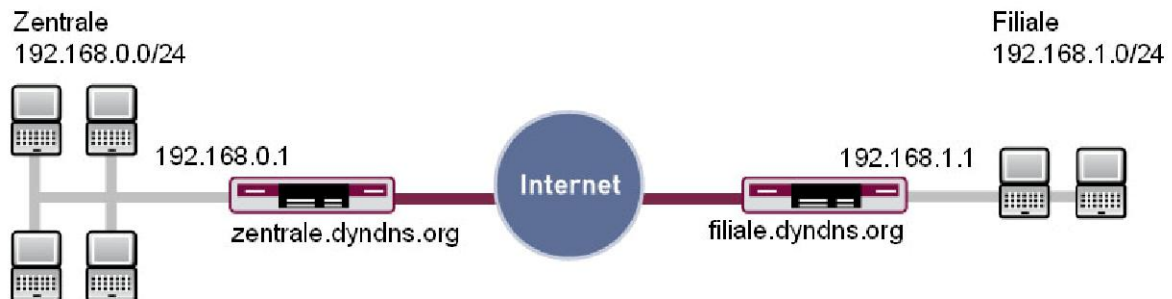


1. IPSec Verbindung zwischen 2 Gateways mit dynamischen IP Adressen



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPSec Verbindung mit dynamischen IP-Adressen auf beiden Seiten beschrieben. Außerdem werden Sie einen Eintrag für Ihren DynDNS Namen in dem Gateway konfigurieren. Diese Anleitung zeigt die Konfiguration auf Release 7.4.4.

Zur Konfiguration wird hierbei das FCI verwendet.

1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Gateways.
- Für das IPSec Gateway ist ein Bootimage ab Version 7.4.4 zu verwenden.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider.
- Für beide Gateways müssen Sie einen DynDNS Namen registriert haben.

1.3 Konfiguration

Die Anleitung konfiguriert ein Beispiel auf Seiten der Zentrale.

Um IPSec zu konfigurieren, müssen Sie im Folgenden Menü Einstellungen vornehmen:

VPN -> IPSec

In dem Untermenü "IPSec Peers" haben Sie die Möglichkeit mit **New** Verbindungspartner für IPSec hinzuzufügen.

INFO

Bei der Erstkonfiguration von IPSec konfiguriert das Gateway automatisch für Sie einige Standard Parameter. Diese sind für den weiteren Verlauf der IPSec Konfiguration notwendig und werden in den Tabellen hinterlegt.

1.3.1 IPSec Peer Parameter

Erstellen Sie in folgendem Menü eine neue Verbindung für IPSec:

VPN -> IPSec -> IPSec Peers -> New

Peer Parameters										
Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down									
Description	<input type="text" value="Filiale"/>									
Peer Address	<input type="text" value="filiale.dyndns.org"/>									
Peer ID	Fully Qualified Domain Name <input type="text" value="zentrale"/>									
Preshared Key	<input type="text" value="••••••••"/>									
Interface Routes										
Default Route	<input checked="" type="radio"/> No <input type="radio"/> Yes									
Local IP Address	<input type="text" value="192.168.0.1"/>									
Destination IP Address / Netmask	<table border="1"> <thead> <tr> <th>Remote IP Address</th> <th>Netmask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text" value="192.168.1.0"/></td> <td><input type="text" value="255.255.255.0"/></td> <td><input type="button" value="🗑"/></td> </tr> <tr> <td colspan="3" style="text-align: center;"><input type="button" value="+"/></td> </tr> </tbody> </table>	Remote IP Address	Netmask		<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="🗑"/>	<input type="button" value="+"/>		
Remote IP Address	Netmask									
<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="🗑"/>								
<input type="button" value="+"/>										

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 ID	Hier tragen Sie eine Identifikation des Partners ein (In der Filiale unter Local ID eingetragen).
Preshared Key	Das gemeinsame Passwort von beiden Gateways.
Local IP Address	Hier steht Ihre lokale IP Adresse vom Ethernet Interface.
Destination IP Address / Netmask	Hier konfigurieren Sie das zu erreichende Partner Netz.

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

- Benennen Sie den Eintrag unter Description: **z.B. Filiale**.
- Bei Peer Address geben Sie: **filiale.dyndns.org** an.
- Bei Peer ID geben Sie: **Fully Qualified Domain Name / filiale** an.
- Im Preshared Key tragen Sie **z.B. bintec** als Passwort ein.
- Unter Local IP Address tragen Sie **192.168.0.1** ein
- Unter Destination IP Address / Netmask fügen Sie mit **+** einen Eintrag hinzu.
- Tragen Sie in die Felder **192.168.1.0 / 255.255.255.0** ein.
- Bestätigen Sie Ihre Eingaben mit **OK**.

