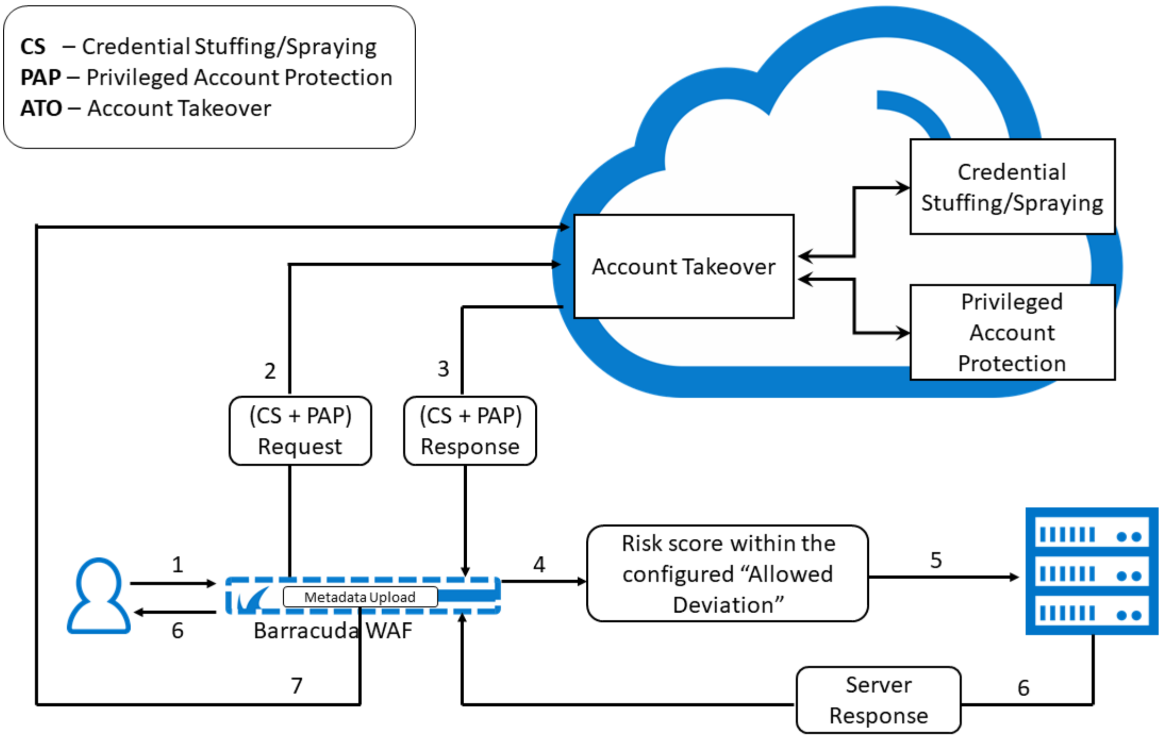
Privileged Account Protection

https://campus.barracuda.com/doc/96768651/

Privileged Account Protection is a part of the Account Takeover Protection provided by the Barracuda Web Application Firewall. In Privileged Account Protection, various session data elements, such as the connecting entity's geolocation, user agent, header value, and network details, are evaluated. If the risk score generated by Privileged Account Protection for connecting a client is within the configured permissible threshold, then the client is allowed to access the back-end application. If the risk score exceeds the threshold, a notification is sent to the administrator to flag the client for follow-up action. For details on the various types of follow-up actions, see Attacks Description - Action Policy.

