# Table of Contents

Table of Contents ........................................................................................................................................2

1.0 Introduction ........................................................................................................................................3
  1.1 Scope of Document ............................................................................................................................3
  1.2 Prerequisites .......................................................................................................................................3

2.0 GlobalProtect Configuration ..................................................................................................................4
  2.1 Configuring User Authentication ........................................................................................................5
  2.2 Authentication Profile ........................................................................................................................6
  2.3 Configuring the SSL VPN Global Protect ............................................................................................7
    2.3.1 Configuring the security zone ........................................................................................................7
    2.3.2 Configuring the tunnel interface ....................................................................................................8
    2.3.3 Configuring the SSL Certificate ..................................................................................................10
    2.3.4 Configuring the portal ................................................................................................................12
    2.3.5 Configuring the gateway ..............................................................................................................15

3.0 AAA Configuration: Sequence of Procedures ......................................................................................18
  3.1 Procedure 1: Configure the PALO ALTO NETWORKS Gate ..............................................................18
  3.2 Procedure 2: Assign Group(s) to the PALO ALTO NETWORKS Gate ................................................19
  3.3 Procedure 3 (optional): Create An Out-of-Band Delivery Gateway ................................................21
  3.4 Procedure 4 (optional): Assign An SMS Token ................................................................................23

4.0 Sample Authentication ..........................................................................................................................24
1.0 Introduction

Palo Alto Networks GlobalProtect provides security for host systems, such as laptops, that are used in the field by allowing easy and secure login from anywhere in the world. With GlobalProtect, users are protected against threats even when they are not on the enterprise network, and application and content usage is controlled on the host system to prevent leakage of data, etc. This document covers the configuration of GlobalProtect with ActivID AAA for remote access VPN with HID Global solutions.

The HID Global Identity Assurance solutions that work with Palo Alto Networks incorporate VPN solutions that are versatile, with strong authentication that is flexible, scalable, and simple to manage. HID Global Identity Assurance offers two solutions:

- ActivID® AAA Server for Remote Access addresses the security risks associated with a mobile workforce remotely accessing systems and data.
- ActivID® Appliance offers support for multiple authentication methods that are useful for diverse audiences across a variety of service channels (SAML, Radius, etc.), including user name and password, mobile and PC soft tokens, one-time passwords, and transparent Web soft tokens.

1.1 Scope of Document

This document describes how to set up ActivID AAA authentication with Palo Alto Networks GlobalProtect to enable authentication via a hard/soft token or an OTP received by Email/SMS using an SSL-protected Palo Alto Networks VPN.

1.2 Prerequisites

- ActivID AAA Server is up-to-date (version 6.7) with LDAP users and groups already configured.
- For OOB authentication (optional):
  - There is an existing Short Message Peer-to-Peer Protocol (SMPP) gateway to send one-time-password OOB codes to users.
  - User phone numbers are declared in a functioning LDAP server.
- Palo Alto Networks PAN OS 6.0 and later
- GlobalProtect is already installed
2.0 GlobalProtect Configuration

1. Launch a supported web browser and enter the URL of the PAN management interface
   https://ip_mgt_address
2. The browser automatically opens the Palo Alto Networks login page.
3. Enter admin in both the **Name** and **Password** fields, and click **Login**.
2.1 Configuring User Authentication

Identify the authentication method that will be used to authenticate GlobalProtect users. Palo Alto Networks next-generation firewalls support local database, LDAP, RADIUS or Kerberos authentication servers for authenticating users.

In this case we will use the ActivID AAA (Radius Server) for authenticating users.

1. Navigate to **Device > Server Profiles > Radius**.

2. Specify the **ActivID AAA IP address, port** and the **shared secret**.

3. Click **OK**.
2.2 Authentication Profile

The authentication profile refers to the authentication method configured in the previous step. The authentication profile is then used to associate the authentication method in the GlobalProtect Portal configuration.

To create an authentication profile for the radius users created above:

1. Click on the Device tab

2. From the left pane, click Authentication Profile and click Add.

3. Enter a Name for the profile.

4. Choose the authentication method as RADIUS.
5. Select the HID server created previously (e.g., HID_IDP).
6. Click OK.
7. If only certain users groups are authorized, in the “allow list”, specify the groups authorized and remove “all” which is set by default.