INFO

Bedenken Sie bitte, dass Sie in Ihrer Produktiv-Umgebung einen bedeutend längeren PreShared Key nutzen sollten. Empfehlenswert ist eine Länge von 20 Zeichen bei der Verwendung von Sonderzeichen, Zahlen und Klein/Groß Buchstaben.

1.3.2 Phase 1 Profil

Im folgenden Untermenü können Sie Phase 1 Vorlagen verändern oder mit New hinzufügen:

VPN -> IPSec -> Phase-1 Profiles

Phase-1 (IKE) Parameters													
Description	Filiale												
Proposal	<table border="1"> <thead> <tr> <th>Encryption</th> <th>Authentication</th> <th></th> </tr> </thead> <tbody> <tr> <td>AES</td> <td>MD5</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>3DES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>3DES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Encryption	Authentication		AES	MD5	<input checked="" type="checkbox"/>	3DES	MD5	<input type="checkbox"/>	3DES	MD5	<input type="checkbox"/>
Encryption	Authentication												
AES	MD5	<input checked="" type="checkbox"/>											
3DES	MD5	<input type="checkbox"/>											
3DES	MD5	<input type="checkbox"/>											
DH Group	<input type="radio"/> 1(768 Bit) <input checked="" type="radio"/> 2(1024 Bit) <input type="radio"/> 5(1536 Bit)												
Lifetime	86400 Seconds 0 KBytes												
Authentication Method	Preshared Keys												
Mode	<input type="radio"/> Main (ID-Protect) <input checked="" type="radio"/> Aggressive <input type="checkbox"/> Strict												
Local ID Type	Fully Qualified Domain Name												
Local ID Value	zentrale												

Advanced Settings

Alive Check	None
-------------	------

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 Type	Wählen Sie hier die Art der Identifikation aus.
Local ID Value	Hier tragen Sie die eigene Identifikation für das Gateway ein.
Alive Check	Schalten Sie hier die Tunnelüberwachung ein oder aus.

Konfigurieren Sie das Phase 1 Profil mit folgenden Parametern:

- Bei Description geben Sie: **z.B. Filiale** ein.
- Die Proposal markieren Sie mit einem **haken** und stellen Sie auf: **AES/MD5**.
- Den Mode stellen Sie auf **aggressiv** da Sie dynamische IP Adressen nutzen.
- Unter Local ID Type wählen Sie: **Fully Qualified Domain Name** aus.
- Unter Local ID Value geben Sie: **zentrale** ein (Steht beim Partner unter Peer ID).
- Alive Check setzen Sie auf: **None**.

1.3.3 Phase 2 Profil

Im folgenden Untermenü können Sie Phase 2 Vorlagen verändern oder mit New hinzufügen:

VPN -> IPSec -> Phase-2 Profiles

Phase-2 (IPSEC) Parameters													
Description	<input type="text" value="Filiale"/>												
Proposal	<table border="1"> <thead> <tr> <th>Encryption</th> <th>Authentication</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text" value="AES-128"/></td> <td><input type="text" value="MD5"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="text" value="3DES"/></td> <td><input type="text" value="MD5"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input type="text" value="3DES"/></td> <td><input type="text" value="MD5"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Encryption	Authentication		<input type="text" value="AES-128"/>	<input type="text" value="MD5"/>	<input checked="" type="checkbox"/>	<input type="text" value="3DES"/>	<input type="text" value="MD5"/>	<input type="checkbox"/>	<input type="text" value="3DES"/>	<input type="text" value="MD5"/>	<input type="checkbox"/>
Encryption	Authentication												
<input type="text" value="AES-128"/>	<input type="text" value="MD5"/>	<input checked="" type="checkbox"/>											
<input type="text" value="3DES"/>	<input type="text" value="MD5"/>	<input type="checkbox"/>											
<input type="text" value="3DES"/>	<input type="text" value="MD5"/>	<input type="checkbox"/>											
Use PFS Group	<input type="checkbox"/> Enabled												
Lifetime	<input type="text" value="28800"/> Seconds <input type="text" value="0"/> KBytes												
Advanced Settings													
IP Compression	<input type="checkbox"/> Enabled												
Alive Check	<input type="text" value="None"/>												

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.
Alive Check	Schalten Sie hier die Tunnelüberwachung ein oder aus.

Konfigurieren Sie das Phase 2 Profil mit folgenden Parametern:

- Bei Description geben Sie: **z.B. Filiale** ein.
- Die Proposal markieren Sie mit einem **haken** und stellen Sie auf: **AES-128/MD5**.
- Alive Check setzen Sie auf: **None**.

