ESET

SECURE AUTHENTICATION

F5 FirePass SSL VPN
Integration Guide

ESET **SECURE AUTHENTICATION**

Copyright © 2013 by ESET, spol. s r.o.
ESET Secure Authentication was developed by ESET, spol. s r.o.
For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.
ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

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 for an F5 FirePass 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 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**).

- An F5 FirePass SSL VPN appliance. This configuration will also work with F5 BIG-IP APM series appliances. RADIUS configuration instructions for BIG-IP APMs may be found here.

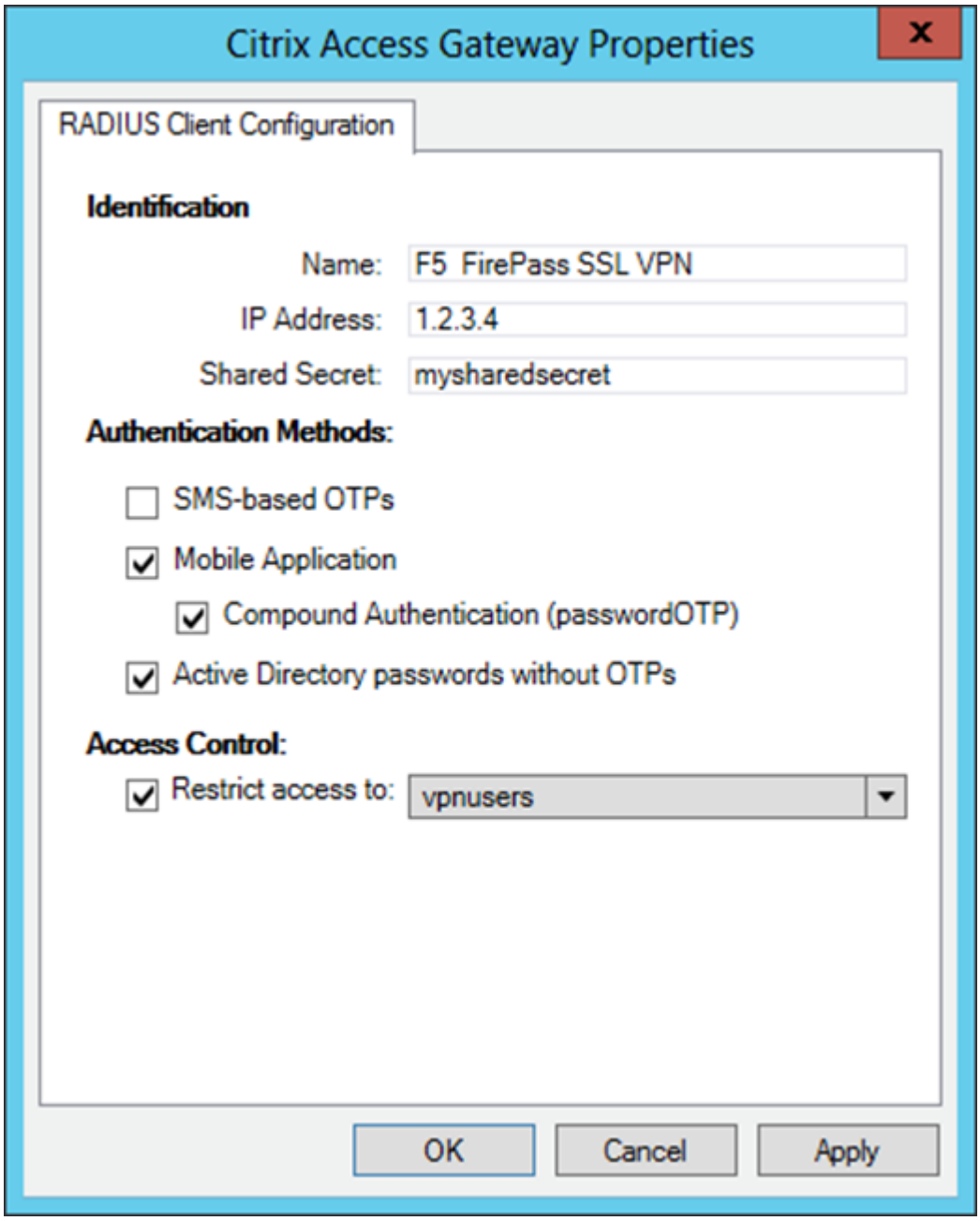

Figure 1

The RADIUS client settings for your F5 FirePass SSL 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 F5 Firepass appliance.

3. Integration instructions

1. Configure your appliance:
   a. Log into your F5 FirePass admin interface.
   b. Click **Users** on the left.
   c. Click **Groups**.
   d. Click **Master Groups**.
   e. Click **Create New Group** (or modify an existing group).
   f. Enter the following information:
      i. **New Group Name**: ESA
      ii. **Users in group**: external
      iii. **Authentication method**: RADIUS
   g. Click **Create**.
   h. Navigate to the **Authentication** tab for your new group.
   i. Enter the following information:
      i. **Timeout**: 30
      ii. **Retries**: 2
      iii. **Server**: The IP address of your ESA RADIUS server
      iv. **Port**: 1812
      v. **Shared Secret**: The shared secret you used, as per **Figure 1**.
      vi. **Confirm Shared Secret**: Same as above
   j. Click **Save Settings**.

2. Test the authentication:
   a. Navigate to the URL that you normally use for SSL VPN logins with your F5 FirePass 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 in Esa123999111.

4. Troubleshooting

If you are unable to authenticate via the ESA RADIUS server, ensure 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 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 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.