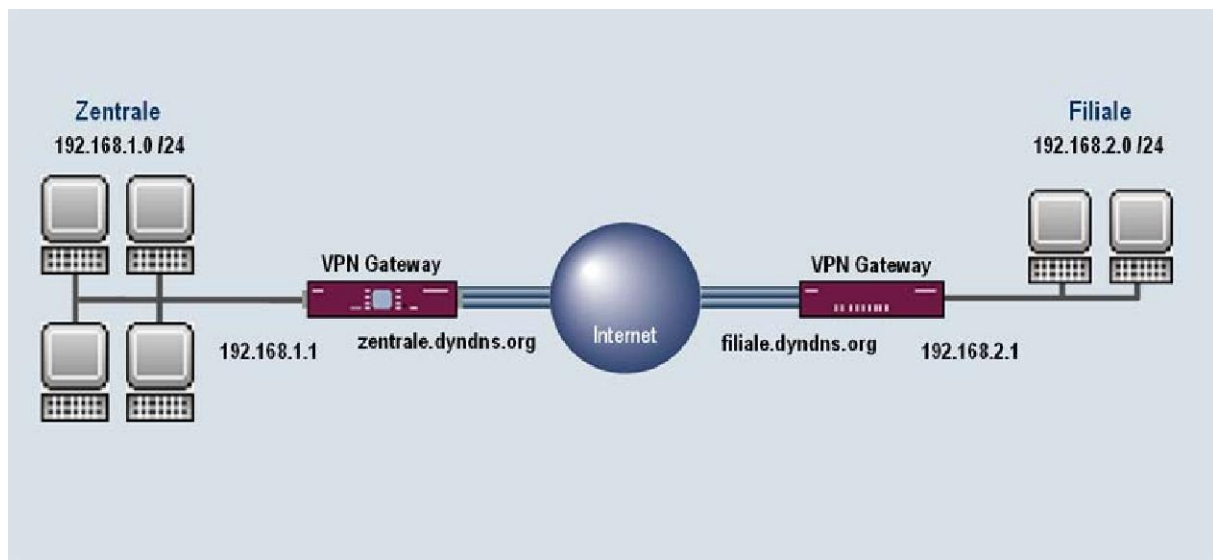


1. IPsec Verbindung zwischen 2 Gateways mit dynamischen IP Adressen



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPsec Verbindung beschrieben. 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

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Gateways
- Für das IPsec Gateway ist ein Bootimage ab Version 7.1.1 zu verwenden.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider
- Auf beiden Gateways müssen Sie DynDNS für den Internet Zugang konfiguriert haben

1.3 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.

INFO

Bei der Erstkonfiguration von IPsec startet der Wizard. Den sollten Sie ausführen, um Default Parameter für IPsec zu generieren. Die Vorgehensweise beim Anlegen von Verbindungen ist jedoch beim Wizard und beim manuellen Konfigurieren fast identisch.