1.3.4 DynDNS konfigurieren

Erstellen Sie einen neuen Eintrag im Router für Ihren registrierten DynDNS Namen. Gehen Sie dazu in folgendes Menü:

Local Services -> DynDNS Client -> DynDNS Update -> New

Basic Parameters	
Host Name	<input type="text" value="zentrale.dyndns.org"/>
Interface	<input type="text" value="Internet"/>
User Name	<input type="text" value="zentrale"/>
Password	<input type="password" value="....."/>
Provider	<input type="text" value="dyndns"/>
Enable Update	<input checked="" type="checkbox"/> Enabled

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Hostname	Tragen Sie hier den kompletten Hostnamen ein, den Sie registriert haben.
Interface	Wählen Sie das Internet Interface aus.
Username	Geben Sie Ihren Benutzernamen an.
Password	Geben Sie Ihr Passwort an.

Provider	Hier wählen Sie Ihren DynDNS Provider aus.
Enable Update	Aktivieren oder Deaktivieren Sie den Eintrag.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Unter Hostname tragen Sie: **z.B. zentrale.dyndns.org** ein.
- Wählen Sie bei Interface: **z.B. Internet** aus.
- Tragen Sie unter Username: **z.B. zentrale** ein.
- Bei Password geben Sie: **z.B. passwort** an.
- Der Provider ist: **dyndns**.
- Enable Update: **aktivieren** Sie.

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 in folgendes Menü:

Maintenance -> Diagnostics -> Ping Test

Wenn Sie eine IP-Adresse der Remote Seite angeben, sollten Sie eine ähnliche Meldung erhalten:

Ping Test	
Test Ping Address	<input type="text" value="192.168.0.1"/>
Output	
<pre> PING 192.168.0.1: 64 data bytes 64 bytes from 192.168.0.1: icmp_seq=0. time=1. ms 64 bytes from 192.168.0.1: icmp_seq=1. time=1. ms 64 bytes from 192.168.0.1: icmp_seq=2. time=1. ms 64 bytes from 192.168.0.1: icmp_seq=3. time=1. ms 64 bytes from 192.168.0.1: icmp_seq=4. time=1. ms ----192.168.0.1 PING Statistics---- 5 packets transmitted, 5 packets received, 0% packet loss round-trip (ms) min/avg/max = 1/1/1 </pre>	
<input type="button" value="Go"/>	

1.6 Konfigurationsschritte im Überblick

IPSec Peer Parameter		
Feld	Menü	Wert
Description	VPN -> IPSec -> IPSec Peers -> New	z.B. Filiale
Peer Address	VPN -> IPSec -> IPSec Peers -> New	filiale.dyndns.org
Peer ID	VPN -> IPSec -> IPSec Peers -> New	FQDN / filiale
Preshared Key	VPN -> IPSec -> IPSec Peers -> New	bintec
Local IP Address	VPN -> IPSec -> IPSec Peers -> New	192.168.0.1
Destination IP Address Netmask	VPN -> IPSec -> IPSec Peers -> New	192.168.1.0/ 255.255.255.0

Phase 1 Profiles		
Feld	Menü	Wert
Description	VPN -> IPSec -> Phase-1 Profiles -> New	z.B. Filiale
Proposal	VPN -> IPSec -> Phase-1 Profiles -> New	AES/MD5
Mode	VPN -> IPSec -> Phase-1 Profiles -> New	aggressiv
Local ID Type	VPN -> IPSec -> Phase-1 Profiles -> New	Fully Qualified Domain Name
Local ID Value	VPN -> IPSec -> Phase-1 Profiles -> New	zentrale
Alive Check	VPN -> IPSec -> Phase-1 Profiles -> New	None

Phase 2 Profiles		
Feld	Menü	Wert
Description	VPN -> IPSec -> Phase-2 Profiles -> New	z.B. Filiale
Proposal	VPN -> IPSec -> Phase-2 Profiles -> New	AES-128/MD5
Alive Check	VPN -> IPSec -> Phase-2 Profiles -> New	None

DynDNS		
Feld	Menü	Wert
Hostname	Local Services -> DynDNS Client -> DynDNS Update	zentrale.dyndns.org
Interface	Local Services -> DynDNS Client -> DynDNS Update	Internet
Username	Local Services -> DynDNS Client -> DynDNS Update	z.B. zentrale
Password	Local Services -> DynDNS Client -> DynDNS Update	z.B. passwort
Provider	Local Services -> DynDNS Client -> DynDNS Update	dyndns
Enable Update	Local Services -> DynDNS Client -> DynDNS Update	aktivieren