

bintec Workshop
IPsec zwischen 2 Gateways mit Zertifikaten

Ziel und Zweck Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.funkwerk-ec.com.

Haftung Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für bintec-Gateways finden Sie unter www.funkwerk-ec.com.

Als Multiprotokollgateways bauen bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken bintec und das bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

Richtlinien und Normen bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

**Wie Sie Funkwerk Enterprise
Communications GmbH
erreichen**

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1	Einleitung	3
1.1	Szenario	3
1.2	Voraussetzungen	3
2	Konfiguration	5
2.1	Einstellungen	5
2.1.1	Configure Peer Parameter	5
2.1.2	Traffic List Settings	7
2.1.3	Interface IP Settings	8
2.1.4	IPSec Anpassungen	9
3	Kontrolle	13
3.1	Einstellungen im Menü Certificate and Key Management	14
3.1.1	Schlüssel und Request erstellen	14
3.1.2	Zertifikate importieren	17
3.1.3	Zertifikats Anpassungen	18
4	Ergebnis	21
4.1	Kontrolle	21
4.2	Konfigurationsschritte im Überblick	23

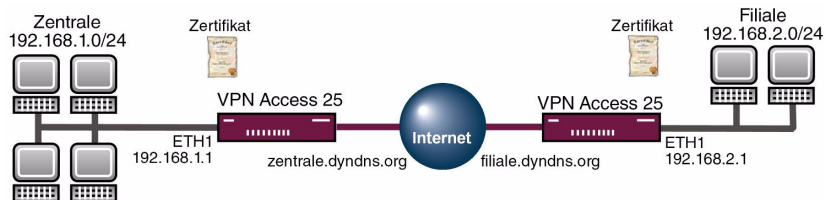
1 Einleitung

Im Folgenden wird die Konfiguration einer IPSec-Verbindung mit Zertifikaten beschrieben.

Die Zertifikate werden zur Authentifizierung genutzt. Die Anleitung zeigt einmal die Konfigurationsschritte für Traffic Lists und den Unterschied zu Interface-basierender Konfiguration. Diese Anleitung zeigt die Konfiguration auf Release 7.1.4 auf der Zentralseite.

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

1.1 Szenario



1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Gateways.
- Für das IPSec Gateway ist ein Bootimage ab Version 7.1.4 zu verwenden.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider.
- Auf beiden Gateways müssen Sie DynDNS oder eine statische IP-Adresse für den Internetzugang konfiguriert haben.

- Sie brauchen eine Zertifizierungsstelle, wo Sie Zertifikate anfordern können.
- Einen TFTP Server im Netzwerk.

2 Konfiguration

Die Anleitung konfiguriert ein Beispiel auf Seiten der Zentrale. Um IPsec zu konfigurieren, müssen Sie im folgenden Menü Einstellungen vornehmen:

HAUPTMENÜ → IPSEC

In dem Untermenü **CONFIGURE PEERS** haben Sie die Möglichkeit mit **APPEND** Verbindungspartner für IPsec hinzuzufügen.



Hinweis

Bei der Erstkonfiguration von IPsec startet der Wizard. Den sollten Sie ausführen, um Default Parameter für IPsec zu generieren. Um Fehler zu vermeiden, konfigurieren Sie als erstes eine Verbindung mit Preshared Key. Erst wenn diese funktioniert, setzen Sie Zertifikate ein.

2.1 Einstellungen

Einstellungen im Menü **IPSEC → CONFIGURE PEERS → APPEND**

2.1.1 Configure Peer Parameter

VPN Access 25 Setup Tool		BinTec Access Networks GmbH	
[IPSEC] [PEERS] [ADD]: Configure Peer		Zentrale	
Description:	Filiale	Oper Status:	down
Admin Status:	up		
Peer Address:	filiale.dyndns.org		
Peer IDs:	filiale		
Pre Shared Key:	bintec		
IPsec Callback >			
Peer specific Settings >			
Virtual Interface:	no		
Traffic List Settings >			
	SAVE		CANCEL
Enter string, max length = 255 chars			

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Geben Sie eine Beschreibung für die Verbindung an.
Peer Address	Hier geben Sie die Gateway IP-Adresse oder DynDNS Namen des Verbindungspartners ein.
Peer IDs	Hier tragen Sie eine Identifikation des Partners ein (in der Filiale unter LOCAL ID eingetragen).
Pre Shared Key	Das gemeinsame Passwort von beiden Gateways.
Virtual Interface	Bestimmen Sie hier, ob Sie Traffic List oder Interface Routing konfigurieren.
Traffic List Settings	Hier konfigurieren Sie die Traffic List Einträge (Virtual Interface steht auf: no).
Interface IP Settings	Hier konfigurieren Sie die Interface IP Einträge (Virtual Interface steht auf: yes).

