censornet.

Juniper configuration

Contents

censornet.

Guide for implementing SMS PASSCODE protection with Juniper.

This document outlines the process of configuring a Juniper with SMS PASSCODE Radius Client protection.
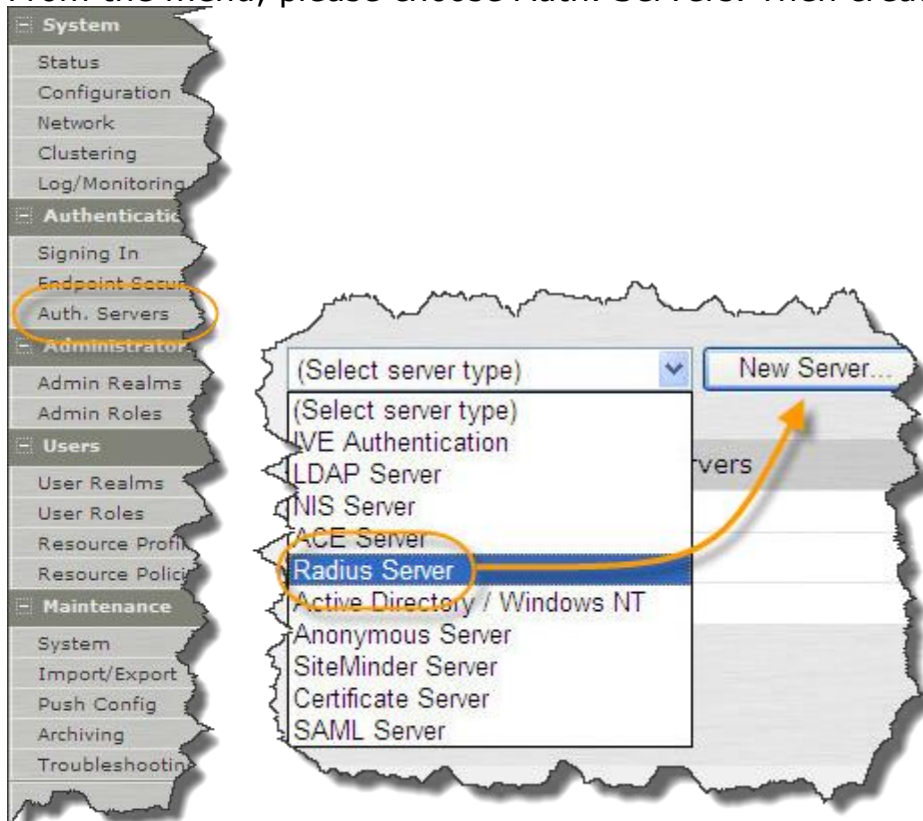
Prerequisites

Juniper SA or Juniper MAG series.
Microsoft radius server (NPS)

Configuration Guide

When setting up the Juniper concentrator, it has to be configured to use authentication with radius.
From the menu, please choose Auth. Servers. Then create a new Radius server.

Name is a friendly name of your own choice.
The Authentication port 1812 is a standard radius port (UDP).
Shared secret must match the shared secret entered in the NPS radius client.

Name:	Radsrv
NAS-Identifier:	
Primary Server	
Radius Server:	1.1.2.2
Authentication Port:	1812
Shared Secret:	••••••••
Accounting Port:	1813
NAS-IP-Address:	
Timeout:	10 seconds
Retries:	3

When this configuration is saved, please add a radius rule

Custom Radius Rules

Delete ↑ ↓ New Radius Rule…

censornet.

Please setup custom Challenge rule and reject rule.

Incoming Packet type: "Access Challenge" or "Access Reject"
Radius attribute "Reply-message (18)"
Operand: "Matches the expression"
Value: "(.*)"
Please choose "show generic login page"
Save the configuration

To configure and set up the radius server, please refer to the SMS PASSCODE administration guide.