Fortinet FortiGate FortiOS v6 VPN Configuration Guide

Contents

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

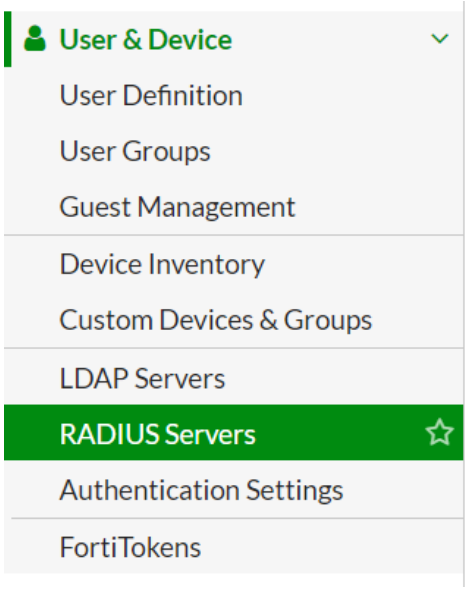
This document outlines how to configure a FortiGate for MFA protection with Censornet MFA.

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.

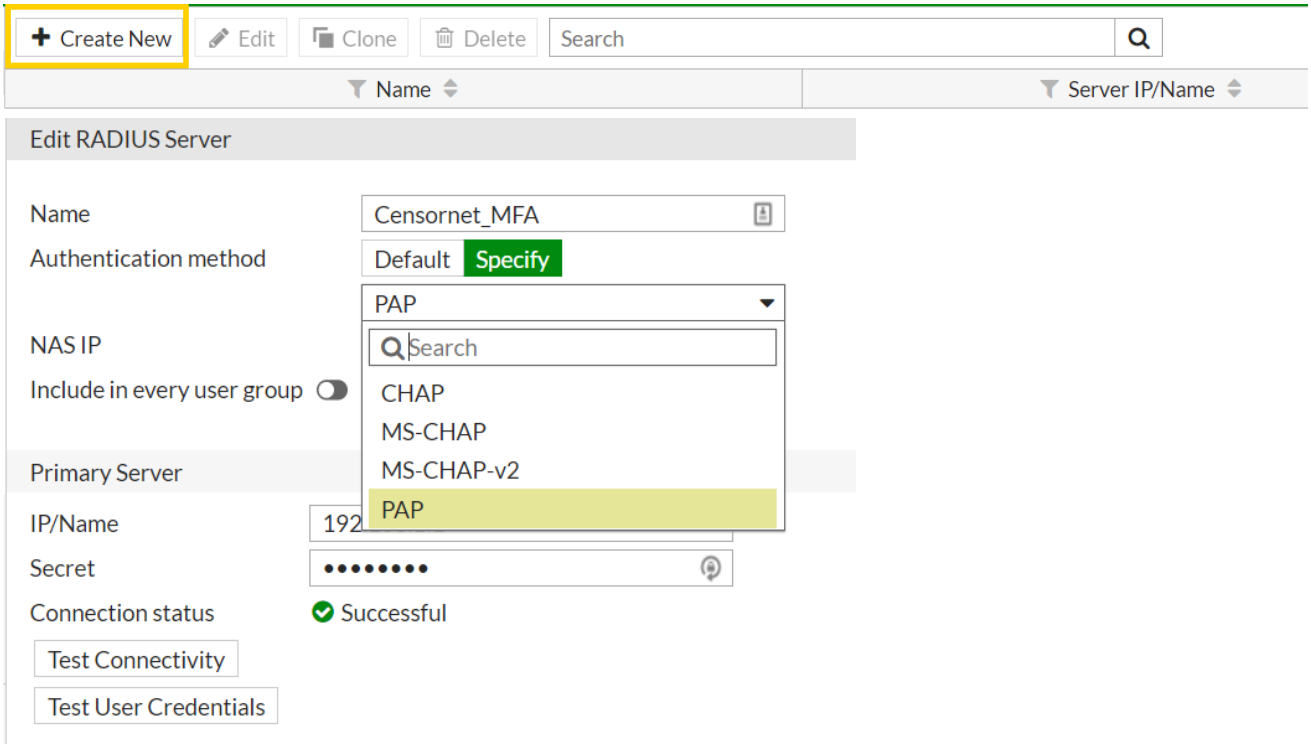
censornet.

