Bintec/Teldat VPN gateway configuration

Contents

Bintec/Teldat VPN gateway configuration for SMS PASSCODE

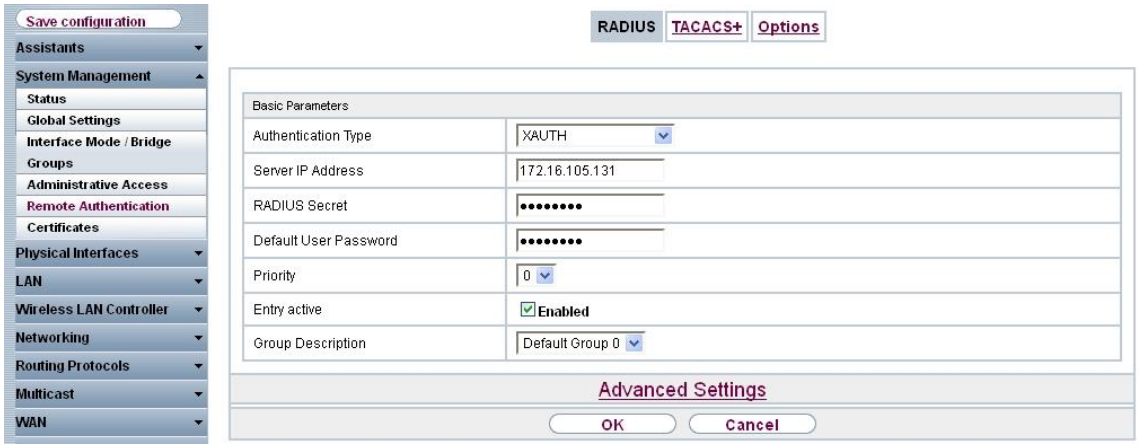
In this scenario about the VPN configuration on the Bintec gateway, an IPSec peer configuration entry is created which allows the simultaneous connection of multiple clients (IPSec Multi-User). Following the IPSec pre-shared key authentication, the One-Time Passcode (OTP) authentication between the Bintec VPN client and the SMS PASSCODE™ server is completed via a RADIUS server, in this case a Microsoft Network Policy Server (NPS).

> **Note**
>
> Instead of the **Multi-User IPSec configuration**, there is also the option to create a separate IPSec peer configuration entry for each VPN client.
> The priority of the Multi-User IPSec peer must always be lower than other IPSec peer configuration entries.

Connect Radius

To connect the RADUIS server to the Bintec VPN gateway, go to the following menu:

1. Go to **System Management** -> **Remote Authentication** -> **RADIUS** ->**New**.

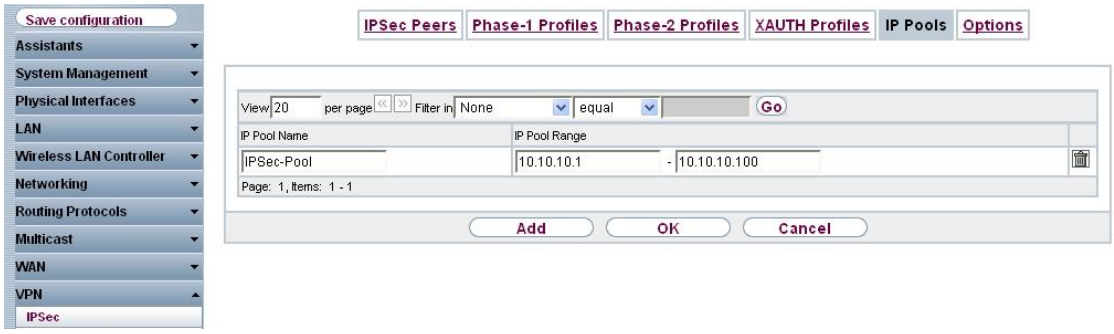


System Management->**Remote Authentication**->**RADIUS**->**New**
Proceed as follows:

1. Select **Authentication Type** *XAUTH* in order to enable authentication via the Windows Server.
2. Enter the**Server IP Address**, e.g. *172.16.105.131* , to communicate with the Microsoft RADIUS server.
3. Enter the shared password used for communication between the RADIUS server and your device, e.g. *supersecret* .
4. Press **OK** to confirm your entries.