Tabelle 2-1: Relevante Felder in **IPSEC → CONFIGURE PEERS → APPEND**

Gehen Sie folgendermaßen vor, um die Einstellungen im Peer vorzunehmen:

- Bei **DESCRIPTION** geben Sie *Filiale* an.
- Bei **PEER ADDRESS** geben Sie *filiale.dyndns.org* an.
- Bei **PEER IDs** geben Sie *filiale* an.
- Im **PRE SHARED KEY** tragen Sie *bintec* als Passwort ein.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Wenn Sie Ihre Verbindung mit Traffic List konfigurieren möchten, dann gehen Sie zu Abschnitt "[Traffic List Settings](#)" auf [Seite 7](#).

Wenn Sie Ihre Verbindung mit Interface Routing konfigurieren möchten, dann gehen Sie zu Abschnitt "[Interface IP Settings](#)" auf [Seite 8](#).

2.1.2 Traffic List Settings

- Gehen Sie zu **IPSEC → CONFIGURE PEERS → APPEND**.
- **VIRTUAL INTERFACE** belassen Sie auf *no*.
- Gehen Sie in das Untermenü **TRAFFIC LIST SETTINGS → APPEND**, um die Traffic List zu bearbeiten. (Sollten Sie den Wizard benutzen, verlassen Sie das Menü mit **SAVE**, um die Traffic List Einträge zu erstellen).

VPN Access 25 Setup Tool		BinTec Access Networks GmbH	
[IPSEC] [PEERS] [EDIT] [TRAFFIC] [EDIT]:Traffic Entry (Filiale)		Zentrale	
Description:	Filiale		
Protocol:	dont-verify		
Local:			
Type: net	Ip: 192.168.1.0	/	24
Remote:			
Type: net	Ip: 192.168.2.0	/	24
Action:	protect		
Profile	*autogenerated*	edit	>
	SAVE		CANCEL

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Geben Sie eine Beschreibung für den Eintrag an.
Local IP	Geben Sie hier das lokale Netz mit zugehöriger Subnetmask (in Bit) an.
Remote IP	Geben Sie hier das Remote Netz mit zugehöriger Subnetmask (in Bit) an.

Tabelle 2-2: Relevante Felder in **TRAFFIC LIST SETTINGS → APPEND**

Gehen Sie folgendermaßen vor, um Ihren Eintrag zu konfigurieren:

- Als **DESCRIPTION** geben Sie *Filiale* an.

- Unter **LOCAL IP** tragen Sie *192.168.1.0* mit der Mask *24* ein.
- Unter **REMOTE IP** tragen Sie *192.168.2.0* mit der Mask *24* ein.
- Speichern Sie mit **SAVE** ab.
- Verlassen Sie alle weiteren Menüs mit **Save** oder **Exit**, bis Sie sich im **IPSEC** Hauptmenü befinden. Konfigurieren Sie weiter ab Punkt [“IPSec Anpassungen” auf Seite 9](#).

2.1.3 Interface IP Settings

- Gehen Sie zu **IPSEC → CONFIGURE PEERS → APPEND**
- **VIRTUAL INTERFACE** stellen Sie auf *yes*.
- Gehen Sie in das Untermenü **INTERFACE IP SETTINGS → BASIC IP-SETTINGS**, um das Routing zu bearbeiten. (Sollten Sie den Wizard benutzen, verlassen Sie das Menü mit **SAVE**, um die Routingeinträge zu erstellen).