1.3.1 Einstellungen im Menü IPSEC -> Configure Peers -> APPEND

1.3.1a Configure Peer Parameter

```

VPN Access 25 Setup Tool                               BinTec Access Networks GmbH
[IPSEC][PEERS][ADD]: Configure Peer                   zentrale
-----
Description:      Filiale
Admin Status:    up           Oper Status:  down

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 hierbei 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)

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

- Benennen Sie den Eintrag **Filiale**
- 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

Wenn Sie Ihre Verbindung mit Traffic List konfigurieren möchten, dann gehen Sie zu Abschnitt **1.3.1b**

Wenn Sie Ihre Verbindung mit Interface Routing konfigurieren möchten, dann gehen Sie zu Abschnitt **1.3.1c**

1.3.1b Traffic List Settings

- 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 hierbei 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

Gehen Sie folgendermassen vor um Ihren Eintrag zu konfigurieren:

- Als Beschreibung geben Sie **Filiale** an
- Unter Lokal 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 Main Menü befinden. Konfigurieren Sie weiter ab Punkt **1.3.1d**

1.3.1c Interface IP Settings

- 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 Routing Einträge 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 hierbei 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 Subnetmask, die zum Remotenetz gehört

Gehen Sie folgendermassen vor um Ihren 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 Main Menü befinden.

1.3.1d IPsec Anpassungen

Im folgenden Untermenü können Sie PHASE 1 Vorlagen verändern oder mit ADD hinzufügen:

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 : 1 (Blowfish/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 > </pre>	
SAVE	CANCEL
Enter string, max length = 255 chars	

Folgende Felder sind hierbei 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

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals lassen Sie auf: **1 (Blowfish/MD5)**
- Den Mode stellen Sie auf **aggressiv** da Sie dynamische IP Adressen haben
- Unter Local ID geben Sie **zentrale** ein (Ihre Local ID steht beim Partner unter Peer IDs)

Im folgenden Untermenü können Sie PHASE 2 Vorlagen verändern oder mit ADD hinzufügen:

IPSEC -> IPsec (Phase 2) Defaults -> EDIT

VPN Access 25 Setup Tool [IPSEC] [PHASE2] [EDIT]	BinTec Access Networks GmbH zentrale
<p>Description (Idx 1) : *autogenerated*</p> <p>Proposal : 1 (ESP(Blowfish/MD5) no Co</p> <p>Lifetime : use default</p> <p>Use PFS : none</p> <p>Heartbeats : none</p> <p>Propagate PMTU : no</p> <p>View Proposals ></p> <p>Edit Lifetimes ></p> <p style="text-align: center;">SAVE CANCEL</p> <hr/> <p>Enter string, max length = 255 chars</p>	

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Description	Geben Sie dem PHASE 2 Profil einen Namen
Proposal	Mit diesem Algorithmus wird die PHASE 2 verschlüsselt
Heartbeats	Baut den Tunnel ab, wenn der Partner nicht mehr reagiert

1.4 Ergebnis

Sie haben eine IPsec Verbindung zwischen 2 Gateways konfiguriert. Dazu haben Sie dynamische IP Adressen auf Seiten des Providers verwendet. Um zum Partner Gateway eine Verbindung aufbauen zu können, verwenden Sie auf beiden Seiten DynDNS. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter auf der Filialseite konfigurieren.

1.5 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." A1
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 62.10.10.10:50
0/62.10.10.10:1023 -> 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: 62.10.10.20:5
00 (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: 62.10.10.20:5
00 (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 3b7
a0be7]
04:30:59 DEBUG/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): SA 1 estab
lished 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 estab
lished 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 K
b 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
```

1.6 Konfigurationsschritte im IPSEC Menü im Überblick

----- Configure Peer -----		
Feld	Menü	Wert
Description	Configure Peers > APPEND	Filiale
Peer Address	Configure Peers > APPEND	filiale.dyndns.org
Peer IDs	Configure Peers > APPEND	filiale
Pre Shared Key	Configure Peers > APPEND	bintec

----- Traffic List -----		
Feld	Menü	Wert
Description	Configure Peers > Traffic List Settings > APPEND	Filiale
Local IP	Configure Peers > Traffic List Settings > APPEND	192.168.1.0 /24
Remote IP	Configure Peers > Traffic List Settings > APPEND	192.168.2.0 /24

----- IP Routing -----		
Feld	Menü	Wert
IP Transit Network	Configure Peers > Interface IP Settings > Basic IP	no
Local IP Address	Configure Peers > Interface IP Settings > Basic IP	192.168.1.1
Remote IP Address	Configure Peers > Interface IP Settings > Basic IP	192.168.2.0
Remote Netmask	Configure Peers > Interface IP Settings > Basic IP	255.255.255.0

----- Phase 1 -----		
Feld	Menü	Wert
Proposal	IKE (Phase 1) Defaults > edit > ADD	1 (Blowfish/MD5)
Mode	IKE (Phase 1) Defaults > edit > ADD	aggressiv
Local ID	IKE (Phase 1) Defaults > edit > ADD	zentrale

----- Phase 2 -----		
Feld	Menü	Wert
Proposal	IPsec (Phase 2) Defaults > edit > ADD	1 (ESP(Blowfish/MD5) no Co)