ESET Tech Center

How do I configure my Cisco® ASA SSL VPN device for use with ESET Secure Authentication?

Ondersteuning | ESET Nederland - 2017-11-28 - Comments (0) - ESET Secure Authentication

https://support.eset.com/kb3481

Introduction

This article describes how to configure a Cisco® ASA SSL VPN device to authenticate users against an ESA Server. Before proceeding, verify that you've installed the RADIUS Server component of ESET Secure Authentication and can access the RADIUS service that allows external systems to authenticate users.

Before your Cisco® ASA SSL VPN device can use the ESA Server to authenticate users via RADIUS, it must be set up as a RADIUS client on the ESA Server. Next, your server running the ESA RADIUS service must be setup as a RADIUS Server on the Cisco® ASA SSL VPN device. Once these configurations have been specified, you can start logging into your Cisco® ASA SSL VPN device using ESA OTPs.

> NOTE:
>
> This integration guide utilizes **VPN does not validate AD user name and password** VPN type for this particular VPN appliance. If you wish to utilize other VPN type, refer to generic description of VPN typesand verify with the vendor if the VPN appliance supports it.

Step I - RADIUS client configuration

To allow the Cisco® ASA SSL VPN device to communicate with your ESA Server, you must configure the Cisco® ASA SSL VPN device as a RADIUS client on your ESA Server:

1. Launch the **ESA Management Console** (found

under **Administrative Tools**).
2. Navigate to **RADIUS Servers** and locate the hostname of the server running the ESA RADIUS service.
3. Right-click the hostname and select **Add Client** from the context menu.
4. Configure a RADIUS client (see Figure 1-1).
5. Click **OK** - you will be prompted to restart the RADIUS Service, do so from the Services control panel.

Configuring your RADIUS client

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**). Make sure that the check box next to **Mobile Application** is selected.

Figure 1-1

ESA has now been configured to communicate with the Cisco® ASA SSL VPN device. You must now configure the Cisco® ASA SSL VPN device to communicate with the ESA Server.

Step II - Configure your Cisco® ASA device

Follow the steps below:

1. Log into your Adaptime Services Device Manager.
2. Navigate to **Configuration → Remote Access VPN**.
3. Click **Clientless SSL VPN → Connection Profiles** and ensure that the check box below **Allow access** is selected on the relevant interface (see Figure 2-1, step 1).
4. Click **Add** under **Connection Profiles** (see Figure 2-1, step 2).
    1. Navigate to the **Basic** tab of the **Add Clientless Remote Access Connection Profile** window.
    2. Type a name for your connection profile (for example, **ESA**).
    3. Ensure that the authentication method is set to **AAA only**.

4. Click **Manage** in the **Authentication** section and define a new service group:

    i. Click **Add** under **AAA Service Groups**.
    ii. Enter a name for the new group (for example, **ESA-RADIUS**), ensure that the protocol is set to to **RADIUS** and click **OK**.
    iii. Select your **Server Group** and click **Add** in the **Servers in selected group** panel.
    iv. Set the following parameters to the values shown below (see Figure 2-2):

        i. **Interface Name:** The ASA interface on which your ESA RADIUS server may be reached
        ii. **Server Name or IP Address:** The hostname/IP address of your ESA RADIUS server
        iii. **Timeout:** 30 seconds
        iv. **Server Authentication Port:** 1812
        v. **Server Account Port:** N/A since ESA does not support RADIUS accountint, but set to 1813
        vi. **Retry Interval**: 10 seconds
        vii. **Server Secret Key:** Your RADIUS server shared secret (see Figure 1-1)
        viii. **Microsoft CHAPv2 Capable**: Not selected

    v. Click **OK**
    vi. Click **OK**

Figure 2-1

Figure 2-2

Step III - Test the connection

To test the newly configured connection:

1. Connect to your ASA VPN using an account with Mobile Application 2FA using ESA enabled. 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, type Esa123999111.

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 per Verifying ESA RADIUS Functionality.
2. If no faults were fixed and 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 there is no firewall blocking UDP 1812 between you VPN device and your RADIUS server
4. If you are still unable to connect, contact ESET technical support.

- Tags
- ESA