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[IPSEC] [PEERS] [EDIT] [IP] [BASIC]: IP-Settings (Filiale)	Zentrale
IP Transit Network	no
Local IP Address	192.168.1.1
Default Route	no
Remote IP Address	192.168.2.0
Remote Netmask	255.255.255.0
SAVE	CANCEL
Use <Space> to select	

Folgende Felder sind relevant:

Feld	Bedeutung
IP Transit Network	Bestimmen Sie hier, ob Sie ein Transitnetz nutzen möchten.
Local IP Address	Geben Sie hier Ihre lokale IP-Adresse von Ihrem Ethernet Interface an.
Remote IP Address	Hier konfigurieren Sie das zu erreichende Partner Netz.
Remote Netmask	Dies ist die Subnetzmaske, die zum Remote-netz gehört.

Tabelle 2-3: Relevante Felder in **INTERFACE IP SETTINGS** → **BASIC IP-SETTINGS**

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- **IP TRANSIT NETWORK** lassen Sie auf *no*.
- Unter **LOCAL IP ADDRESS** tragen Sie *192.168.1.1* ein.
- Unter **REMOTE IP ADDRESS** tragen Sie *192.168.2.0* ein.
- Die **REMOTE NETMASK** stellen Sie auf *255.255.255.0*
- Speichern Sie mit **SAVE** ab. Verlassen Sie alle weiteren Menüs mit **Save** oder **Exit**, bis Sie sich im **IPSEC** Hauptmenü befinden.

2.1.4 IPsec Anpassungen

In folgendem Untermenü können Sie PHASE 1 Vorlagen verändern oder neue Profile mit **ADD** hinzufügen.

- Gehen Sie zu **IPSEC** → **IKE (PHASE 1) DEFAULTS** → **EDIT**.

VPN Access 25 Setup Tool [IPSEC] [PHASE1] [EDIT]	BinTec Access Networks GmbH Zentrale
<pre> Description (Idx 1) : *autogenerated* Proposal : 19 (Rijndael/MD5) Lifetime : use default Group : 2 (1024 bit MODP) Authentication Method : Pre Shared Keys Mode : aggressiv Heartbeats : none Block Time : 0 Local ID : zentrale Local Certificate : none CA Certificates : Nat-Traversal : enabled View Proposals > Edit Lifetimes > SAVE CANCEL </pre>	
Enter string, max length = 255 chars	

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Geben Sie dem PHASE 1 Profil einen Namen.
Proposal	Mit diesem Algorithmus wird die PHASE 1 verschlüsselt.
Mode	Der Mode bestimmt die Methode des IKE Aufbaus.
Local ID	Hier tragen Sie die eigene Identifikation für das Gateway ein.

Tabelle 2-4: Relevante Felder in **IPSEC → IKE (PHASE 1) DEFAULTS → EDIT**

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die **PROPOSAL** stellen Sie auf *19 (Rijndael/MD5)*.
- Den **MODE** stellen Sie auf *aggressive*, da Sie dynamische IP-Adressen haben.
- Unter **LOCAL ID** geben Sie *zentrale* ein (Ihre Local ID steht beim Partner unter **PEER ID**).

In folgendem Untermenü können Sie PHASE 2 Vorlagen verändern oder neue Profile mit **ADD** hinzufügen:

- Gehen Sie zu **IPSEC → IPSEC (PHASE 2) DEFAULTS → EDIT**.

VPN Access 25 Setup Tool [IPSEC] [PHASE2] [EDIT]	BinTec Access Networks GmbH Zentrale
Description (Idx 1) : *autogenerated*	
Proposal	: 23 (ESP(Rijndael/MD5))
Lifetime	: use default
Use PFS	: none
Heartbeats	: both
Propagate PMTU	: no
View Proposals >	
Edit Lifetimes >	
SAVE	CANCEL
Enter string, max length = 255 chars	

Folgende Felder sind relevant:

Feld	Bedeutung
Proposal	Mit diesem Algorithmus wird die PHASE 2 verschlüsselt.
Heartbeats	Baut den Tunnel ab, wenn der Partner nicht mehr reagiert.

Tabelle 2-5: Relevante Felder in **IPSEC → IPSEC (PHASE 2) DEFAULTS → EDIT**

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Verändern Sie die **PROPOSAL** auf 23 (ESP(Rijndael/MD5)).
- Stellen Sie **HEARTBEATS** auf *both*.

