ESET

SECURE AUTHENTICATION

Cisco ASA 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 Cisco ASA Series appliance set up for SSL VPN access.

2. Prerequisites

Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Cisco Internet Protocol Security (IPSec) SSL VPN 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 Cisco ASA Series Appliance. The supported appliances are:

  5505
  5510
  5520
  5540
  5550
  5580-20
  5580-40
  5585-X-SSP20
  5585-X-SSP60

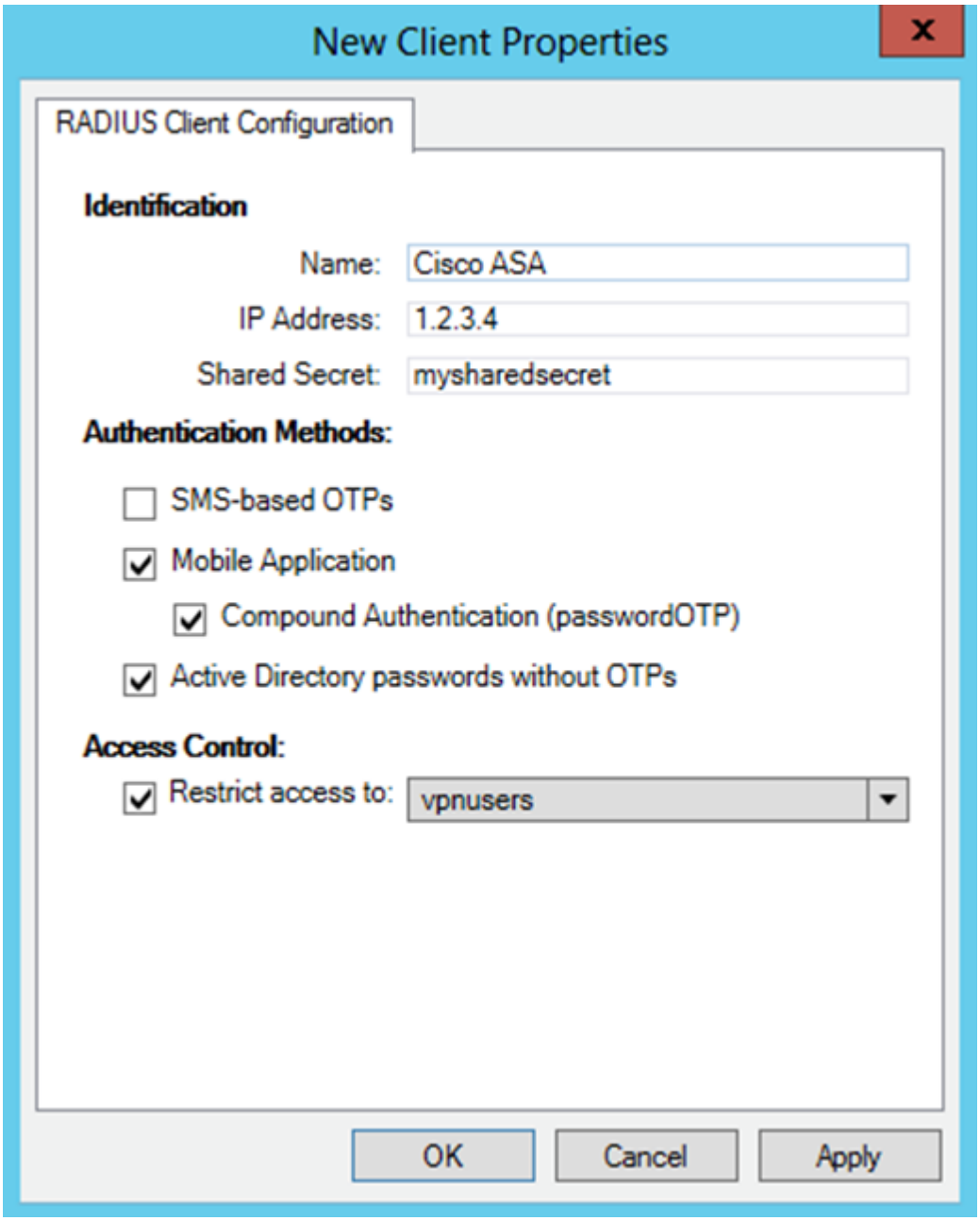

Figure 1

In this picture, you can see the RADIUS client settings for your Cisco ASA device. Note that the check boxes next to **Mobile Application** and **Compound Authentication (passwordOTP)** must be selected, and that the IP address is the originating address of packets from your Cisco ASA VPN appliance.

