SonicWall SSL VPN and SendQuick for One-Time-Password Configuration Guide

Prepared by

TalariaX Pte Ltd
76 Playfair Road
#08-01 LHK2
Singapore 367996

Tel: +65 62802881
Fax: +65 62806882

E-mail: info@talariax.com
Web: www.talariax.com

JUNIPER SA SSL VPN & SENQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

This document is prepared as a guide to configure Juniper SA SSL VPN to run with SendQuick Conexa for One-time-password via SMS.

The pre-requisite is that SendQuick Conexa OTP server is configured with RADIUS on port 1812. Ensure that both applications are using the same port for radius.

It is recommended that the Juniper SSL VPN to be running firmware 6.5R5 (15991)

2.0 CONFIGURE JUNIPER SSLVPN

In the Juniper SSL VPN configuration, selection **Authentication > Authentication Servers** and configure **NEW RADIUS Authentication Server** as shown below.

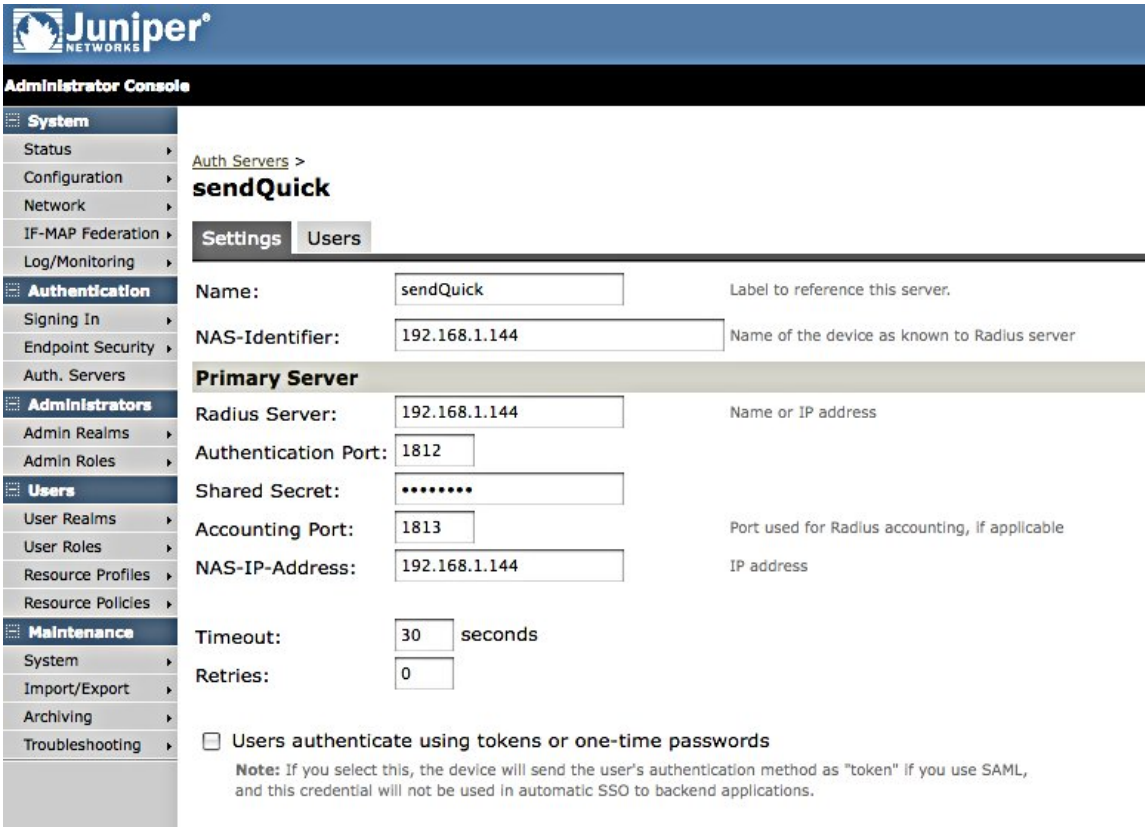

Figure 1: Authentication Server Configuration

You will need to configure the following as shown above:

- Name (of the authentication server)
- NAS Identifier (include a name)
- Radius Server (IP address of sendQuick Conexa)
- Authentication Port (for Radius): 1812 (this must be 1812 as this is the port used in Conexa)
- Shared secret (the same secret need to be included in Conexa)
- Accounting port and others are optional