3 Kontrolle

Um die IPSec Verbindung zu testen, gehen Sie wie folgt beschrieben vor:

- Geben Sie an der Shell des Gateways Folgendes ein:
ipsecGlobMaxSysLogLevel=debug.
- Danach starten Sie den Debug Modus mit *debug all&*.
- Geben Sie einen Ping von Ihrem Host in der Zentrale zum Host in der Filiale ab.

Jetzt sollten Sie folgende Meldungen erhalten:

```
04:30:58 INFO/IPSEC: New Bundle -40 (Peer 1 Traffic 2)
04:30:58 INFO/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): created
192.168.1.0/192.168.1.0:0 < any > 192.168.2.0/192.168.2.0:0 rekeyed 0
04:30:58 DEBUG/INET: dnsd: qry from 127.0.0.1:1064 id 75 "filiale.dyndns.org." A 1
04:30:58 DEBUG/INET: dnsd: cache 62.10.10.20 for filiale.dyndns.org.
04:30:58 DEBUG/INET: dnsd: rsp to 127.0.0.1:1064 id 75 "filiale.dyndns.org." A 1/0/0
04:30:59 DEBUG/INET: NAT: new outgoing session on ifc 300 prot 17
62.10.10.10:500/62.10.10.10:1023 -> 62.10.10.20:500
04:30:59 DEBUG/IPSEC: P1: peer 1 (62.10.10.20) sa 1 (I): identified ip 62.10.10.10 -> ip
62.10.10.20
04:30:59 INFO/IPSEC: P1: peer 1 (62.10.10.20) sa 1 (I): Vendor ID: 62.10.10.20:500
(fqdn(any:0,[0..6]=filiale)) is 'BINTEC'
04:30:59 INFO/IPSEC: P1: peer 1 (62.10.10.20) sa 1 (I): Vendor ID: 62.10.10.20:500
(fqdn(any:0,[0..6]=filiale)) is 'BINTEC Heartbeats Version 1'
04:30:59 INFO/IPSEC: P1: peer 1 (62.10.10.20) sa 1 (I): done id fqdn(any:0,[0..7]=zentrale) -> id
fqdn(any:0,[0..6]=filiale) AG[cf5ea38f 8aaa6e28 : 4ae27eda 3b7a0be7]
04:30:59 DEBUG/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): SA 1 established
ESP[2b342411] in[0] Mode tunnel enc blowfish-cbc(16) auth md5(16)
04:30:59 DEBUG/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): SA 2 established
ESP[43bfc201] out[0] Mode tunnel enc blowfish-cbc(16) auth md5(16)
04:30:59 INFO/IPSEC: Activate Bundle -40 (Peer 1 Traffic 2)
04:30:59 DEBUG/INET: NAT: new outgoing session on ifc 300 prot 50 62.10.10.10:0/62.10.10.10:0 ->
62.10.10.20:0
04:30:59 INFO/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): established (62.10.10.10<-
>62.10.10.20) with 2 SAs life 28800 Sec/0 Kb rekey 23040 Sec/0 Kb Hb none
04:30:59 DEBUG/INET: NAT: new incoming session on ifc 300 prot 50 62.10.10.10:0/62.10.10.10:0 <-
62.10.10.20:0
```

3.1 Einstellungen im Menü Certificate and Key Management

Um einen privaten und einen öffentlichen Schlüssel zu erstellen, den Sie für den Zertifikatsrequest brauchen, müssen Sie in folgendes Untermenü:

IPSEC → CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → CREATE

3.1.1 Schlüssel und Request erstellen

VPN Access 25 Setup Tool		BinTec Access Networks GmbH	
[IPSEC] [CERTMGMT] [KEYS] [CREATE]: IPsec Configuration -		Zentrale	
Create Keys			
Description:	key1		
Algorithm:	rsa		
Key Size (Bits):	1024		
RSA Public Exponent:	65537		
Create		Exit	
Enter string, max length = 255 chars			

Folgendes Feld ist relevant:

Feld	Bedeutung
Description	Geben Sie dem Schlüssel einen Namen.

