funkwerk
enterprise communications

bintec Workshop

IPsec between 2 Gateways with Certificates

Version 0.9

Purpose

This document is part of the user's guide to the installation and configuration of bintec gateways running software release 7.1.4 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our **Release Notes**, especially when carrying out a software update to a later release level. The latest **Release Notes** can be found at www.funkwerk-ec.com.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, changes and **Release Notes** for bintec gateways can be found at www.funkwerk-ec.com.

As multiprotocol gateways, bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

bintec and the bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

Guidelines and standards

bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.funkwerk-ec.com.

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +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 France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

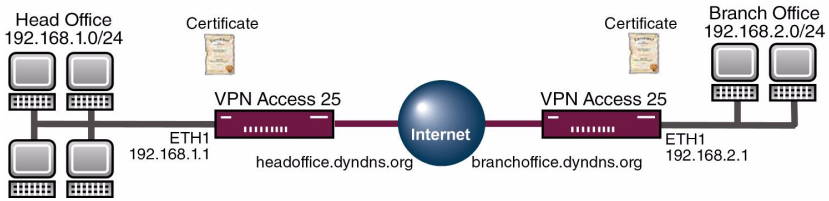
1 Introduction

The configuration of an IPSec connection with certificates is described in the following chapters.

The certificates are used for authentication. The instructions first show the configuration steps for traffic lists and the difference over interface-based configuration. These instructions show the configuration to Release 7.1.4 on the head office side.

The Setup Tool is used for the configuration.

1.1 Scenario



1.2 Requirements

The following are required for the configuration:

- Basic configuration of the gateway.
- A boot image of version 7.1.4 or later must be used for the IPSec gateway.
- A working Internet access to the provider.
- You must have configured DynDNS or a static IP address for the Internet access at both gateways.

- You need a certification authority (CA) from which you can request certificates.
- A TFTP server in the network.

2 Configuration

The instructions cover the configuration of an example on the head office side. You must make settings in the following menu for configuring IPSec:

MAIN MENU ➜ IPSEC

The ***CONFIGURE PEERS*** submenu offers you the **APPEND** option for adding connection partners for IPSec.

Note

The Wizard starts for the initial configuration of IPSec. You should execute this to generate default parameters for IPSec. To avoid errors, first configure a connection with preshared key. Do not use certificates until this connection works.

2.1 Settings

Settings in the ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND*** menu

2.1.1 Configure Peer Parameters

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PEERS][ADD]: Configure Peer                          Head Office

     Description:       branch office
     Admin Status:      up        Oper Status:   down

     Peer Address:      branchoffice.dyndns.org
     Peer IDs:          branch office
     Pre Shared Key:    bintec

     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: no
     Traffic List Settings >



                           SAVE                              CANCEL

Enter string, max. length = 255 chars
```

The following fields are relevant:

Field	Meaning
Description	Enter a description for the connection.
Peer Address	Enter the gateway IP address or DynDNS name of the connection partner.
Peer IDs	For entering an identification for the partner (entered in the branch office under ***LOCAL ID***).
Pre Shared Key	The password shared by the two gateways.
Virtual Interface	Here you determine if you configure a traffic list or interface routing.
Traffic List Settings	For configuring the traffic list entries (virtual interface set to: no).
Interface IP Settings	For configuring the interface IP entries (virtual interface set to: yes).

Table 2-1: Relevant fields in ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***

Proceed as follows to make the settings in the peer:

- Enter *branch office* for ***DESCRIPTION***.
- Enter *branchoffice.dyndns.org* for ***PEER ADDRESS***.
- Enter *branch office* for ***PEER IDS***.
- Enter *bintec* as password in ***PRE SHARED KEY***.
- Press **SAVE** to confirm your settings.

If you wish to configure your connection with a traffic list, go to the section “Traffic List Settings” on page 7.

If you wish to configure your connection with interface routing, go to the section “Interface IP Settings” on page 8.

2.1.2 Traffic List Settings

- Go to ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***.
- Leave ***VIRTUAL INTERFACE*** set to *no*.
- Go to the ***TRAFFIC LIST SETTINGS*** ➜ ***APPEND*** submenu to edit the traffic list. (If you use the Wizard, press **SAVE** to exit the menu to create traffic list entries).

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][TRAFFIC][EDIT]:Traffic Entry (Branch Office) Head
Office

     Description:   branch office

     Protocol:      don't 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
```

The following fields are relevant:

Field	Meaning
Description	Enter a description for the entry.
Local IP	Enter the local network with associated subnetmask (in bits).
Remote IP	Enter the remote network with associated subnetmask (in bits).