An address pool must be created to assign an IP pool to the VPN profile of the Multi-User IPSec peer.

1. Go to **VPN** -> **IPSec** -> **IP Pools** -> **Add**

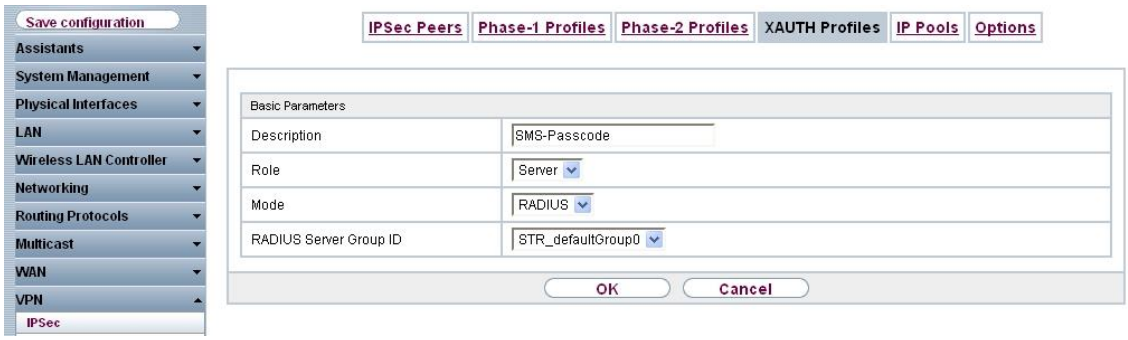


VPN -> **IPSec** -> **IP Pools** -> **Add**

Proceed as follows:

1. Enter the name of the IP pool for **IP Pool Name**, e.g. *IPSec-Pool* .
2. For **IP Pool Range**, enter the first IP address of the address pool in the first field, e.g. *10.10.10.1* .
3. Enter the last IP address of the address pool in the second field, e.g. *10.10.10.100* .
4. Click **Add**.

A profile must then be created in order to be able to refer to the RADIUS server.
Go to **VPN** -> **IPSec** -> **XAUTH Profiles** -> **New**.



