ->Routen ->Konfiguration	<i>Host-Route über</i>

Feld	Menü	Wert
	von IPv4-Routen ->Neu	<i>Schnittstelle</i>
Schnittstelle	Netzwerk ->Routen ->Konfiguration von IPv4-Routen ->Neu	<i>WAN_TELEKOM2</i>
Ziel-IP-Adresse/Netzmaske	Netzwerk ->Routen ->Konfiguration von IPv4-Routen ->Neu	<i>185.236.104.114</i>

Neuen DynDNS-Client anlegen

Feld	Menü	Wert
Hostnamen	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	<i>wan1</i>
Schnittstelle	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	<i>Germany - Telekom Business</i>
Benutzername	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	Ihre E-Mail-Adresse
Passwort	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	Ihr Passwort
Provider	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	<i>z. B. webfilter</i>
Aktualisierung aktivieren	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	<i>Aktiviert</i>
Hostnamen	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	<i>wan2</i>
Schnittstelle	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	<i>Telekom2</i>
Benutzername	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	Ihre E-Mail-Adresse
Passwort	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	Ihr Passwort
Provider	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	<i>z. B. webfilter2</i>
Aktualisierung aktivieren	Lokale Dienste ->DynDNS-Client ->DynDNS-Aktualisierung ->Neu	<i>Aktiviert</i>

DNS Domänenweiterleitung einrichten

Feld	Menü	Wert
Weiterleiten	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	<i>Domäne</i>

Feld	Menü	Wert
Domäne	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	*
Weiterleiten an	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	<i>DNS-Server</i>
Quellschnittstelle	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	<i>BRIDGE_BR0</i>
Primärer DNS-Server (IPv4/IPv6)	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	z. B. <i>185.236.104.104</i>
Sekundärer DNS-Server (IPv4/IPv6)	Lokale Dienste ->DNS ->Domänenweiterleitung ->Neu	z. B. <i>185.236.105.105</i>

Firewall - Schnittstellengruppe anlegen

Feld	Menü	Wert
Beschreibung	Firewall ->Schnittstellen ->IPv4-Gruppen ->Neu	z. B. <i>WAN-Schnittstellen</i>
Mitglieder	Firewall ->Schnittstellen ->IPv4-Gruppen ->Neu	<i>WAN_GERMANY - TELEKOM BUSINESS</i> und <i>WAN_TELEKOM2</i>

Firewall-Regeln anlegen

Feld	Menü	Wert
Quelle	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>BRIDGE_BR0</i>
Ziel	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>LAN_LOCAL</i>
Dienst	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>dns</i>
Aktion	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>Zugriff</i>
Quelle	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>BRIDGE_BR0</i>
Ziel	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>WAN-Schnittstellen</i>
Dienst	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>dns</i>
Aktion	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>Verweigern</i>