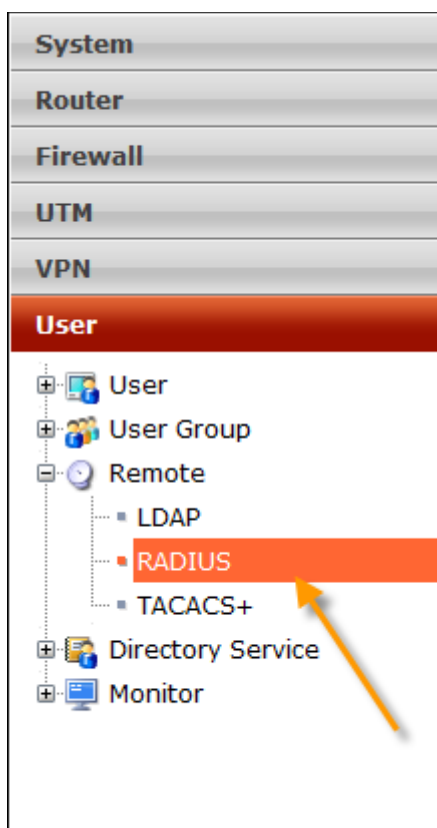Fortinet FortiGate/FortiWiFI configuration

Contents

Configuring the FortiGate/FortiWifi© for SSL VPN connections

This document outlines how to configure Fortinet for MFA protection with SMS PASSCODE.

To complete the setup it is required that you have a Fortinet© VPN product such as FortiGate© or FortWifi©, a Microsoft radius server (NPS), an installation of the core components of SMS PASSCODE and SMS PASSCODE Radius client protection. Please refer to the *SMS PASSCODE administrators guide* for further guidance to install the SMS PASSCODE components.
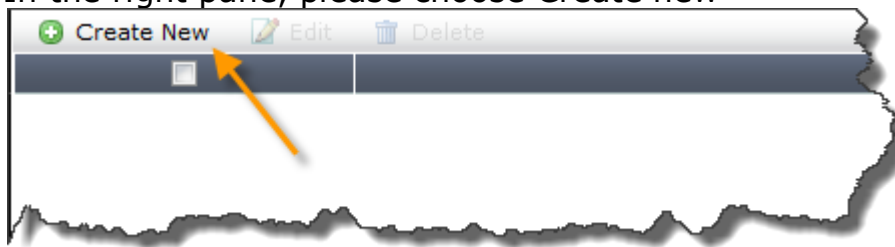
The Radius Server.

To configure the FortiGate/FortiWifi with the SMS PASSCODE protected radius server, navigate to User, Remote, Radius.

In the right pane, please choose Create new

Name: Choose a friendly name (you are going to use this, when setting up group).

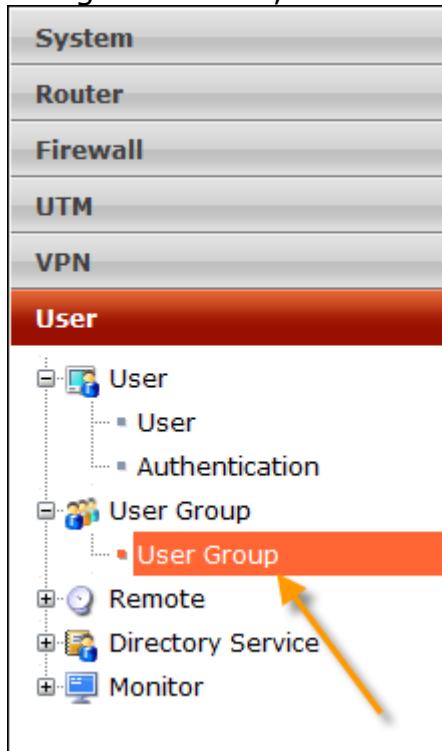Primary Server Name/IP: the name or IP address of the SMS PASSCODE protected radius server

Primary Server Secret: The same shared secret that you have entered in the radius server's radius client.