Tabelle 3-6: Relevante Felder in **IPSEC → CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → CREATE**

Gehen Sie folgendermaßen vor, um die Einstellungen vorzunehmen:

- Unter **DESCRIPTION** geben Sie *key1* ein.
- Gehen Sie auf **Create**, um den Schlüssel zu erstellen (Die Erstellung kann einige Sekunden dauern).
- Verlassen Sie das Menü mit **Exit**.
- Gehen Sie in das Untermenü **REQUEST CERT.**

Zertifikatsanforderungen können Sie in diesem Menü erstellen:

IPSEC → CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[IPSEC]..[ENROLL]: IPsec Configuration - Certificate Enrollment	Zentrale
Key to enroll:	1 (key1)
Method:	Upload
Subject Name:	CN=Zentrale
Subject Alternative Names (optional):	
Type	Value
NONE	
NONE	
NONE	
Signing algorithm to use:	md5WithRSAEncryption
Server:	192.168.1.2
Filename:	Zentrale.req base64
Start	Exit

Folgende Felder sind relevant:

Feld	Bedeutung
Key to enroll	Geben Sie dem Schlüssel einen Namen.
Method	Hier wählen Sie automatische oder manuelle Anforderung.
Subject Name	Geben Sie Ihre Identifikation im X.500 Format an.
Subject Alternative Names	Hier können Sie weitere Identifikationen angeben.
Signing algorithm	Der Signaturalgorithmus.
Server	Die IP-Adresse von dem TFTP Server.
Filename	Der Dateiname des Requests.

Tabelle 3-7: Relevante Felder in **IPSEC → CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT**

Gehen Sie folgendermaßen vor, um Ihren Eintrag zu konfigurieren:

- Geben Sie bei **KEY TO ENROLL** Ihren gerade erstellten Schlüssel *key1* an.
- Die **METHOD** stellen Sie auf *Upload*.
- Als **SUBJECT NAME** schreiben Sie *CN=Zentrale*.
- Alle **SUBJECT ALTERNATIVE NAMES** stellen Sie auf *NONE*.
- Den **SIGNING ALGORITHM** belassen Sie auf *md5WithRSAEncryption*.
- Bei **SERVER** geben Sie die IP des TFTP Servers an *192.168.1.2*.
- Unter **FILENAME** geben Sie *Zentrale.req* an.