Table 2-2: Relevant fields in ***TRAFFIC LIST SETTINGS*** ➜ ***APPEND***

Proceed as follows to configure your entry:

- Set ***DESCRIPTION*** to *branch office*.
- Under ***LOCAL IP*** enter *192.168.1.0* with mask *24*.
- Under ***REMOTE IP*** enter *192.168.2.0* with mask *24*.
- Press **SAVE** to confirm.
- Exit all other menus with **Save** or **Exit** until the ***IPSEC*** main menu opens. Continue the configuration from "IPSec Changes" on page 9 onwards.

2.1.3 Interface IP Settings

- Go to ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***.
- Set ***VIRTUAL INTERFACE*** to *yes*.
- Go to the ***INTERFACE IP SETTINGS*** ➜ ***BASIC IP SETTINGS*** submenu to edit the routing. (If you use the Wizard, press **SAVE** to exit the menu to create routing entries).

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][IP][BASIC]: IP Settings (Branch Office)  Head
Office

  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
```

The following fields are relevant:

Field	Meaning
IP Transit Network	For selecting whether you use a transit network.
Local IP Address	Enter the local IP address of your Ethernet interface.
Remote IP Address	For configuring the partner network to be reached.
Remote Netmask	This is the subnetmask belonging to the remote network.

Table 2-3: Relevant fields in ***INTERFACE IP SETTINGS ➜ BASIC IP SETTINGS***

Proceed as follows to configure the entry:

- Leave ***IP TRANSIT NETWORK*** set to *no*.
- Enter an address under ***LOCAL IP ADDRESS***, e.g. *192.168.1.1*.
- Enter *192.168.2.0* under ***REMOTE IP ADDRESS***.
- Set ***REMOTE NETMASK*** to *255.255.255.0*.
- Press **SAVE** to confirm. Exit all other menus with **Save** or **Exit** until the ***IPSEC*** main menu opens.

2.1.4 IPSec Changes

You can change PHASE 1 defaults or add new profiles with ***ADD*** in the following submenu.

- Go to ***IPSEC ➜ IKE (PHASE 1) DEFAULTS ➜ EDIT***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PHASE1][EDIT]                                        Head Office

   Description (Idx 1) :    *autogenerated*
   Proposal            :  19 (Rijndael/MD5)
   Lifetime            :  use default
   Group               :  2 (1024-bit MODP)
   Authentication Method :  Pre Shared Keys
   Mode                :  aggressive
   Heartbeats          :  none
   Block Time          :  0
   Local ID            :  Head Office
   Local Certificate   :  none
   CA Certificates     :
   Nat Traversal       :  enabled

   View Proposals >
   Edit Lifetimes >

                          SAVE                          CANCEL

Enter string, max. length = 255 chars
```

The following fields are relevant:

Field	Meaning
Description	Give the PHASE 1 profile a name.
Proposal	PHASE 1 is encrypted with this algorithm.
Mode	The mode determines the IKE setup method.
Local ID	For entering the local identification of the gateway.

Table 2-4: Relevant fields in ***IPSEC*** ➜ ***IKE (PHASE 1) DEFAULTS*** ➜ ***EDIT***

Configure the defaults with the following parameters:

- Set ***PROPOSAL*** to *19 (Rijndael/MD5)*.
- Set ***MODE*** to *aggressive*, as you have dynamic IP addresses.
- Enter *head office* under ***LOCAL ID*** (your local ID is set under ***PEER ID*** at the partner).

