ESET SECURE AUTHENTICATION

Palo Alto SSL VPN Integration Guide
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Overview</td>
<td>4</td>
</tr>
<tr>
<td>2. Prerequisites</td>
<td>5</td>
</tr>
<tr>
<td>3. Integration instructions</td>
<td>6</td>
</tr>
<tr>
<td>4. Troubleshooting</td>
<td>7</td>
</tr>
</tbody>
</table>
1. Overview

This document describes how to enable ESET Secure Authentication (ESA) Two-Factor Authentication (2FA) for a Palo Alto Next-Generation Firewall appliance.

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 types and verify with the vendor if the VPN appliance supports it.
2. Prerequisites

Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Palo Alto SSL VPN 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 Palo Alto Next-Generation SSL-VPN Appliance. The supported appliances are:
  
  - PA-5000 Series Firewall
  - PA-4000 Series Firewall
  - PA-2000 Series Firewall
  - PA-500 Series Firewall
  - VM-Series

![Palo Alto Properties](image)

**Figure 1**
This screenshot shows the RADIUS client settings for your Palo Alto 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 Palo Alto appliance.

3. Integration instructions

1. Add a RADIUS server profile:
   a. Using a web browser, log in to the Palo Alto administrative interface.
   b. Click the Device tab, navigate to Server Profiles and click RADIUS on the left.
   c. Click Add to add a new RADIUS server profile.
   d. Name your server profile (for example, ESA).
   e. In the Server list section, click Add and add the details of your RADIUS server:
      i. IP Address: The IP Address of your ESA RADIUS server
      ii. Shared Secret: The shared secret you used when adding the Palo Alto SSL VPN as a client (for example, mysharedsecret in Figure 1)
      iii. Port: 1812
   f. Click OK to save the RADIUS profile.

2. Add an Authentication Profile:
   a. In the Device tab, click Authentication Profile.
   b. Click New.
   c. Name the profile, for example, ESA 2FA.
   d. Select RADIUS from the Authentication drop-down menu.
   e. Select the RADIUS profile that you created in step 1.d for example, ESA from the Server Profile drop-down menu.
   f. Click OK to save your changes.

3. Configure the SSL-VPN:
   a. Navigate to SSL-VPN under the Network tab.
   b. If you are modifying an existing profile, click it to edit its settings, otherwise click Add.
   c. Select the Authentication Profile that you created in step 2.c. from the Authentication Profile drop down menu.
   d. After verifying your other VPN settings, click OK to save changes.

4. Testing the connection:
   a. Connect to your Palo Alto VPN using a user account configured 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, 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 your old Authentication Profile on the VPN device and verify that you are able to connect.
3. If you are able to connect with the old profile, restore the new profile 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.