ESET

SECURE AUTHENTICATION

Cisco ASA Internet Protocol Security (IPSec) 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 IPsec VPN access.

2. Prerequisites

Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Cisco 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 following appliances are supported:

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

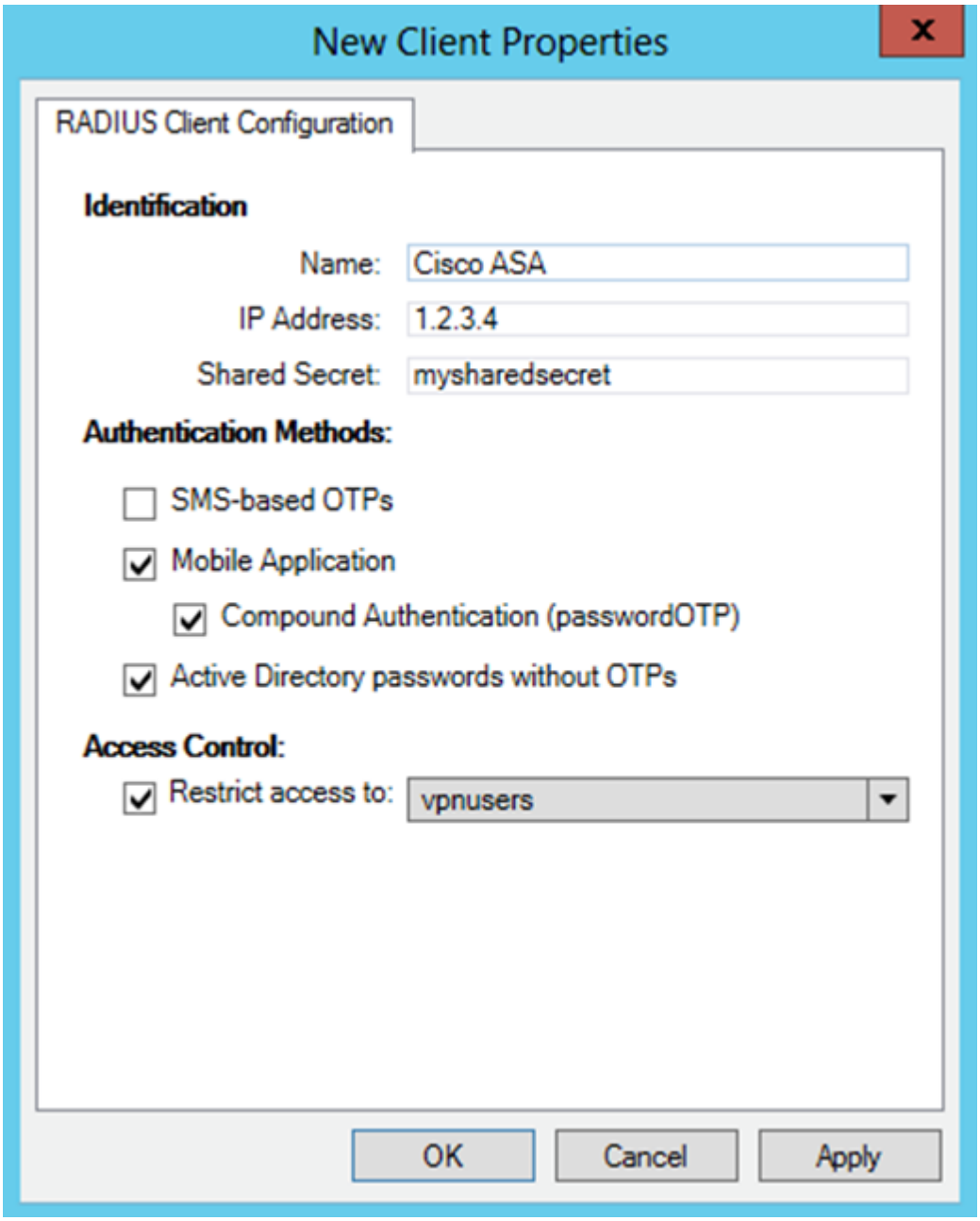

Figure 1

In this screenshot, you can see the RADIUS client settings for your Cisco ASA appliance. 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 **Network (client) Access** > **IPSec (IKEv1) Connection Profiles**.
    d. Create a new Connection Profile
    e. In the **Basic** tab of the **IPsec Remote Access Connection Profile** window:
        i. Under **IKE Peer Authentication**, enter the pre-shared key that will be entered into each end-user's VPN client. It should be a strong password.
        ii. In the **Authentication** section, click **Manage**.
        iii. Under **AAA Service Groups**, click **Add**.

iv. Enter a name for the new group, (for example., **ESA-RADIUS**), ensure that the protocol is set to **RADIUS** , then click **OK**.

v. Select your **Server Group** and click **Add** in the **Servers in selected group** panel.

vi. Enter the following (as shown in **Figure 2**):

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**: N/A since ESA does not support RADIUS accounting, but set to 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**.