VPN -> **IPSec** -> **XAUTH Profiles**-> **New**

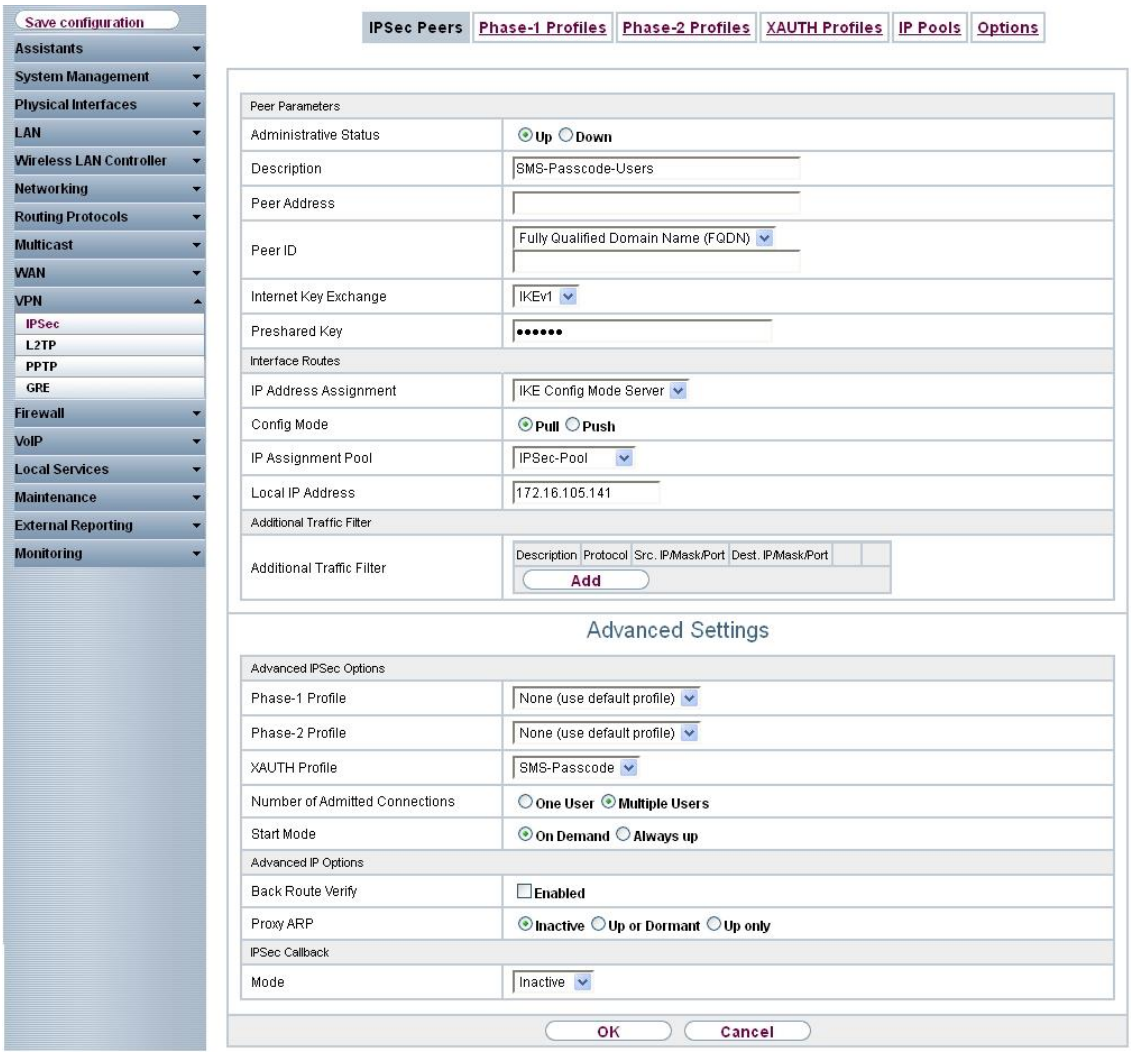
Proceed as follows to set up a profile:

1. Enter a **Description** for this XAuth profile, e.g. *SMS Passcode.*

2. Select the **Role** of the gateway for the XAuth authentication; in this instance, *Server.*
3. Under **Mode** select *RADIUS.* Authentication is carried out via the RADIUS server.
4. Confirm with **OK**.

Now the actual **IPSec Peer** is created.

1. Go to **VPN** -> **IPSec** -> **IPSec Peers** -> **New**



VPN -> **IPSec** -> **IPSec Peers** -> **New**

Proceed as follows:

1. Enter a **Description** of the peer which identifies it, e.g. *SMS Passcode User.*
2. In this scenario, no IPSec peer ID is saved to enable the Multi-User IPSec connections.
3. Under **Preshared Key** enter the password agreed with the peer, e.g. *supersecret*.
4. For **IP Address Assignment**, select the configuration mode of the interface; in this instance, *Server In IKE Configuration Mode*.
5. Select a configured **IP Assignment Pool**, e.g. *IPSec Pool*.
6. Enter the LAN IP address of the VPN gateway under **Local IP Address**, e.g. *172.16.105.141*.
7. Click **Advanced Settings**.

8. If selecting *None (Use Standard Profile)*, the profile indicated as standard in **Phase 1 Profile**/**Phase 2 Profile** is used.
9. Select the **XAUTH Profile** that has already been configured, e.g. *SMS Passcode*.
10. For **Number of Admitted Connections**, set it to *Multiple Users* to enable IPSec Multi-User mode.
11. Leave the remaining settings unchanged and confirm them with **OK**.