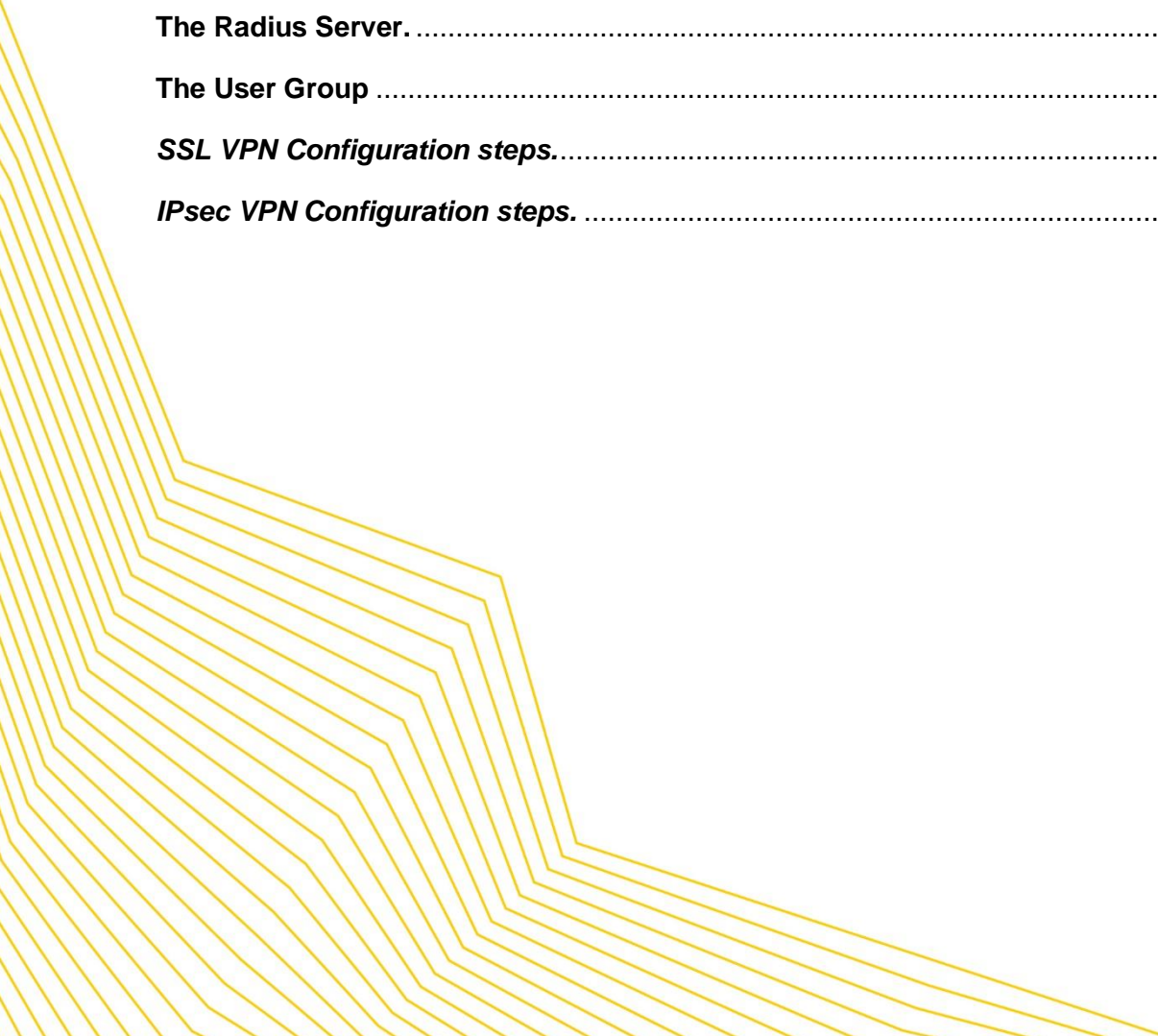




Fortinet FortiGate FortiOS v6 VPN Configuration Guide

Contents

The Radius Server	2
The User Group	4
SSL VPN Configuration steps	5
IPsec VPN Configuration steps	6





Configuring a FortiGate running FortiOS version 6 for SSL VPN or IPsec dial-up VPN.