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



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

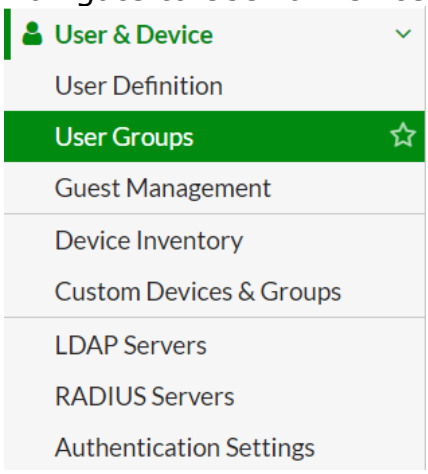
Primary Server Name/IP: the name or IP address of the Censornet MFA protected radius server

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

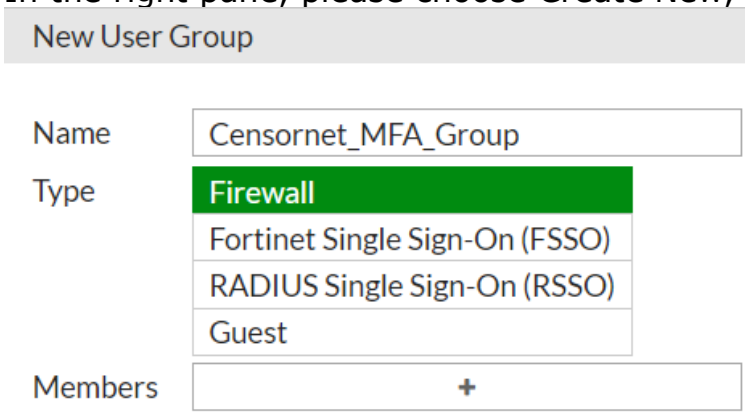
Authentication Scheme: Choose the radio button "Specify Authentication Protocol". Choose PAP.

The User Group

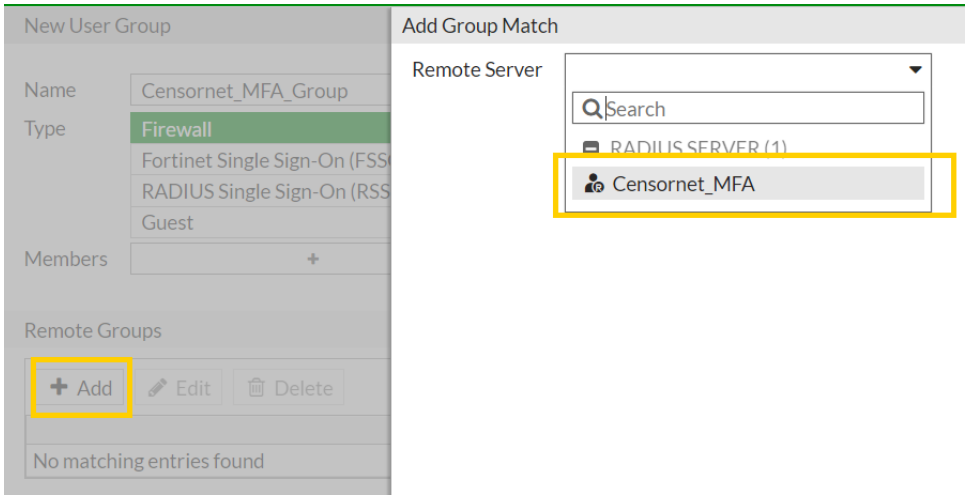
Navigate to User & Device, User Group



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

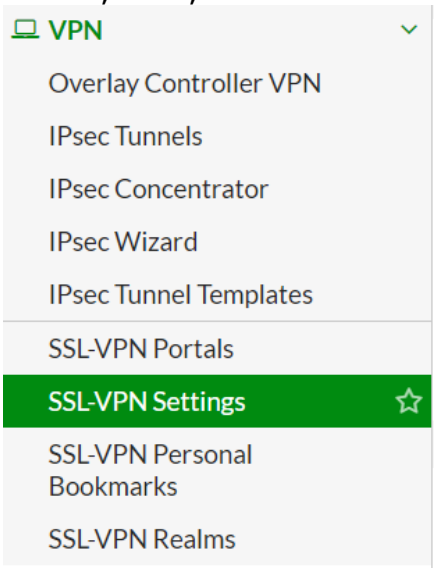


Under Remote Group, please select Add, Select the RADIUS server created in the earlier steps.