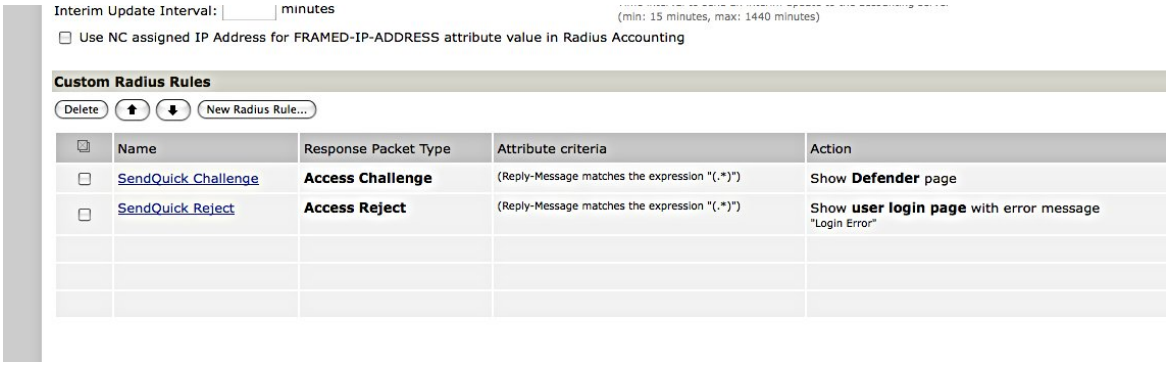

Figure 2: Custom Radius Rule

Then, configure the Custom Radius Rules as shown above to allow Juniper to show the right page for Access Challenge and Error page respectively.

Note:
"Access Challenge" has to be added where the "Reply-Message" matches the expression "(.*)" and in that case shows "show GENERIC LOGIN page". This will present the OTP field for the user.

Edit the Custom Radius Rule as shown in Figure 3 and 4 below. The final result should be as shown in Figure 2.

Figure 3 is the Custom Rule for Access Challenge while Figure 4 is the Custom Rule for Access Reject.