Authentication Scheme: Choose the radio button "Specify Authentication Protocol". Choose PAP.
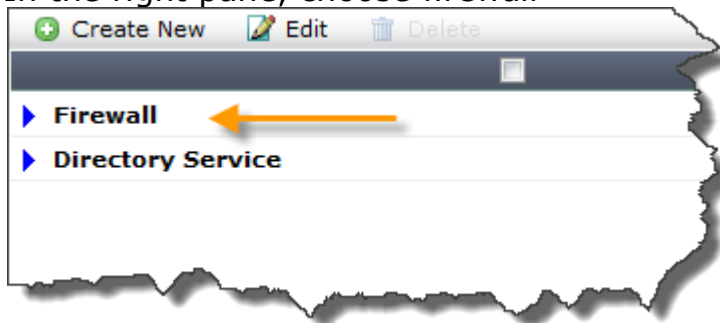
The User Group

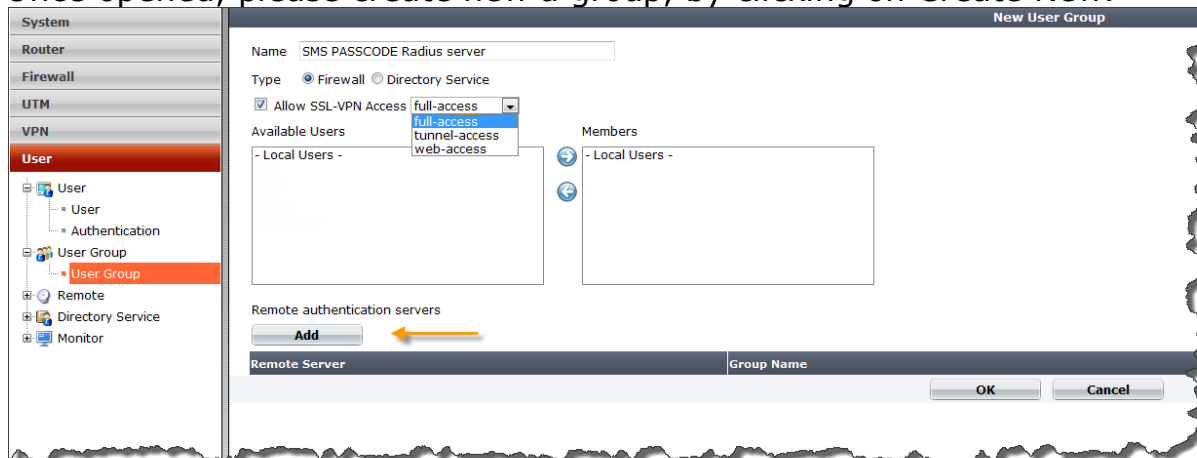## Navigate to User, User Group

In the right pane, choose firewall

Once opened, please create new a group, by clicking on Create New.

Name: choose a friendly name of your own choice
Type: Firewall
Check the checkbox "Allow SSL-VPN", and choose the appropriate setting
Click add on the remote authentication servers, and add the radius server. The
radius server is located by the friendly name; you named the radius server
when configuring it. Click ok.
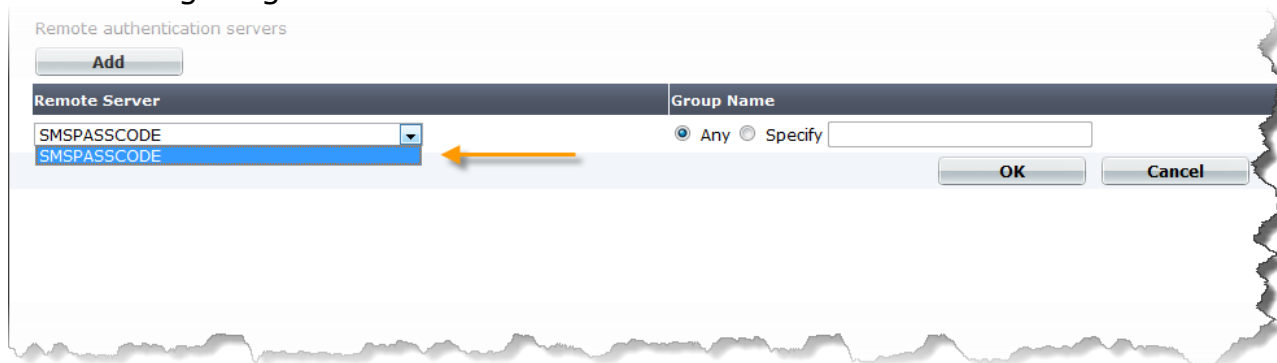
Clients using Dead Peer Detection will have their connection killed, if it times out
before the passcode entry. You should therefore be care full using Dead Peer
Detection.
The Fortinet