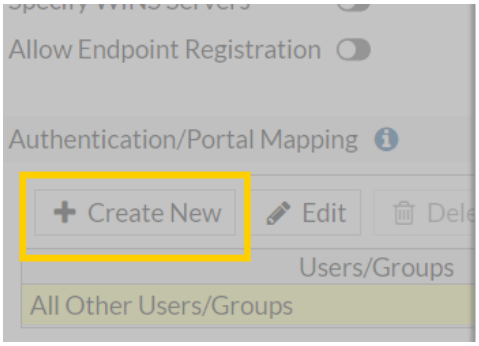


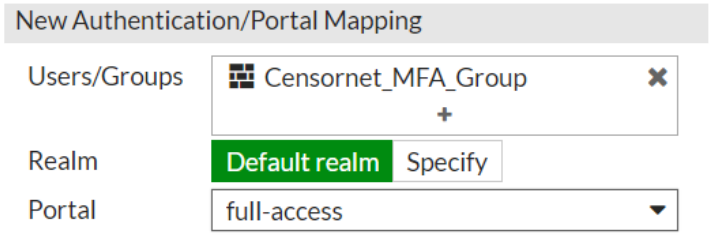
SSL VPN Configuration steps.

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.



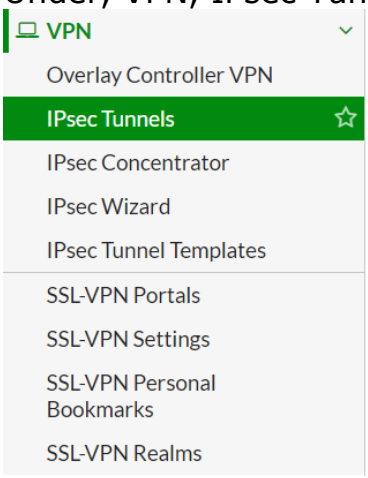


Complete the setup of your FortiGate by configuring the required policy that allows traffic from the SSL VPN interface to the internal Lan, for further assistance please refer to your FortiGate documentation.

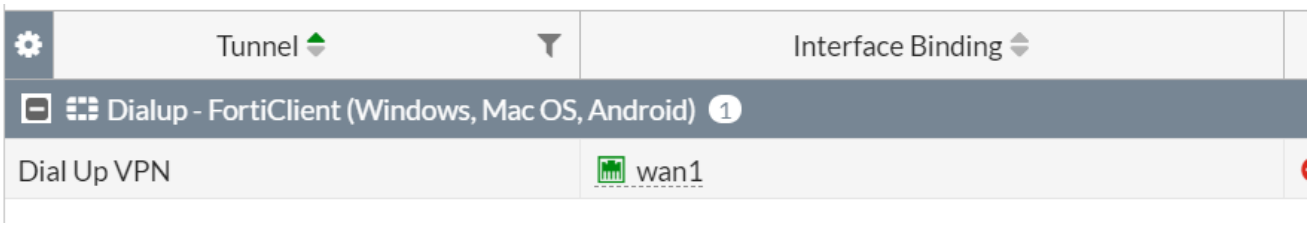
censornet.

IPsec VPN Configuration steps.

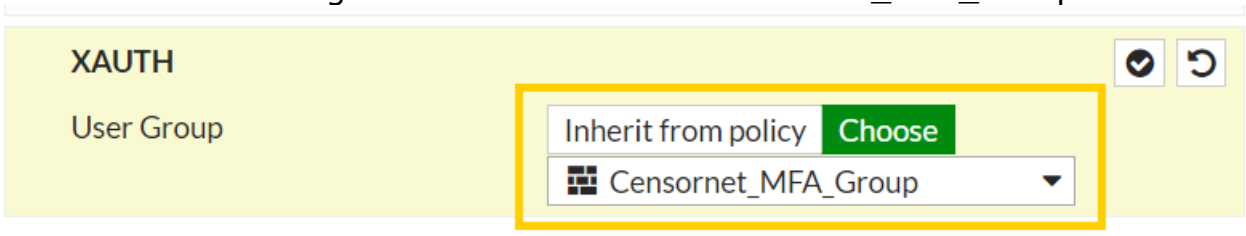
Under, VPN, IPsec Tunnels



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.