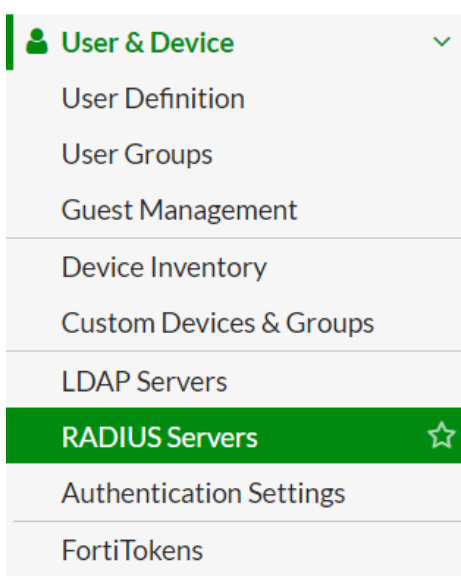
This document outlines how to configure a FortiGate for MFA protection with Censornet MFA.

To complete the setup, it is required that you have a Fortinet© VPN product such as FortiGate, a Microsoft radius server (NPS), and an installation of the Censornet MFA Authentication Client Software powered by SMS PASSCODE. Please refer to the Censornet support site for further guidance to install the Censornet MFA Authentication Client Software.



The Radius Server.

To configure the FortiGate with the Censornet MFA protected radius server, navigate to User & Device, RADIUS Servers.





In the right pane, please choose Create New

The screenshot shows the 'Edit RADIUS Server' configuration page. At the top, there is a toolbar with buttons for '+ Create New', 'Edit', 'Clone', and 'Delete', along with a search field. Below the toolbar are two filter dropdowns for 'Name' and 'Server IP/Name'. The main configuration area includes:

- Name:** Censornet_MFA
- Authentication method:** Default **Specify** (highlighted in green)
- NAS IP:** PAP (selected in the dropdown menu)
- Include in every user group:**
- Primary Server:**
 - IP/Name:** 192...
 - Secret:** [masked]
- Connection status:** Successful
- Buttons:** Test Connectivity, Test User Credentials

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

Primary Server Name/IP: the name or IP address of the Censornet MFA 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 & Device, User Group

- User & Device ▼
 - User Definition
 - User Groups** ☆
 - Guest Management
 - Device Inventory
 - Custom Devices & Groups
- LDAP Servers
- RADIUS Servers
- Authentication Settings

In the right pane, please choose Create New, Select Type Firewall

New User Group

Name

Type

- Firewall**
- Fortinet Single Sign-On (FSSO)
- RADIUS Single Sign-On (RSSO)
- Guest

Members

Under Remote Group, please select Add, Select the RADIUS server created in the earlier steps.

New User Group

Name

Type

- Firewall**
- Fortinet Single Sign-On (FSSO)
- RADIUS Single Sign-On (RSSO)
- Guest

Members

Remote Groups

+ Add

No matching entries found

Add Group Match

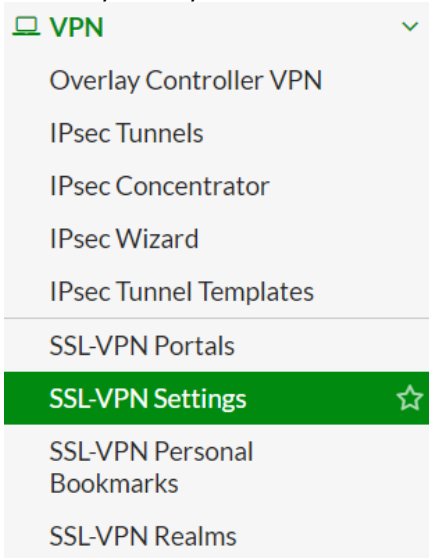
Remote Server

- RADIUS SERVER (1)
- Censornet_MFA**

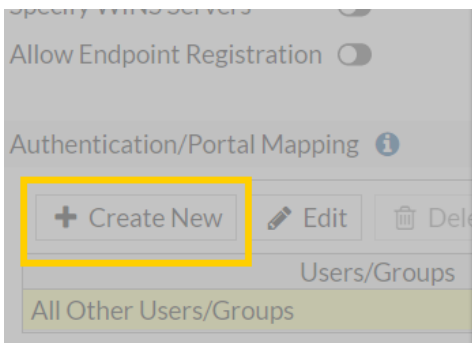


SSL VPN Configuration steps.