You can change PHASE 2 defaults or add new profiles with ***ADD*** in the following submenu:

- Go to ***IPSEC*** ➜ ***IPSEC (PHASE 2) DEFAULTS*** ➜ ***EDIT***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PHASE2][EDIT]                                       Head Office

   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
```

The following fields are relevant:

Field	Meaning
Proposal	PHASE 2 is encrypted with this algorithm.
Heartbeats	Clears the tunnel if the partner no longer responds.

Table 2-5: Relevant fields in ***IPSEC*** ➜ ***IPSEC (PHASE 2) DEFAULTS*** ➜ ***EDIT***

Configure the defaults with the following parameters:

- Change ***PROPOSAL*** to *23 (ESP(Rijndael/MD5))*.
- Set ***HEARTBEATS*** to *both*.

3 Checking the Connection

Proceed as follows to check the IPSec connection:

- Enter the following in the shell of the gateway:
  `ipsecGlobMaxSysLogLevel=debug`.
- Then start the debug mode with *debug all&*.
- Send a ping from your host at the head office to the host at the branch office.

You should now receive the following messages:

```
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 "branchoffice.dyndns.org." A 1
04:30:58 DEBUG/INET: dnsd: cache 62.10.10.20 for branchoffice.dyndns.org.
04:30:58 DEBUG/INET: dnsd: rsp to 127.0.0.1:1064 id 75 "branchoffice.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]=branchoffice)) 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]=branchoffice)) 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]=headoffice) ->
id fqdn(any:0,[0..6]=branchoffice) 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 Settings in Certificate and Key Management Menu

You must open the following menu to create a private and public key, which you need for the certificate request:

IPSEC ➜ CERTIFICATE AND KEY MANAGEMENT ➜ KEY MANAGEMENT ➜ CREATE

3.1.1 Creating Key and Request

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][CERTMGMT][KEYS][CREATE]: IPsec Configuration -    Head Office
                                 Create Keys

     Description:           key1
     Algorithm:             rsa
     Key Size (Bits):       1024
     RSA Public Exponent:   65537


                    Create                                  Exit

Enter string, max. length = 255 chars
```

The following field is relevant:

Field	Meaning
Description	Give the key a name.

Table 3-1: Relevant fields in ***IPSEC ➜ CERTIFICATE AND KEY MANAGEMENT ➜ KEY MANAGEMENT ➜ CREATE***

Proceed as follows to make the settings:

- Enter *key1* under ***DESCRIPTION***.
- Go to **Create** to create the key (this setting can take a few seconds).
- Leave the menu with **Exit**.
- Go to the **REQUEST CERT** submenu.

You can create certificate requests in this menu:

IPSEC ➜ CERTIFICATE AND KEY MANAGEMENT ➜ KEY MANAGEMENT ➜ REQUEST CERT

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC]..[ENROLL]: IPsec Configuration -           Head Office
                   Certificate Enrollment

     Key to enroll:              1 (key1)

     Method:       Upload

     Subject Name: CN=Head Office

     Subject Alternative Names (optional):
       Type   Value
       NONE
       NONE
       NONE

     Signing algorithm to use:   md5WithRSAEncryption
     Server:   192.168.1.2
     Filename: headoffice.req                                  base64

               Start                                 Exit
```

The following fields are relevant:

Field	Meaning
Key to enroll	Give the key a name.
Method	Select automatic or manual request.
Subject Name	Enter your identification in X.500 format.
Subject Alternative Names	Here you can enter more IDs.
Signing algorithm	The signature algorithm.
Server	The IP address of the TFTP server.
Filename	The file name of the request.

Table 3-2: Relevant fields in ***IPSEC ➜ CERTIFICATE AND KEY MANAGEMENT ➜ KEY MANAGEMENT ➜ REQUEST CERT***

Proceed as follows to configure your entry:

- Enter the key you have just created *key1* for ***KEY TO ENROLL***.
- Set ***METHOD*** to *Upload*.
- Enter *CN=Head Office* as ***SUBJECT NAME***.
- Set all ***SUBJECT ALTERNATIVE NAMES*** to *NONE*.
- Leave the ***SIGNING ALGORITHM*** set to *md5WithRSAEncryption*.
- Enter the IP of the TFTP server *192.168.1.2* for ***SERVER***.
- Enter *headoffice.req* under ***FILENAME***.

