ESET SECURE AUTHENTICATION

Check Point Software 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 Check Point Software SSL VPN appliance.

2. Prerequisites

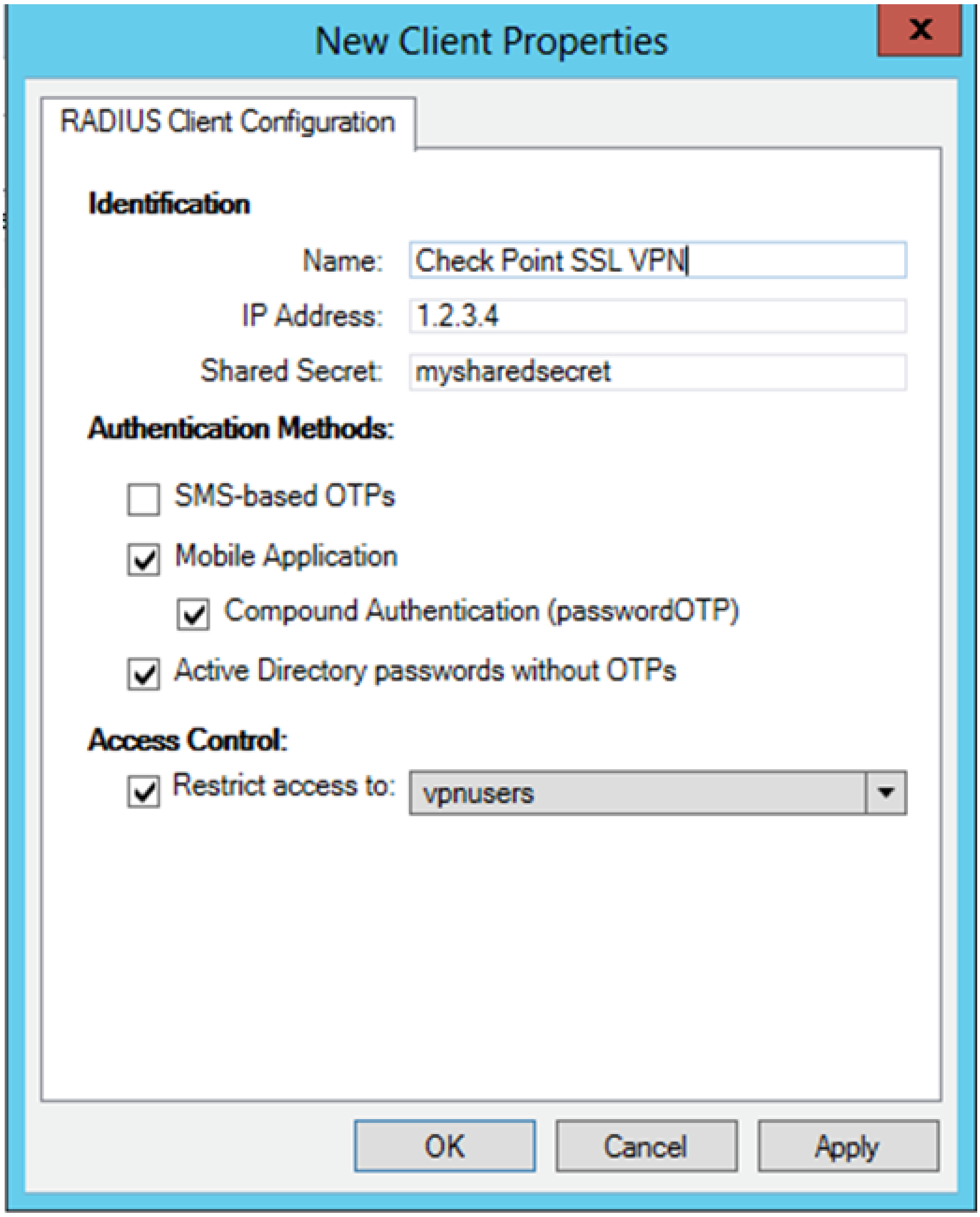
Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Check Point SSL VPN configured as a client, as per **Figure 1**.

Note: To prevent locking any existing, non-2FA enabled AD users from your VPN, it is recommended that you allow Active Directory passwords without OTPs during the transitioning phase. It is also recommended to limit vpn access to a security group (**vpnusers** in this example).

- A Check Point Software SSL VPN Appliance. Known supported appliances are:

VPN-1
Firewall-1



New Client Properties

Identification

Name: Check Point 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 Check Point Software 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 Check Point Software appliance.

3. Integration instructions

1. Add a new RADIUS server:
   a. Open your **Check Point SmartDashboard**.
   b. Expand the **Servers and OPSEC Applications** page.
   c. Right-click **Servers** and select **New** > **RADIUS...**.
   d. Name your new server (for example, ESA).
   e. Click **New** next to the **Host** field.
   f. Select **General Properties** on the left.
   g. Add a name for the server, which may not be the same name you chose in step d. (for example, ESAradserv).
   h. Enter the IPv4 address of your ESA RADIUS server.
   i. Click **OK**.
   j. Select **New Radius** (for port 1812) from the **Service** drop-down menu.
   k. Enter your shared secret, as per **Figure 1**.
   l. Select PAP as the protocol.
   m. Click **OK**.

2. Create a test user:
   a. Navigate to and expand **Users and Administrators**.
   b. Right click **Users** and select **New User** > **Default...**.
   c. In the user properties window, under the **general** tab, enter the AD user name of your test user (e.g., Alice)
   d. In the **Authentication** tab:
      i. Set the authentication scheme to **RADIUS**.
      ii. Select the server you created in step 1-d (for example, ESA).
   e. Click **OK**.

3. Test the authentication:
   a. Launch your **SecureClient**.
   b. Enter the credentials of your test user from step 2:
      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 use 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.