Under, VPN, SSL-VPN Settings



Under Authentication/Portal Mapping, Select Create New and choose the new Censornet_MFA_Group as the Users/Group and chose the required Portal type.



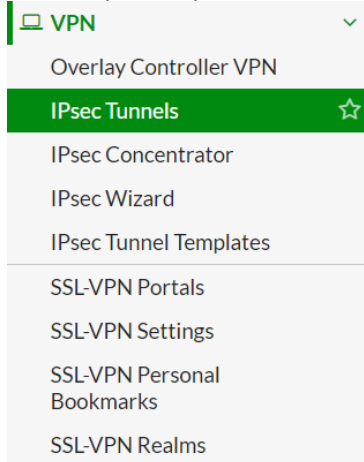
New Authentication/Portal Mapping	
Users/Groups	<input type="text" value="Censornet_MFA_Group"/>
Realm	<input type="text" value="Default realm"/> Specify
Portal	<input type="text" value="full-access"/>

Complete the setup of your FortiGate by configuring the required policy that allows traffic from the SSL VPN interface to the internal Lan, for further assistance please refer to your FortiGate documentation.

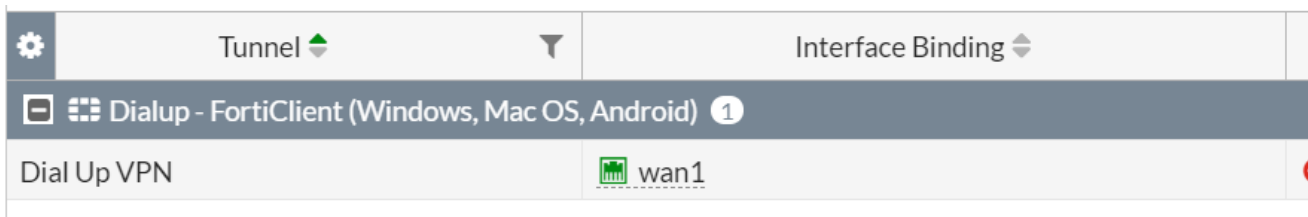


IPsec VPN Configuration steps.

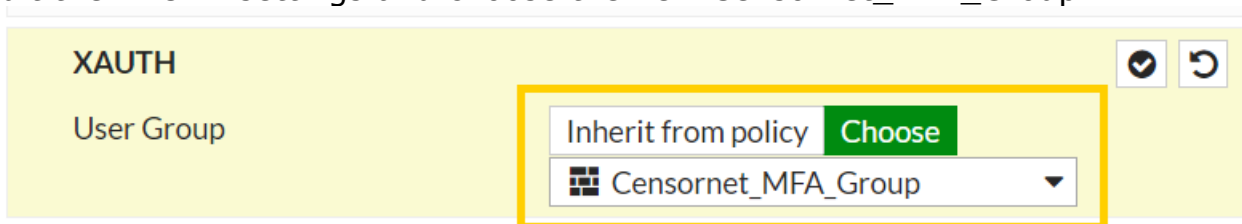
Under, VPN, IPsec Tunnels



Edit the VPN tunnel.



Edit the XAUTH settings and choose the new Censornet_MFA_Group.



FortiGate IPsec uses MS-Chap to send the challenge-response to the NPS server, Censornet's MFA solution only supports PAP.

Follow this KB on how to change the FortiGate to use PAP

<https://help.clouduss.com/mfa-knowledge-base/configure-forti-gate-to-use-pap-for-challenge-response>

Complete the setup of your FortiGate by configuring the required policy that allows traffic from the SSL VPN interface to the internal Lan, for further assistance please refer to your FortiGate documentation.