Now you must request a certificate from a certification authority using the certificate request. The request is similar to the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBUjCBvAIBADATMREwDwYDVQQDEwhaZW50cmFsZTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA6B8S00i9Zcn7AxKcs+a44Vh/Nr10nXQ6XjOiknGmb4M1Vuw/
nqUn6YnCmlGJ1xFHrDTHa6dBa3Q/IVWd3ZL/dsGQcymB77JkKGVutySxu3nl6OHt
u7nUOZWjKfBuoZImJ4L/WaNxUM+/6bLpvMkc5WMnHrv8Ixot5sEVZU3Eu68CAwEA
AaAAMA0GCSqGSIb3DQEBBAUAA4GBAAyXiDjkrOgyWjqZjnGrw/RZHRrGyArkLLjy
GwEn3VFG8iE0i2gclfsor61zyHtFNtuaMKRvHV9845Yp++0p6GnHJVgXBvs9jALL
FCz5j6C2TXyKoVLhv4eYAKOCJX9OOK7+fipt6wP3/LgvEquoqaJh3jwqEcxnjmrr
6Z5hMFtE
-----END CERTIFICATE REQUEST-----
```

You must now copy the certificate issued by the certification authority into the directory of the TFTP server. Name the certificate *headoffice.crt*.

You still need the certificate of the certification authority that issued the certificate, which you must also copy into the directory of the TFTP server. Name the certificate *Ca.crt*. Now go the following menu to import your own certificate into the IPSec gateway:

IPSEC ➜ CERTIFICATE AND KEY MANAGEMENT ➜ OWN CERTIFICATES ➜ DOWNLOAD

3.1.2 Importing Certificates

- Go to ***IPSEC*** ➜ ***CERTIFICATE AND KEY MANAGEMENT*** ➜ ***OWN CERTIFICATES*** ➜ ***DOWNLOAD***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][CERTMGMT][OWN][GETCERT]: IPsec Configuration -     Head Office
                                 Get Certificate

     Import a Certificate/CRL using:  TFTP

     Type of certificate: Own Certificate



     Server:   192.168.1.2
     Name:     headoffice.crt                                  auto

             START                                  EXIT
```

The following fields are relevant:

Field	Meaning
Server	Enter the IP address of the TFTP server.
Name	For entering the file name of the certificate.

Table 3-3: Relevant fields in ***IPSEC*** ➜ ***CERTIFICATE AND KEY MANAGEMENT*** ➜ ***OWN CERTIFICATES*** ➜ ***DOWNLOAD***

Proceed as follows to configure your entry:

- Enter *192.168.1.2* for ***SERVER***.
- Enter *headoffice.crt* for ***NAME***.
- Go to **START** to import the certificate.
- Leave the next two menus with **EXIT**.

Go the following menu to import the certificate of the certification authority into the IPSec gateway:

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

The certificate is imported in exactly the same way as your own certificate. After you have imported the certificate of the CA (*Ca.crt*) into the gateway, edit it and set ***TYPE OF CERTIFICATE*** to *Certificate Authority no CRLs*.

Hinweis

If you wish to use CRLs, you must also import the CRL file of the certification authority into the VPN gateway.

3.1.3 Adapting Certificates

To adapt the connection previously configured with a preshared key to certificates, you must go to the following menu:

IPSEC ➜ IKE (PHASE 1) DEFAULTS ➜ EDIT

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PHASE1][EDIT]                                       Head Office

   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=Head Office>
   Local Certificate    :  1 (headoffice.crt)
   CA Certificates      :
   Nat Traversal        :  enabled