**Important:** When you specify a specific group, you must use a specific RADIUS dictionary on the AAA Server and also create an authorization profile. For more information on this topic, refer to the guide named 4TRESS_AAA_AdminGuide.pdf, specifically the section called Create a New RADIUS Authorization Profile. Also refer to the following vendor-specific requirements: https://live.paloaltonetworks.com/docs/DOC-3189.

2.3 Configuring the SSL VPN Global Protect

You must configure the SSL connection and related attributes in order utilize the GlobalProtect functionality:

- **Portal** - Palo Alto Networks firewall that provides centralized management for the GlobalProtect system.
- **Gateways** - Palo Alto Networks firewalls that provide security enforcement for traffic from GlobalProtect agents.

The following sections describe the steps for the attributes that must be configured:

2.3.1 Configuring the Security zone

A security zone identifies one or more sources or destination interfaces on the firewall. When you define a security policy rule, you must specify the source and destination security zones of the traffic.

In our example, we have created “layer 3” zone named “VPN SSL” in order to identify traffic come from VPN SSL users.

1. To create this zone, click on the tab **Network**

2. From the left pane, click **Zones**.
3. Click **Add** to add a new zone.

4. Enter a **Name** for the zone.

5. Choose **Layer 3** for type.

6. Select **Enable User Identification**.

7. Click **OK**.

2.3.2 Configuring the tunnel interface

Each SSL connection (like a tunnel) is bound to a tunnel interface. It is necessary to assign the tunnel interface to the same virtual router as the incoming (clear text) traffic. This way, when a packet comes to the firewall, the route lookup function can determine the appropriate tunnel to use. The tunnel interface appears to the system as a normal interface, and the existing routing infrastructure can be applied.

In our example, the interface "**tunnel.10**" will be used for the VPN SSL traffic.
1. To create this tunnel interface, click on the tab **Network**, then on the left pane, click **Interfaces**, and then click on the sub-tab **Tunnel**

![Network interface screenshot]

2. Click **Add** to add a new tunnel.
3. Enter an **ID** for the tunnel (“10”).

![Tunnel interface screenshot]

4. Assign the security zone created previously (in our example “VPN SSL”).
5. Click **OK**.
2.3.1 Configuring the SSL Certificate

This section describes how to create the SSL certificate which is presented when the users establish the VPN SSL connection.

1. To create or import the SSL Certificate, click on the tab **Network**, then from the left pane click **Certificate**.

2. If you have requested a certificate to a Certification Authority (e.g., VeriSign), you can import it by clicking **Import**.
Click **Generate** to create a CSR for a self-signed certificate.

3. Confirm that the new certificate can be seen in the GUI.
2.3.2 Configuring the portal

Portal configuration requires, specifying the certificate required by the gateway, authentication method used by portal, and optional agent certificates.

1. Click on the tab **Network**, then from the left pane, click **Interfaces > GlobalProtect > Portal**.

2. In the **Network Settings** section configure the following:
   - **Interface**: from the drop down menu, select the public interface used by end users to connect to the VPN SSL.
   - **IP address**: from the drop down menu, choose the IP of the interface you choose in the precedent step.
   - **Server Certificate**: from the drop down menu, choose the Certificate created for GlobalProtect.
3. In the *Authentication* section, for *Authentication Profile*, select the authentication profile defined previously.

4. Using the menu from the left pane, click *Client Configuration*. 
5. Click **Add** to define the VPN SSL policies for your users in order to assign the VPN SSL gateway your users have to use.
   - In the **General** tab, give a **Name** to the profile
   - Choose the **Connect Method**, in this example “on-demand” is chose as client certificate authentication is not required

6. In the **User/User Group** tab select the users. In this example, **any** users was selected
7. In the Gateways tab, define the external gateway where the users selected in the precedent step are redirected. In our example, we have only one gateway and all users are redirected to this gateway.

8. In this example, configurations under the Agent and Data Collection tab are optional.
9. Click OK.

2.3.3 Configuring the gateway

1. Click on the Network tab

2. From the left pane, click Interfaces > GlobalProtect > Gateway > General Tab.
3. Choose the server certificate and the user authentication profile defined previously.

4. Click the tab **Client configuration** on the left pane.

5. Under the sub-tab **Tunnel Settings**, select the **Tunnel Interface** created previously ("tunnel.10").
6. Under the sub-tab *Network Settings*:
   - Define the primary and secondary DNS, the suffix DNS, the WINS servers.
   - Define the IP address assigned to the devices connected via the VPN SSL.
   - Define the destination network routed via the VPN SSL.

