ESET

SECURE AUTHENTICATION

SonicWall SSL VPN Integration Guide

ESET **SECURE AUTHENTICATION**

Customer Care Worldwide: www.eset.eu/support
Customer Care North America: www.eset.com/support

REV. 7/22/2013

Contents

1. Overview

This document describes how to enable ESET Secure Authentication (ESA) Two-Factor Authentication (2FA) for a SonicWall SRA VPN device.

2. Prerequisites

Configuring the VPN device for 2FA requires:

- A functional ESA RADIUS server that has your SonicWall SSL VPN device configured as a client, as shown in **Figure 1**.

Note: To prevent locking any existing, non-2FA enabled AD users out of your VPN, we recommend that you allow Active Directory passwords without OTPs during the transitioning phase. It is also recommended that you limit VPN access to a security group (for example **VPNusers**).

- A SonicWall SRA SSL-VPN Appliance. The supported appliances are:

  E-Class SRA Series
  SRA Series
  RA Series (although interfaces may differ from this guide, the same concepts will apply)

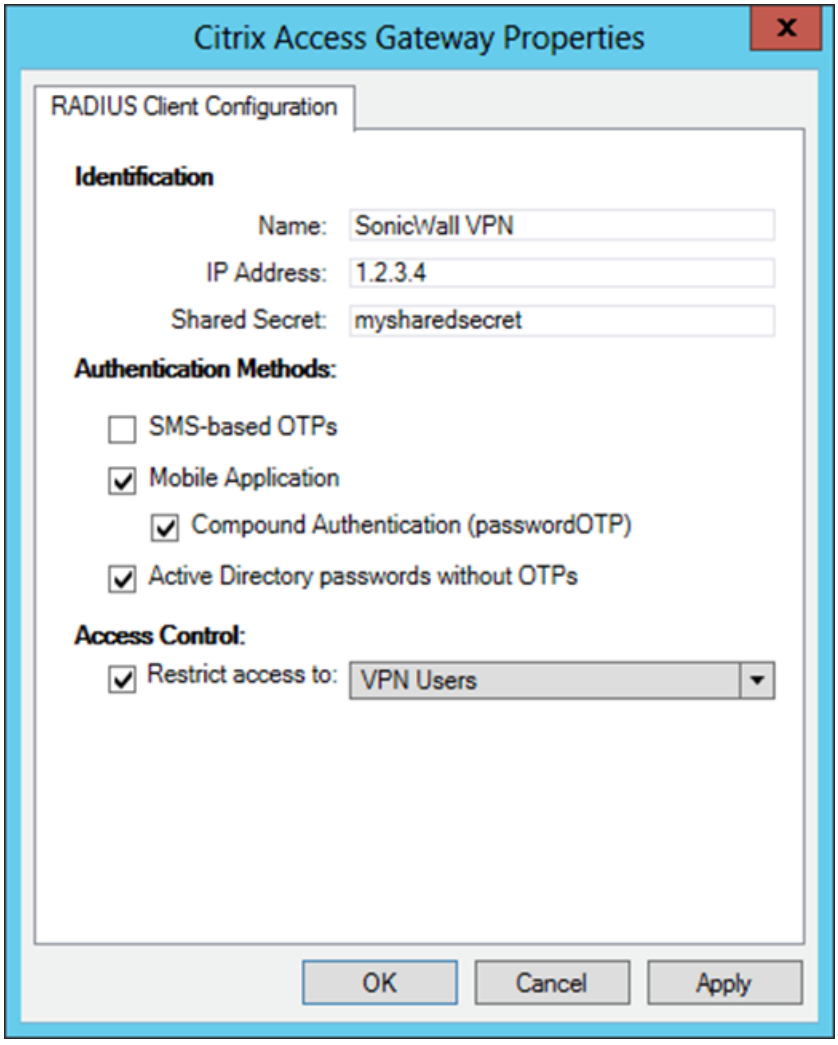

Figure 1

This screenshot shows The RADIUS client settings for your SonicWall VPN device. Note that the check boxes next to **Mobile Application**, **Compound Authentication** and **Active Directory passwords without OTPs** must be selected and the **IP Address** is the internal address of your SonicWall appliance.

3. Integration instructions

1. Add a RADIUS Server:
   a. Using a web browser, Log into the SonicWall administrative interface.
   b. Navigate to **Portal** > **Domain** on the left.
   c. Click **Add Domain**.
   d. From the **Authentication type** drop-down menu, select **Radius**.
   e. Enter a descriptive name for the authentication domain in the **Domain Name** field, for example, **ESA Radius**.
   f. Under **Primary Radius Server**, enter the following details:
      i. **Radius Server Address**: The IP address of your ESA RADIUS server.
      ii. **Radius server port**: 1812 (or custom port if you are overriding).
      iii. **Secret Password**: As shown in **Figure 1**
      iv. **Radius Timeout**: 30 seconds
      v. **Max retries**: 2
      vi. **Portal Layout Name**: Select your portal layout.
      vii. Optionally, add the details of a backup ESA RADIUS server.
   g. Click **Add** to update the configuration. The domain will be added to the **Domain Settings** table.

2. Testing the connection:
   a. Connect to your **SSL-VPN** using a user account that has been configured to use with Mobile Application 2FA using ESA. When prompted for a password, append the OTP generated by the Mobile Application to your AD password. For example, if the user has an AD password of Esa123 and an OTP of 999111, type in Esa123999111.

4. Troubleshooting

If you are unable to authenticate via the ESA RADIUS server, ensure that you have performed the following steps:

1. If this is a new SonicWall VPN setup, try logging in without a WiKID one-time password before adding in two-factor authentication. This will make troubleshooting easier.
2. Run a smoke test against your RADIUS server, as described in the **Verifying ESA RADIUS Functionality** document.
3. Verify that RADIUS authentication is enabled on the SonicWall server:
   a. Navigate to the **VPN** window in the administrative interface and select the **Configure** tab.
   b. In the **Security Association** field,select **GroupVPN**.
   c. Select the check box next to **Require XAUTH/RADIUS**.
4. Verify that there is no firewall blocking UDP 1812 between your VPN device and your RADIUS server.
5. If you are still unable to connect, contact ESET technical support.