   View Proposals >
   Edit Lifetimes >

                         SAVE                          CANCEL
```

The following fields are relevant:

Field	Meaning
Description	Give the PHASE 1 profile a name.
Proposal	PHASE 1 is encrypted with this algorithm.
Authentication Method	For selecting the authentication method.
Mode	The mode determines the IKE setup method.
Heartbeats	Checks the VPN partner for reachability.
Local ID	For entering the local identification of the gateway.
Local Certificate	Here you select your own certificate.

Table 3-4: Relevant fields in ***IPSEC ➜ IKE (PHASE 1) DEFAULTS ➜ EDIT***

Configure the defaults with the following parameters:

- Set ***PROPOSAL*** to *19 (Rijndael/MD5)*.
- Set ***AUTHENTICATION METHOD*** to *RSA Signatures*.
- Restore ***MODE*** to *id_protect*, as you are using certificates.
- Set ***HEARTBEATS*** to *both*.
- Enter *<CN=Head Office>* under ***LOCAL ID***. This is your subject name from the certificate.
- For ***LOCAL CERTIFICATE*** select your own certificate *1(headoffice.crt)*.
- Set ***NAT TRAVERSAL*** to *disabled*.

Now you must make a change in the following menu:

IPSEC ➜ CONFIGURE PEERS ➜ EDIT

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT]: Configure Peer              Head Office

     Description:       branch office
     Admin Status:      up        Oper Status:   up

     Peer Address:      branchoffice.dyndns.org
     Peer IDs:          <CN=Branch Office>


     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: no
     Traffic List Settings >



                          SAVE                          CANCEL

Enter string, max. length = 255 chars
```

Change the following field with the indicated values:

Field	Description
Peer IDs	Here you enter the subject name of the IPSec partner stated in the certificate: *<CN=Branch Office>*.

4 Result

You have configured an IPSec connection with certificates between 2 gateways, using dynamic IP addresses in combination with DynDNS on the provider's side. As the instructions only show the example on the head office side, you must also configure the connection parameters on the branch office side.

4.1 Checking the Connection

Proceed as follows to check the IPSec connection:

- Enter the following in the shell of the gateway: `ipsecGlobMaxSysLogLevel=debug`.
- Then start the debug mode with `debug all&`.
- Send a ping from your host at the head office to the host at the branch office.

You should now receive the following messages:

```
14:24:39 INFO/IPSEC: New Bundle -253 (Peer 1 Traffic 2)
14:24:39 INFO/IPSEC: P2: peer 1 (branchoffice) 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 (branchoffice) sa 1 (I): identified ip 62.10.10.10 -> ip
62.10.10.20
14:24:39 INFO/IPSEC: P1: peer 1 (branchoffice) sa 1 (I): Vendor ID: 62.10.10.20:500 (No Id) is
'BINTEC'
14:24:39 INFO/IPSEC: P1: peer 1 (branchoffice) 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 (branchoffice) sa 1 (I): done id
der_asn1_dn(any:0,[0..20]=CN=Head Office) -> id der_asn1_dn(any:0,[0..19]=CN=Branch Office)
IP[828c005d ecf69620 : cbffd735 3a37ec50]
14:24:40 DEBUG/IPSEC: P2: peer 1 (branchoffice) traf 2 bundle -253 (I): SA 1 established
IPComP[00000002] in[1] Mode tunnel comp deflate
14:24:40 DEBUG/IPSEC: P2: peer 1 (branchoffice) traf 2 bundle -253 (I): SA 2 established
IPComP[00000002] out[1] Mode tunnel comp deflate
14:24:40 DEBUG/IPSEC: P2: peer 1 (branchoffice) 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 (branchoffice) 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 (branchoffice) 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
```

Note

Please note that IPSec connections with certificates cannot be set up if the date and time are not correct. You should therefore check the date set on both IPSec gateways before every configuration.