7. Under the sub-tab *HIP Notification* you can optionally define the HIP notification policy.

8. Click **OK**.

9. Click **Commit** to complete the configuration.

10. Click **OK** to confirm
3.0 AAA Configuration: Sequence of Procedures

This chapter describes how to configure the ActivID AAA Authentication Server.

3.1 Procedure 1: Configure the PALO ALTO NETWORKS Gate

A gate for the ActivID AAA Server is a group of Network Access Servers (NAS) that is used to simplify administration. For configuration details, please refer to ActivID AAA Server technical documentation.

1. In the tree in the left pane of the Administration Console, expand the Servers line.
2. Right-click on the server to which you want to add a gate, and then click New Gate.

   ![New Gate On Server Server CLIENT04](image)

   - **Gate name**: PAN
   - **Dictionary**: default.rad
   - **Authorized IP addresses and host names**: 10.16.72.149
   - **Default Profile**
     - **Authorization**: <NONE>
     - **Accounting**: <NONE>

3. Enter a **Gate name** (can be any string).
4. Select the **RADIUS** option.
5. Use the Authorized IP addresses and host names section to specify filter(s) for the gate.
6. Click **Add**, and then click **OK**.

7. The ActivID AAA Server uses the RADIUS shared secret to encrypt data between **PALO ALTO NETWORKS** and the AAA authentication server. Click **Shared Secret**, and then modify the appropriate shared secret for your system.

8. Click **OK**.

### 3.2 Procedure 2: Assign Group(s) to the **PALO ALTO NETWORKS** Gate

Remember that you must have user groups created already and the corresponding LDAP configured. For details, refer to the *ActivID AAA Administration Guide*.

1. To assign groups to the **PALO ALTO NETWORKS** Gate, in the tree in the left pane, select the group that you want to assign to the gate.
2. Use the **Group / Gate Assignments** section of the page to specify gate(s) for the group’s users to utilize in order to access a protected resource.

3. Click **Add**.

4. Select the **Gate**, the **AZ profile**, and the **AC profile**.

5. Click **OK**.

**WARNING**: If you specified a specific RADIUS user group name in the Palo Alto Networks gate, then you must use an **AZ profile** with vendor specific attributes (see section 2.2 Authentication Profile).

6. To create an AZ profile, refer to *4TRESS_AAA_AdminGuide.pdf*.
3.3 Procedure 3 (optional): Create An Out-of-Band Delivery Gateway

ActivIdentity 4TRESS AAA supports OOB authentication (SMS) via phones. The actual SMS one-time password is a random number generated by the Appliance and sent to the end user through a delivery gateway. To create a gateway, perform the following steps using the AAA Server Administration Console.

1. Select **Tools**, and then click **Options**.
2. Select the **SMS Gateway** tab.

   ![AAA Server Administration Console Options](image)

3. Select the **Protocol** to use for sending the SMS to the cell phone.
4. For **SMS Center Address**, enter the IP address or domain name of the SMS Center’s server.
5. Enter the **SMS Center Port** number for the above server.
6. Enter the login and password credentials that the AAA Server uses to authenticate to the SMS Center server.
7. For **Cell Phone Number LDAP Attribute**, enter the attribute used by your organization’s LDAP directory for user phone numbers.
8. Customize the text of the message you want sent to users (for example, “Here’s your one time password:”) and then click **OK**.
9. Add two registry entries: one to activate the challenge-response mode for the SMS activation code and the other to customize the Activation message (that appears on the Palo Alto Networks page).

HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivPack\ActivPackServerV6
3.4 Procedure 4 (optional): Assign An SMS Token

You can assign an SMS Token for use as a primary authentication method to a single user or multiple users (bulk assignment).

10. From the AA Server Administration console, from the Devices menu, click SMS Token.

11. Use the search function to search for user(s) to whom you want to assign the token(s). To select multiple users, press either Shift + click or Ctrl + click.

12. Select the user or users from the list, and then click Set.
4.0 Sample Authentication

Configure the PAN agent to connect to the portal. Enter the username / password and Portal IP address or FQDN. Click on apply to connect.

Then log in using your username and the One-Time Password generated by your ActivID Token (the following illustration is using PC Token).

Copied to Clipboard.
Ready to paste into your application.
Another example, with OOB Authentication. The user enters his username and his OOB activation code.

And in the second page, his OTP received on his Mobile or mailbox:
The absence of a mark, product, service name or logo from this list does not constitute a waiver of the HID Global trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein are the trademarks of their respective owners. Any rights not expressly granted herein are reserved.