ESET SECURE AUTHENTICATION

Barracuda 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 Barracuda SSL VPN appliance.

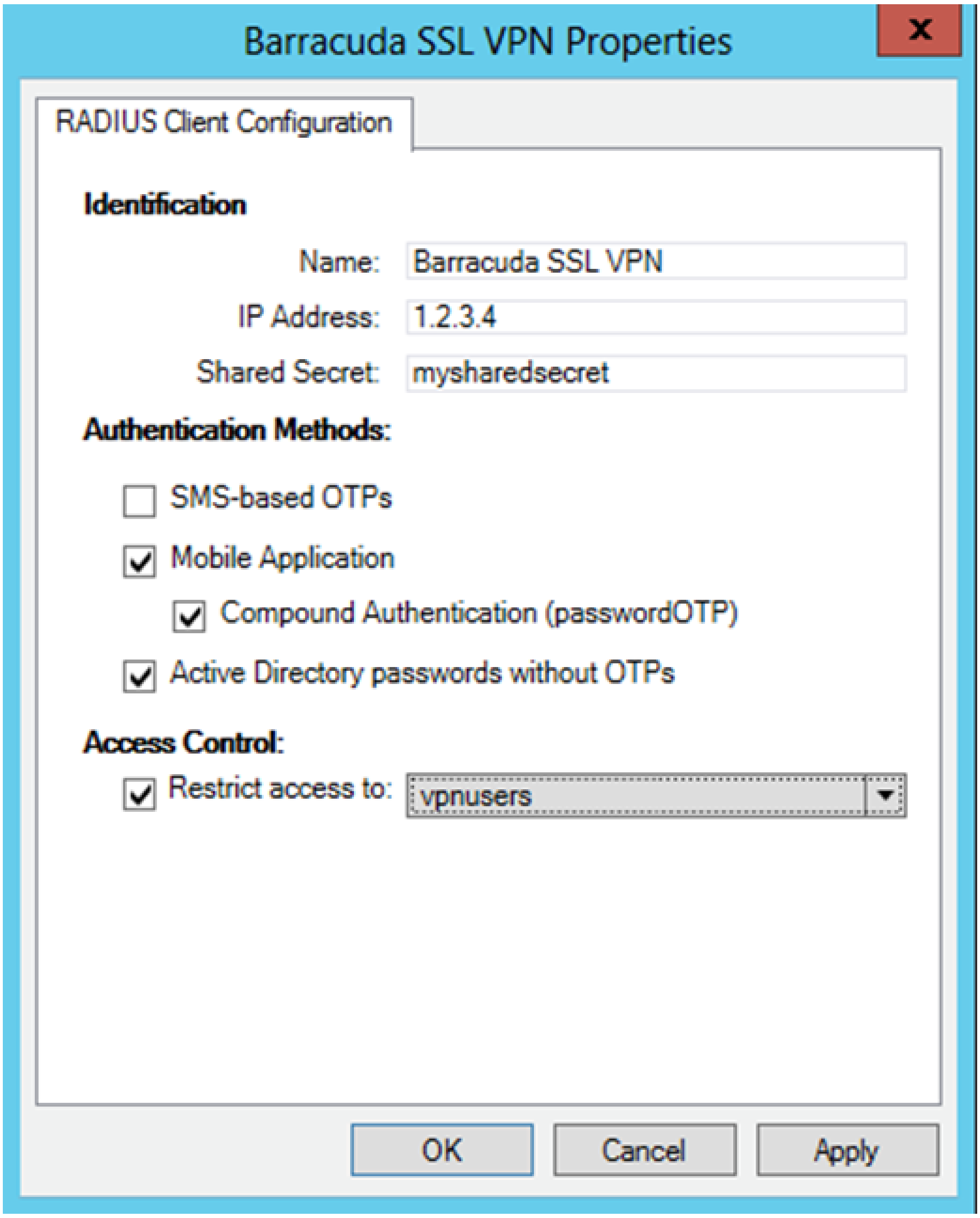
2. Prerequisites

Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Barracuda appliance configured as a client, as per 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 Barracuda SSL VPN appliance



Identification

Name: Barracuda SSL VPN

IP Address: 1.2.3.4

Shared Secret: mysharedsecret

Authentication Methods:

□ SMS-based OTPs

☑ Mobile Application

☑ Compound Authentication (passwordOTP)

☑ Active Directory passwords without OTPs

Access Control:

☑ Restrict access to: vpnusers

Figure 1

The RADIUS client settings for your Barracuda SSL VPN device. Note that the IP address is the internal address of your Barracuda appliance.

3. Integration instructions

1. Create a new authentication scheme:
   a. Login to your Barracuda admin interface.
   b. Click **Access Control** > **Authentication Schemes**.
   c. Create a new scheme using the following values:
      i. **Name**: ESA RADIUS
      ii. **Selected Modules**: Add RADIUS from the **Available Modules** list.
      iii. **Selected Policies**: Add your applicable policies from the **Available Policies** list.
   d. Click **Add**.

2. Configure the settings for your RADIUS server:
   a. Click **Access Control** > **Configuration**.
   b. In the **RADIUS** section, enter following values:
      i. **RADIUS server**: The IP address of your ESA RADIUS server
      ii. **Authentication Port**: 1812
      iii. **Backup RADIUS servers**: Add any redundant ESA RADIUS servers you have configured.
      iv. **Shared Secret**: As shown in **Figure 1**.
      v. **Authentication Method**: PAP
      vi. **Time out**: 30
      vii. **Authentication Retries**: 2
      viii. **Reject challenge**: No
   c. Click **Save changes**.

3. Test authentication:
   a. Navigate to the URL that you normally use for SSL VPN logins with your Barracuda appliance.
   b. Enter the credentials of your test user:
      i. Ensure that you are using a user that has been configured for Mobile Application 2FA using ESA.
      ii. In the password field, 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, then type Esa123999111.

4. Troubleshooting

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

1. Run a smoke test against your RADIUS server, as described in the **Verifying ESA RADIUS Functionality** document.
2. If no you are still unable to connect, revert to an existing sign-in configuration (that does not user 2FA) and verify that you are able to connect.
3. If you are still able to connect using the old settings, restore the new settings and verify that your firewall is not blocking UDP 1812 between your VPN device and your RADIUS server.
4. If you are still unable to connect, contact ESET technical support.