3. Integration instructions

1. Configure your ASA device:
   a. Login to your **Adaptive Services Device Manager** (ASDM).
   b. Navigate to **Configuration** > **Remote Access VPN**.
   c. Click **Clientless SSL VPN** > **Connection Profiles**.
      i. Ensure that the check box below **Allow access** is selected on the relevant interface (Figure 2, step 1).
   d. Click **Add** under **Connection Profiles** (Figure 2, step 2).

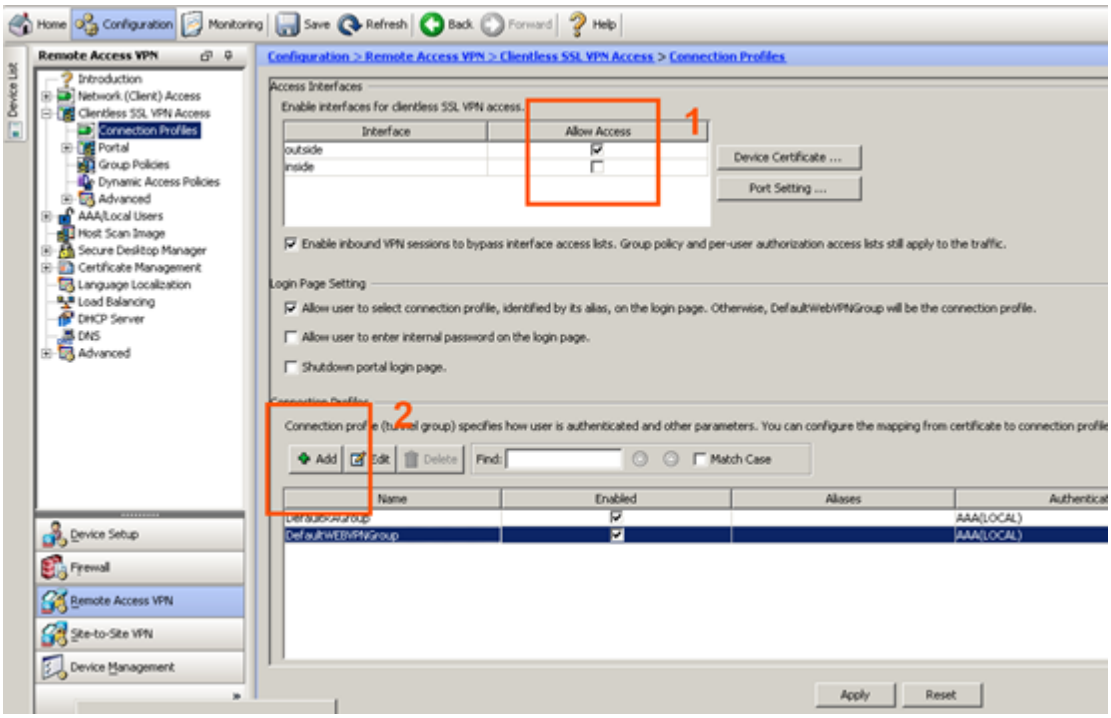

Figure 2

   e. In the **Basic** tab of the **Add Clientless Remote Access Connection Profile** window:
      i. Select a name for your connection profile (for example, **ESA**).
      ii. Ensure that the authentication method is set to AAA only.
      iii. In the **Authentication** section, click **Manage**:
         1. Click **Add** under **AAA Service Groups**.
      iv. Enter a name for the new group, (e.g., **ESA-RADIUS**), ensure that the protocol is set to **RADIUS** and then click **OK**.
      v. Select your **Server Group** and then click **Add** in the selected group panel.
      vi. Enter the following (as shown in **Figure 3**):
         1. **Interface Name**: The ASA interface on which your ESA RADIUS server may be reached.
         2. **Server Name or IP Address**: The hostname/IP address of your ESA RADIUS server.
         3. **Timeout**: 30 seconds
         4. **Server Authentication Port**: 1812 (only change if you are overriding this value).
         5. **Server Accounting Port**: 1813.