Jetzt müssen Sie mit dem Zertifikats Request bei einer Zertifizierungsstelle ein Zertifikat anfordern. Der Request sieht ungefähr so aus:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBUjCBvAIBADATMREwDwYDVQQDEwhaZW50cmFsZTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA6B8S00i9Zcn7AxKcs+a44Vh/Nr10nXQ6Xj0iknGmb4M1Vuw/
nqUn6YnCmlGJ1xFHrDTHa6dBa3Q/IVWd3ZL/dsGQcymB77JkKGVutySxu3nl6Oht
u7nUOZWjKfBuoZImJ4L/WaNxUM+/6bLpvMkc5WMnHrv8Ixot5sEVZU3Eu68CAwEA
AaAAMA0GCSqGSIb3DQEBAUAA4GBAAyXiDjkrOgyWjqZjnGrw/RZHRRGyArkLLjy
GwEn3VFG8iE0i2gclfsor61zyHtFNtuaMKRvHV9845Yp++0p6GnHJVgXBvs9jALL
FCz5j6C2TXyKovLhv4eYAKOCJX90OK7+fipt6wP3/LgvEquoqaJh3jwqEcxnjmrr
6Z5hMftE
-----END CERTIFICATE REQUEST-----
```

Das Zertifikat, welches die Zertifizierungsstelle ausstellt, müssen Sie nun in das Verzeichnis von dem TFTP Server kopieren. Benennen Sie das Zertifikat *Zentrale.crt*.

Sie brauchen noch das Zertifikat der Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Kopieren Sie auch das in das Verzeichnis von dem TFTP Server. Benennen Sie das Zertifikat *Ca.crt*. Danach gehen sie in folgendes Menü, um Ihr eigenes Zertifikat in das IPsec Gateway zu importieren:

IPSEC → CERTIFICATE AND KEY MANAGEMENT → OWN CERTIFICATES → DOWNLOAD

3.1.2 Zertifikate importieren

- Gehen Sie zu **IPSEC → CERTIFICATE AND KEY MANAGEMENT → OWN CERTIFICATES → DOWNLOAD**

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[IPSEC] [CERTMGMT] [OWN] [GETCERT]: IPsec Configuration -	Zentrale
Get Certificate	
Import a Certificate/CRL using: TFTP	
Type of certificate: Own Certificate	
Server: 192.168.1.2	
Name: Zentrale.crt	auto
START	EXIT

Folgende Felder sind relevant:

Feld	Bedeutung
Server	Hier geben Sie die IP-Adresse von dem TFTP Server an.
Name	Hier wird der Dateiname von dem Zertifikat eingetragen.

Tabelle 3-8: Relevante Felder in **IPSEC → CERTIFICATE AND KEY MANAGEMENT → OWN CERTIFICATES → DOWNLOAD**

Gehen Sie folgendermaßen vor, um Ihren Eintrag zu konfigurieren:

- Geben Sie bei **SERVER** *192.168.1.2* an.
- Bei **NAME** wird *Zentrale.crt* eingetragen.
- Gehen Sie auf **START**, um das Zertifikat zu importieren.
- Verlassen Sie die nächsten beiden Menüs mit **EXIT**.

Gehen sie in folgendes Menü, um das Zertifikat der Zertifizierungsstelle in das IPsec Gateway zu importieren:

IPSEC → CERTIFICATE AND KEY MANAGEMENT → CERTIFICATE AUTHORITY CERTIFICATES → DOWNLOAD

Das Importieren erfolgt genauso wie bei Ihrem eigenen Zertifikat. Nach dem Sie das Zertifikat der CA (*Ca.crt*) in das Gateway importiert haben, bearbeiten Sie es und stellen Sie den Punkt **TYPE OF CERTIFICATE** auf *Certificate Authority no CRLs*.



Hinweis

Sollten Sie CRL's verwenden wollen, müssen Sie noch die CRL Datei von der Zertifizierungsstelle in das VPN Gateway importieren.

3.1.3 Zertifikats Anpassungen

Um die zuvor mit Preshared Key konfigurierte Verbindung an Zertifikate anzupassen, müssen Sie in folgendes Menü gehen:

