ESET

SECURE AUTHENTICATION

Citrix NetScaler 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 Citrix NetScaler SSL VPN appliance.

2. Prerequisites

Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Citrix NetScaler 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 Citrix NetScaler SSL VPN Appliance.

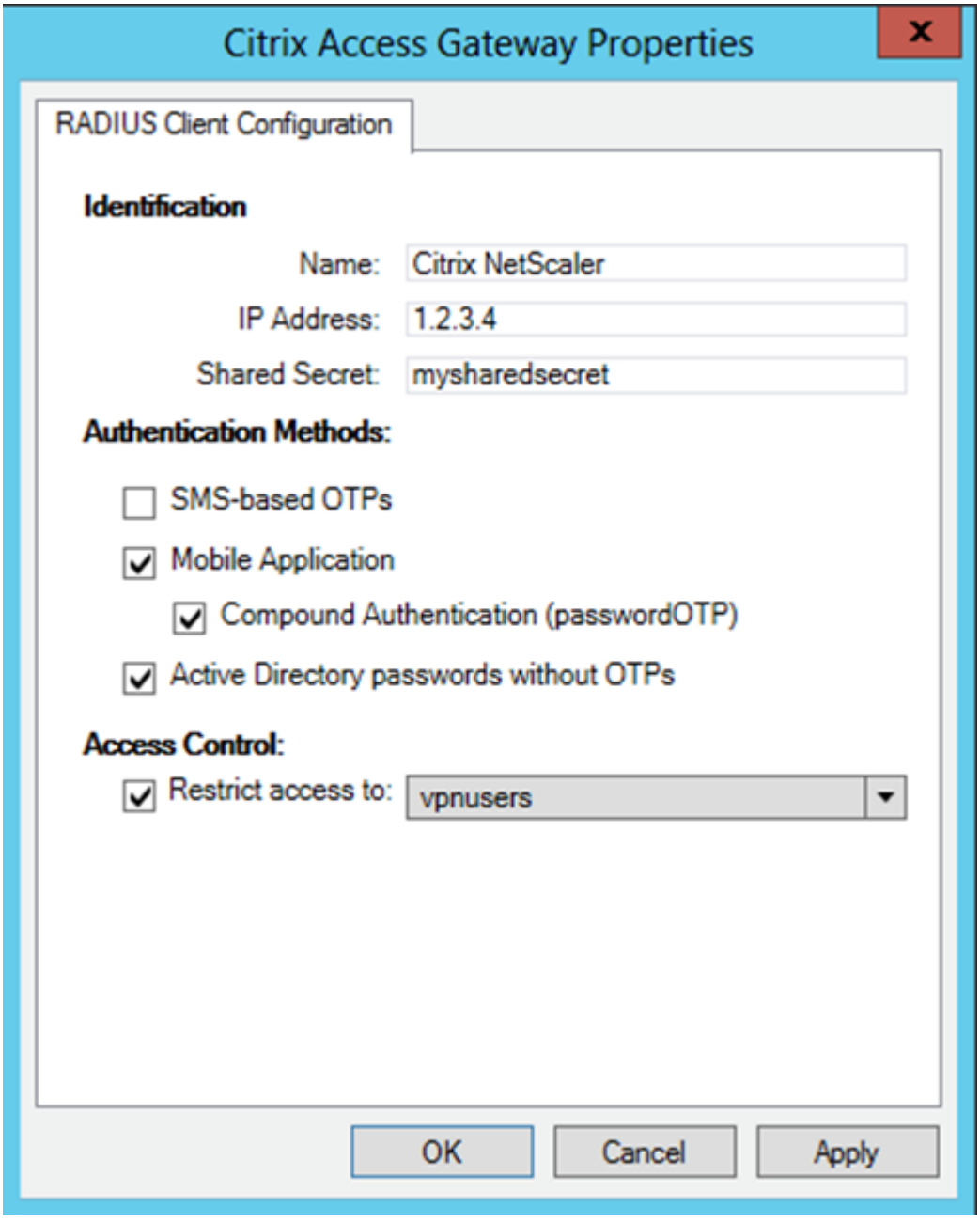

Figure 1

The RADIUS client settings for your NetScaler 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 Citrix appliance.

3. Integration instructions

1. Configure your appliance:
   a. Lo ginto your Citrix NetScaler administrative interface.
   b. Click **Access Gateway** > **Virtual Servers** on the left.
   c. Select your existing **Access Gateway Virtual Server**.
   d. Click **Open**.
   e. In the **Configure Access Gateway Virtual Server** window, navigate to the **Authentication** tab.
   f. In the **Authentication Policies** section, select **Primary** and then click **Insert Policy**.
   g. In the **Configure Authentication Policy** window, enter a name (e.g. ESA Authentication)
   h. In the same window, select **General** from the first drop-down menu and **true** from the second drop-down menu under **Named Expressions**.
   i. Click **Add Expression**.
   j. In the same window, next to the **Servers** field, click **New...**, and enter the following values in the new window:
      i. **Name**: ESA RADIUS
      ii. **IP Address**: The IP Address of your ESA RADIUS Server
      iii. **Secret Key**: As shown in **Figure 1**
      iv. **Confirm Secret Key**: Same as above
      v. **Password Encoding**: PAP
   k. Click **OK**.
   l. Click **OK**.
   m. Click **OK**.
   n. Click **Save**.

2. Test the authentication:
   a. Navigate to your regular URL used for SSL VPN logins
   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.