6. **Retry Interval**: 10 seconds
7. **Server Secret Key**: The Shared Secret as in **Figure 1**.
8. **Microsoft CHAPv2 Capable**: Not selected

vii. Click **OK**.

viii. Click **OK**.

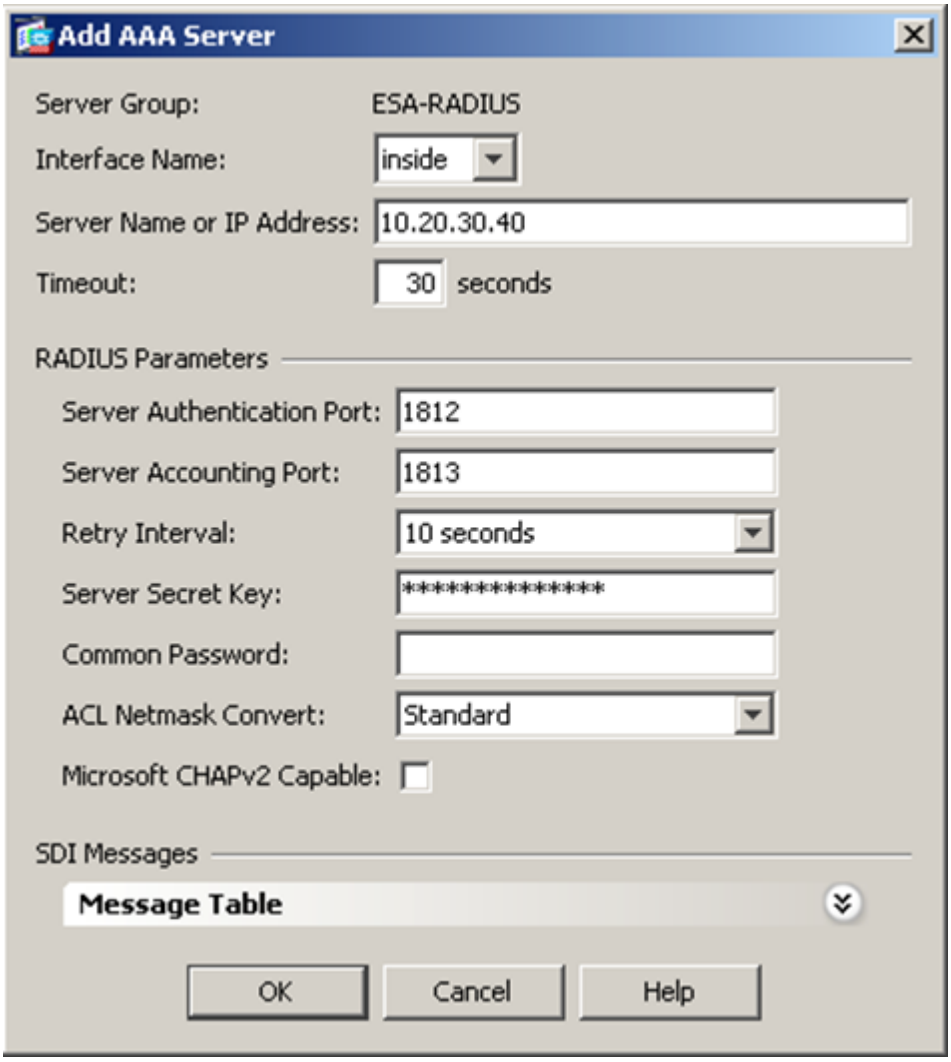

Figure 3

2. Testing the connection:

   a. Connect to your ASA VPN using a user that has been enabled for 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, and 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. Verify that the IP address used in **Figure 1** is the correct IP address.
3. If you are still unable to connect, revert to an old **Connection Profile** on the ASA device's ASDM and verify that you are able to connect to the VPN.
4. If you are able to connect using the old profile, restore the new profile and verify that there is no firewall blocking UDP 1812 between you VPN device and your RADIUS server.
5. If you are still unable to connect, contact ESET technical support.