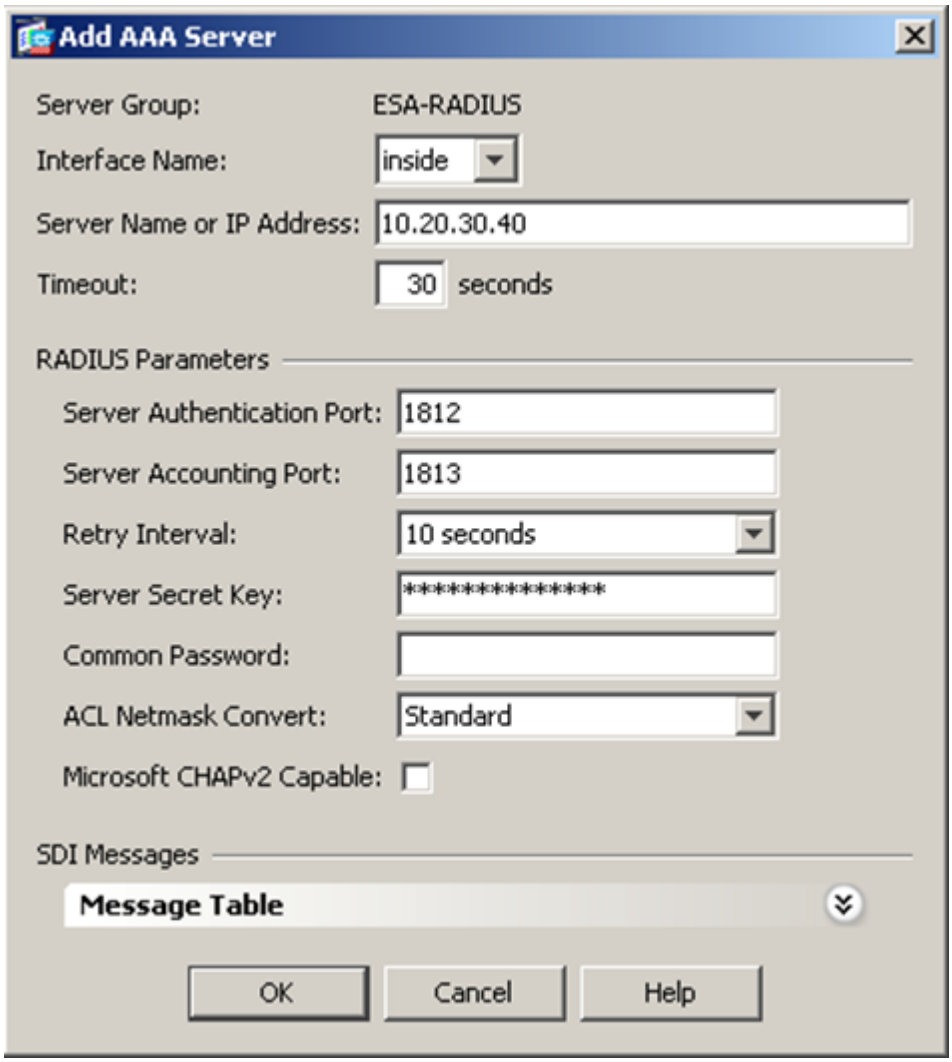

Figure 2

f. Click **PPP** in the left panel:

i. Ensure that only **PAP** is selected.

g. Click **Client Address Assignment**:

i. Select or create the DHCP pool you want to use.

ii. Click **OK**.

h. Click the **Default Group Policy** section:

i. Select the policy you want to use.

ii. Verify that **Enable IPsec Protocol and Enable L2TP IPsec Protocol** are checked.

i. Click **OK**.

2. Testing the connection:

a. Make sure your VPN client is configured correctly:

i. Verify that the **Group Authentication** radio button is selected in the **Authentication** tab of the VPN client's connection properties.

ii. Make sure that the pre-shared key used in step 1-e-i is entered into both **password** fields.

b. Connect to your IPSec 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.