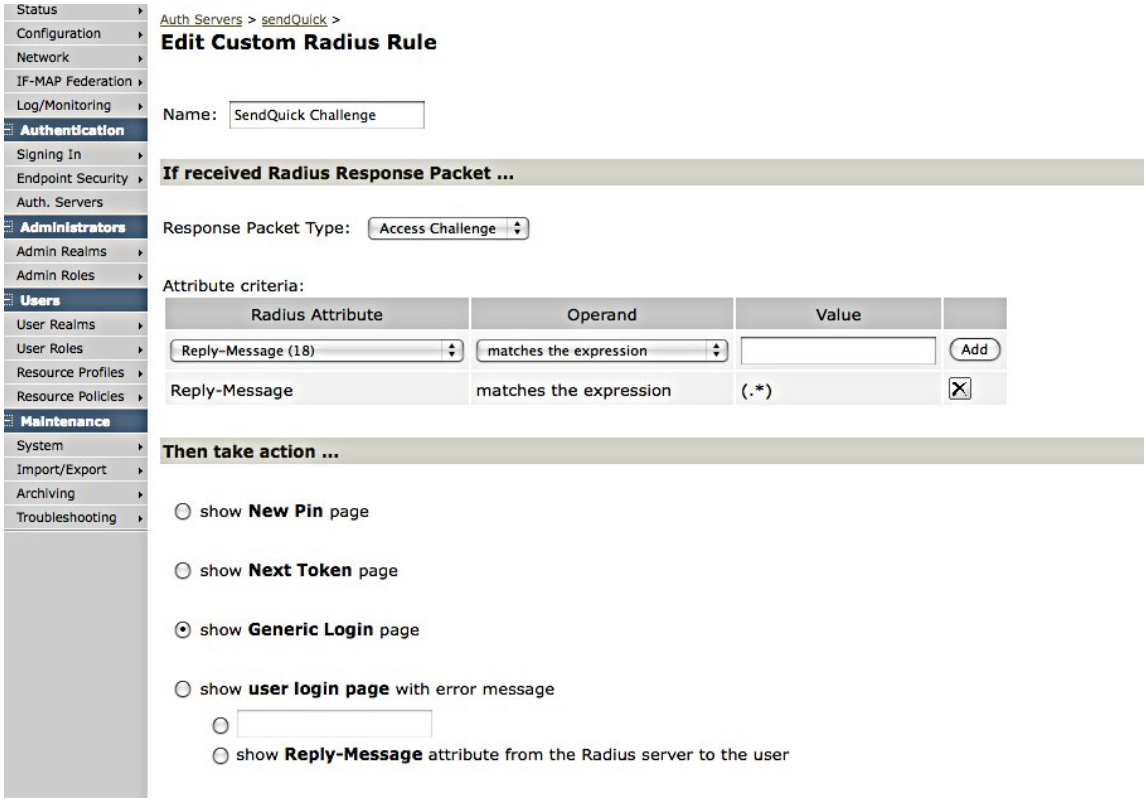

Figure 3: Custom Radius Rule Editing

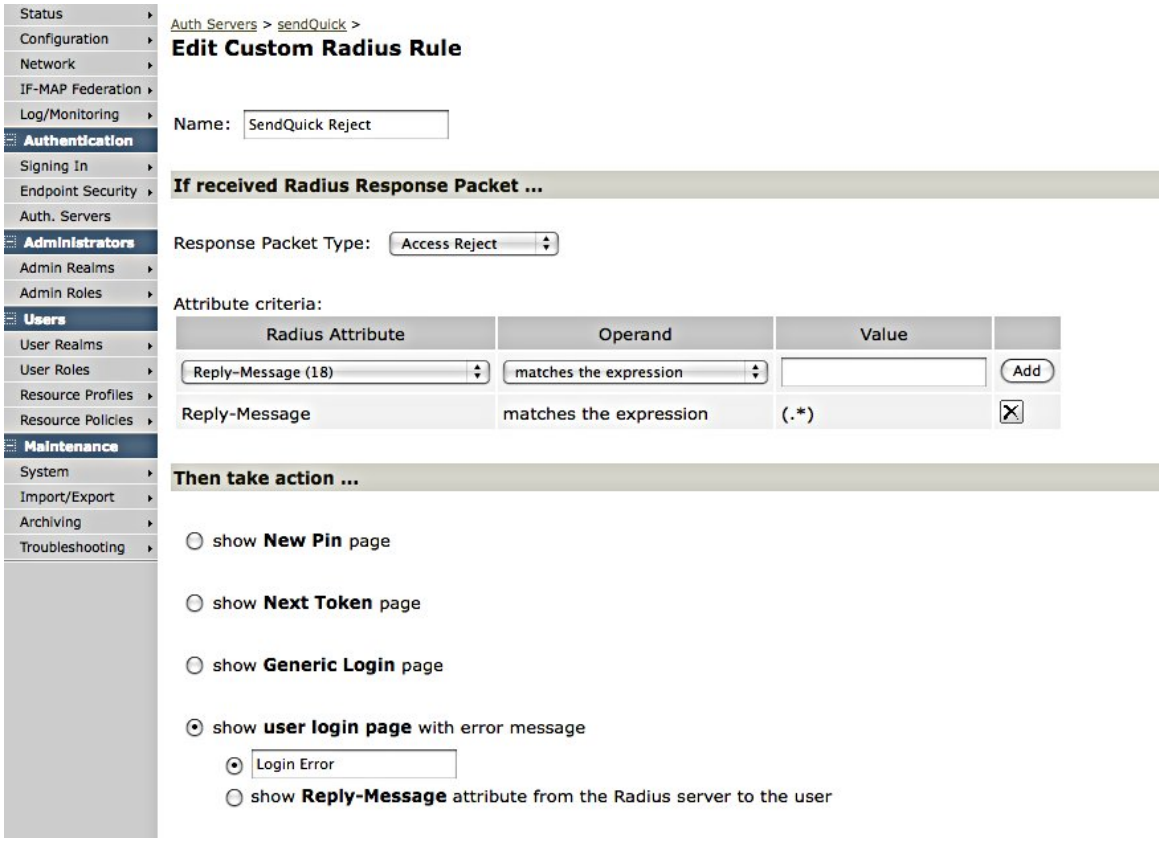

Figure 4: Custom Radius Rule Editing (Access Reject)

3.0 CREATE USER REALM

Create User Realm that use the Authentication Server created in Section 2.0 above for authentication and configure the connection to sendQuick Conexa.