4.2 Overview of Configuration Steps

Configure Peer

Field	Menu	Description
Description	***CONFIGURE PEERS ➜ APPEND***	e.g. *branch office*
Peer Address	***CONFIGURE PEERS ➜ APPEND***	e.g. *branchoffice.dyndns.org*
Peer IDs	***CONFIGURE PEERS ➜ APPEND***	e.g. *<CN=Branch Office>*

Traffic List

Field	Menu	Description
Description	***CONFIGURE PEERS ➜ TRAFFIC LIST SETTINGS ➜ APPEND***	e.g. *branch office*
Local IP	***CONFIGURE PEERS ➜ TRAFFIC LIST SETTINGS ➜ APPEND***	e.g. *192.168.1.0 /24*
Remote IP	***CONFIGURE PEERS ➜ TRAFFIC LIST SETTINGS ➜ APPEND***	e.g. *192.168.2.0 /24*

IP Routing

Field	Menu	Description
IP Transit Network	***CONFIGURE PEERS ➜ INTERFACE IP SETTINGS ➜ BASIC IP***	*no*
Local IP Address	***CONFIGURE PEERS ➜ INTERFACE IP SETTINGS ➜ BASIC IP***	e.g. *192.168.1.1*
Remote IP Address	***CONFIGURE PEERS ➜ INTERFACE IP SETTINGS ➜ BASIC IP***	e.g. *192.168.2.0*

Field	Menu	Description
Remote Netmask	***CONFIGURE PEERS ➜ INTERFACE IP SETTINGS ➜ BASIC IP***	e.g. *255.255.255.0*

Phase 1

Field	Menu	Description
Proposal	***IKE (PHASE 1) DEFAULTS ➜ EDIT ➜ ADD***	e.g. *19 (Rijndael/MD5)*
Authentication Method	***IKE (PHASE 1) DEFAULTS ➜ EDIT ➜ ADD***	*RSA Signatures*
Mode	***IKE (PHASE 1) DEFAULTS ➜ EDIT ➜ ADD***	*id_protect*
Heartbeats	***IKE (PHASE 1) DEFAULTS ➜ EDIT ➜ ADD***	*both*
Local ID	***IKE (PHASE 1) DEFAULTS ➜ EDIT ➜ ADD***	e.g. *<CN=Head Office>*
Local Certificate	***IKE (PHASE 1) DEFAULTS ➜ EDIT ➜ ADD***	e.g. *1 (headoffice.crt)*

Phase 2

Field	Menu	Description
Proposal	***IPSEC (PHASE 2) DEFAULTS ➜ EDIT ➜ ADD***	e.g. *23 (ESP(Rijndael/MD5))*
Heartbeats	***IPSEC (PHASE 2) DEFAULTS ➜ EDIT ➜ ADD***	*both*

Certificates

Field	Menu	Description
Description	***CERTIFICATE AND KEY MANAGEMENT ➜ KEY MANAGEMENT ➜ CREATE***	e.g. *key1*
Key to enroll	***CERTIFICATE AND KEY MANAGEMENT ➜ KEY MANAGEMENT ➜ REQUEST CERT***	e.g. *key1*

Field	Menu	Description
Method	***Certificate and Key Management ➜ Key Management ➜ REQUEST CERT***	*Upload*
Subject Name	***Certificate and Key Management ➜ Key Management ➜ REQUEST CERT***	e.g. *CN=Head Office*
Subject Alternative Names	***Certificate and Key Management ➜ Key Management ➜ REQUEST CERT***	*NONE*
Signing algorithm	***Certificate and Key Management ➜ Key Management ➜ REQUEST CERT***	e.g. *md5WithRSAEncryption*
Server	***Certificate and Key Management ➜ Key Management ➜ REQUEST CERT***	e.g. *192.168.1.2*
Filename	***Certificate and Key Management ➜ Key Management ➜ REQUEST CERT***	e.g. *headoffice.req*
Server	***Certificate and Key Management ➜ Own Certificates ➜ DOWNLOAD***	e.g. *192.168.1.2*
Name	***Certificate and Key Management ➜ Own Certificates ➜ DOWNLOAD***	e.g. *headoffice.crt*
Server	***Certificate and Key Management ➜ Certificate Authority Certificates ➜ DOWNLOAD***	e.g. *192.168.1.2*
Name	***Certificate and Key Management ➜ Certificate Authority Certificates ➜ DOWNLOAD***	e.g. *Ca.crt*
Type of certificate	***Certificate and Key Management ➜ Certificate Authority Certificates ➜ EDIT***	*Certificate Authority no CRLs*