IPSEC → IKE (PHASE 1) DEFAULTS → EDIT

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[IPSEC] [PHASE1] [EDIT]	Zentrale
Description (Idx 1) : *autogenerated* Proposal : 19 (Rijndael/MD5) Lifetime : use default Group : 2 (1024 bit MODP) Authentication Method : RSA Signatures Mode : id_protect Heartbeats : both Block Time : 0 Local ID : <CN=Zentrale> Local Certificate : 1 (Zentrale.crt) CA Certificates : Nat-Traversal : enabled View Proposals > Edit Lifetimes >	
SAVE	CANCEL

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Geben Sie dem PHASE 1 Profil einen Namen.
Proposal	Mit diesem Algorithmus wird die PHASE 1 verschlüsselt.
Authentication Method	Hier wählen Sie die Authentifizierungsmethode.
Mode	Der Mode bestimmt die Methode des IKE Aufbaus.
Heartbeats	Überprüft den VPN Partner auf Erreichbarkeit.
Local ID	Hier tragen Sie die eigene Identifikation für das Gateway ein.
Local Certificate	Hier wählen Sie das eigene Zertifikat aus.

Tabelle 3-9: Relevante Felder in **IPSEC → IKE (PHASE 1) DEFAULTS → EDIT**

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die **PROPOSAL** stellen Sie auf *19 (Rijndael/MD5)*.
- **AUTHENTICATION METHOD** stellen Sie auf *RSA Signatures*.
- Den **MODE** stellen Sie zurück auf *id_protect*, da Sie Zertifikate einsetzen.
- **HEARTBEATS** schalten Sie auf *both*.
- Unter **LOCAL ID** geben Sie *<CN=Zentrale>* ein. Das ist Ihr Subject Name von dem Zertifikat.
- Bei **LOCAL CERTIFICATE** wählen Sie Ihr eigenes Zertifikat aus *1(Zentrale.crt)*.
- **NAT-TRAVERSAL** stellen Sie auf *disabled*.

Jetzt müssen Sie noch eine Anpassung in folgendem Menü machen:

IPSEC → CONFIGURE PEERS → EDIT

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[IPSEC] [PEERS] [EDIT]: Configure Peer	Zentrale
Description: filiale Admin Status: up Oper Status: up Peer Address: filiale.dyndns.org Peer IDs: <CN=Filiale>	
IPSec Callback > Peer specific Settings >	
Virtual Interface: no Traffic List Settings >	
SAVE	CANCEL
Enter string, max length = 255 chars	

Verändern Sie folgendes Feld mit den angegebenen Werten:

Feld	Wert
Peer IDs	Hier tragen Sie den Subject Name des IPSec Partners ein, der im Zertifikat steht: <CN=Filiale>.

4 Ergebnis

Sie haben eine IPSec-Verbindung mit Zertifikaten zwischen 2 Gateways konfiguriert. Dazu haben Sie dynamische IP-Adressen in Kombination mit DynDNS auf Seiten des Providers verwendet. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter auf der Filialseite konfigurieren.

4.1 Kontrolle

Um die IPSec Verbindung zu testen, gehen Sie wie folgt beschrieben vor:

- Geben Sie an der Shell des Gateways folgendes ein:
`ipsecGlobMaxSysLogLevel=debug.`
- Danach starten Sie den Debug Modus mit `debug all&`.
- Geben Sie einen Ping von Ihrem Host in der Zentrale zum Host in der Filiale ab.

Jetzt sollten Sie folgende Meldungen erhalten:

```

14:24:39 INFO/IPSEC: New Bundle -253 (Peer 1 Traffic 2)
14:24:39 INFO/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): created
192.168.1.0/192.168.1.0:0 < any > 192.168.2.0/192.168.2.0:0 rekeyed 0
14:24:39 DEBUG/IPSEC: P1: peer 1 (filiale) sa 1 (I): identified ip 62.10.10.10 -> ip 62.10.10.20
14:24:39 INFO/IPSEC: P1: peer 1 (filiale) sa 1 (I): Vendor ID: 62.10.10.20:500 (No Id) is 'BIN-
TEC'
14:24:39 INFO/IPSEC: P1: peer 1 (filiale) sa 1 (I): Vendor ID: 62.10.10.20:500 (No Id) is 'BINTEC
Heartbeats Version 1'
14:24:40 INFO/IPSEC: P1: peer 1 (filiale) sa 1 (I): done id der_asn1_dn(any:0,[0..20]=CN=Zen-
trale) -> id der_asn1_dn(any:0,[0..19]=CN=Filiale) IP[828c005d ecf69620 : cbffd735 3a37ec50]
14:24:40 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): SA 1 established
IPComp[00000002] in[1] Mode tunnel comp deflate
14:24:40 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): SA 2 established
IPComp[00000002] out[1] Mode tunnel comp deflate
14:24:40 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): SA 3 established ESP[153b2914]
in[0] Mode transport enc rijndael-cbc(16) auth md5(16)
14:24:40 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): SA 4 established ESP[5b3e75c2]
out[0] Mode transport enc rijndael-cbc(16) auth md5(16)
14:24:40 INFO/IPSEC: Activate Bundle -253 (Peer 1 Traffic 2)
14:24:40 DEBUG/INET: NAT: new outgoing session on ifc 300 prot 50 62.10.10.10:0/62.10.10.10:0 ->
62.10.10.20:0
14:24:40 INFO/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): established (62.10.10.10<-
>62.10.10.20) with 4 SAs life 28800 Sec/0 Kb rekey 23040 Sec/0 Kb Hb both
14:24:40 DEBUG/INET: NAT: new incoming session on ifc 300 prot 50 62.10.10.10:0/62.10.10.10:0 <-
62.10.10.20:0

```



Hinweis

Beachten Sie bitte, dass IPSec-Verbindungen mit Zertifikaten nicht zustande kommen, wenn das Datum und die Zeit nicht richtig sind. Daher überprüfen Sie vor jeder Konfiguration das eingestellte Datum auf beiden IPSec Gateways.

4.2 Konfigurationsschritte im Überblick

Configure Peer

Feld	Menü	Wert
Description	CONFIGURE PEERS → APPEND	z.B. <i>Filiale</i>
Peer Address	CONFIGURE PEERS → APPEND	z.B. <i>filiale.dyndns.org</i>
Peer IDs	CONFIGURE PEERS → APPEND	z.B. <i><CN=Filiale></i>

Traffic List

Feld	Menü	Wert
Description	CONFIGURE PEERS → TRAFFIC LIST SETTINGS → APPEND	z.B. <i>Filiale</i>
Local IP	CONFIGURE PEERS → TRAFFIC LIST SETTINGS → APPEND	z.B. <i>192.168.1.0 /24</i>
Remote IP	CONFIGURE PEERS → TRAFFIC LIST SETTINGS → APPEND	z.B. <i>192.168.2.0 /24</i>

IP Routing

Feld	Menü	Wert
IP Transit Network	CONFIGURE PEERS → INTERFACE IP SETTINGS → BASIC IP	<i>no</i>
Local IP Address	CONFIGURE PEERS → INTERFACE IP SETTINGS → BASIC IP	z.B. <i>192.168.1.1</i>
Remote IP Address	CONFIGURE PEERS → INTERFACE IP SETTINGS → BASIC IP	z.B. <i>192.168.2.0</i>
Remote Netmask	CONFIGURE PEERS → INTERFACE IP SETTINGS → BASIC IP	z.B. <i>255.255.255.0</i>

Phase 1

Feld	Menü	Wert
Proposal	<i>IKE (PHASE 1) DEFAULTS → EDIT → ADD</i>	z.B. 19 (Rijndael/MD5)
Authentication Method	<i>IKE (PHASE 1) DEFAULTS → EDIT → ADD</i>	<i>RSA Signatures</i>
Mode	<i>IKE (PHASE 1) DEFAULTS → EDIT → ADD</i>	<i>id_protect</i>
Heartbeats	<i>IKE (PHASE 1) DEFAULTS → EDIT → ADD</i>	<i>both</i>
Local ID	<i>IKE (PHASE 1) DEFAULTS → EDIT → ADD</i>	z.B. <CN=Zentrale>
Local Certificate	<i>IKE (PHASE 1) DEFAULTS → EDIT → ADD</i>	z.B. 1 (Zentrale.crt)

Phase 2

Feld	Menü	Wert
Proposal	<i>IPSEC (PHASE 2) DEFAULTS → EDIT → ADD</i>	z.B. 23 (ESP(Rijndael/MD5))
Heartbeats	<i>IPSEC (PHASE 2) DEFAULTS → EDIT → ADD</i>	<i>both</i>

Zertifikate

Feld	Menü	Wert
Description	<i>CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → CREATE</i>	z.B. key1
Key to enroll	<i>CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT</i>	z.B. key1
Method	<i>CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT</i>	<i>Upload</i>
Subject Name	<i>CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT</i>	z.B. CN=Zentrale
Subject Alternative Names	<i>CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT</i>	<i>NONE</i>

Feld	Menü	Wert
Signing algorithm	CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT	z.B. <i>md5WithRSAEncryption</i>
Server	CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT	z.B. 192.168.1.2
Filename	CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT	z.B. <i>Zentrale.req</i>
Server	CERTIFICATE AND KEY MANAGEMENT → OWN CERTIFICATES → DOWNLOAD	z.B. 192.168.1.2
Name	CERTIFICATE AND KEY MANAGEMENT → OWN CERTIFICATES → DOWNLOAD	z.B. <i>Zentrale.crt</i>
Server	CERTIFICATE AND KEY MANAGEMENT → CERTIFICATE AUTHORITY CERTIFICATES → DOWNLOAD	z.B. 192.168.1.2
Name	CERTIFICATE AND KEY MANAGEMENT → CERTIFICATE AUTHORITY CERTIFICATES → DOWNLOAD	z.B. <i>Ca.crt</i>
Type of certificate	CERTIFICATE AND KEY MANAGEMENT → CERTIFICATE AUTHORITY CERTIFICATES → EDIT	<i>Certificate Authority no CRLs</i>