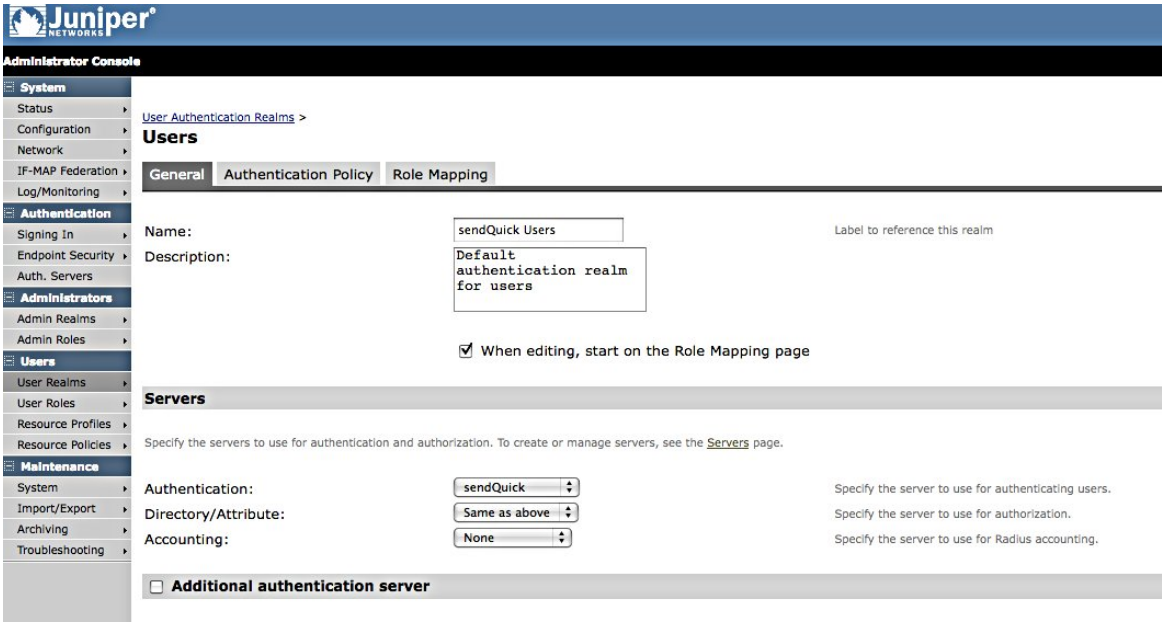

Figure 5: User Realm Configuration

4.0 CREATE SIGN-IN POLICY

Create a Sign-In Policy that uses the Sign In Page from 2.0 and User Realm from 3.0. The login pages can be customized with text and logos of your choice for your users to view.

Figure 6: First Login Page

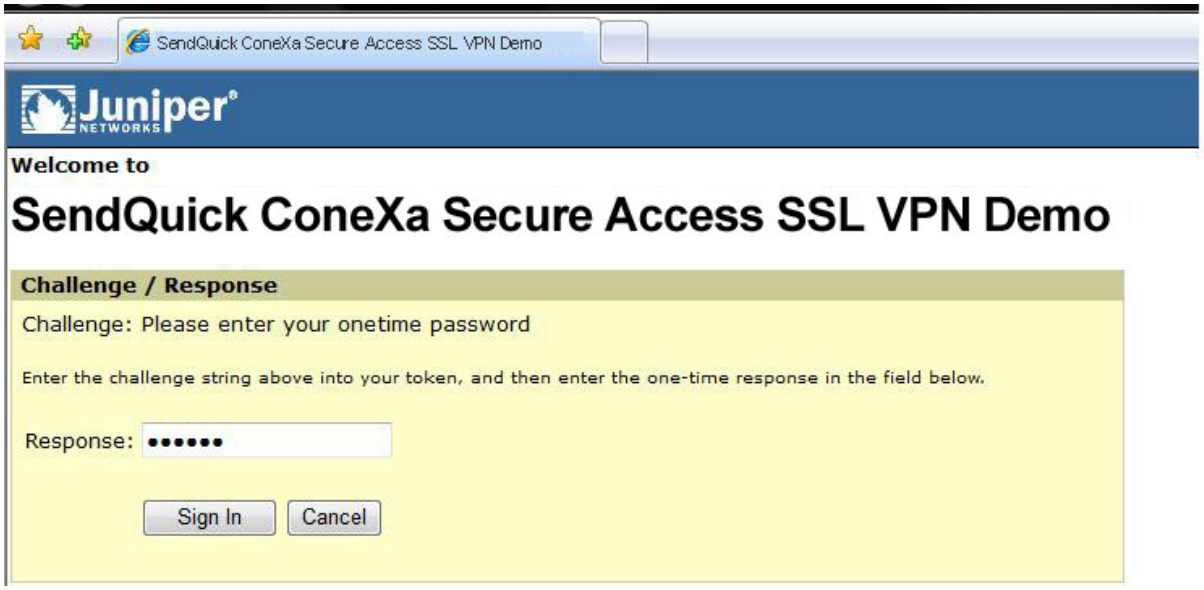

Figure 7: OTP Challenge-Response Page