Privileged Account Protection Workflow

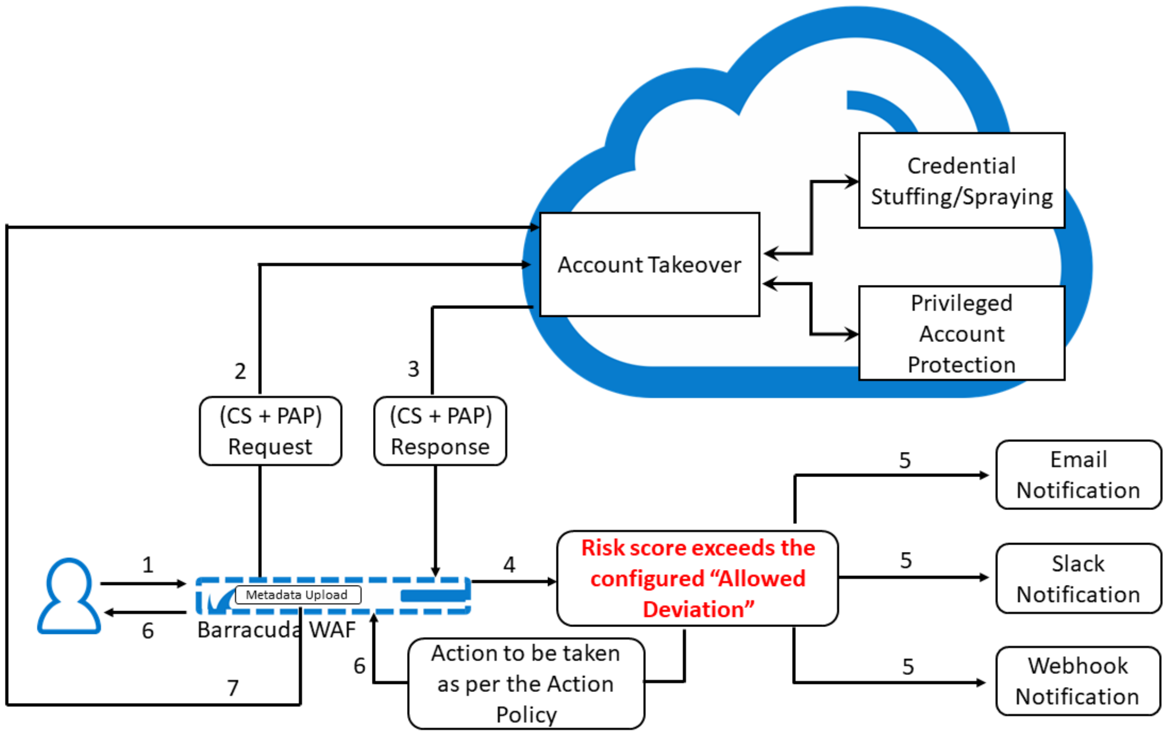
Workflow of Privileged Account Protection When the Allowed Deviation is Within the Specified Threshold:



1. User sends a login request to an application for which **Client Profiling** is enabled.
2. The Barracuda Web Application Firewall sends the credential stuffing/spraying and Privileged Account Protection request to the Account Takeover (ATO) cloud service. The request is evaluated for risk, and a risk score is generated.
3. The ATO service sends the response with the risk score to the Barracuda WAF.
4. The Barracuda WAF checks the risk score.
5. If the risk score is within the configured "Allowed Deviation" threshold, the request is forwarded

to the server.
6. The server sends the response to the Barracuda WAF, and the WAF forwards it to the user.
7. The Barracuda WAF uploads the metadata to the ATO cloud service.

Workflow of Privileged Account Protection When the Allowed Deviation Exceeds the Configured Threshold:



1. User sends a login request to an application for which Client Profiling is enabled.
2. The Barracuda Web Application Firewall sends the credential stuffing/spraying and Privileged Account Protection request to the Account Takeover (ATO) cloud service. The request is evaluated for risk, and a risk score is generated.
3. The ATO service sends the response with the risk score to the Barracuda WAF.
4. The Barracuda WAF checks the risk score.
5. If the risk score exceeds the configured “Allowed Deviation” threshold, an attack event alert is generated. Also, if Slack/Email and Webhook are configured, a notification is sent to the WAF administrator over Slack/email and by HTTP POST request to the configured Webhook URL.
6. The Barracuda WAF responds to the user as per the action policy configured for that attack event.
7. The Barracuda WAF uploads the metadata to the ATO cloud service.

To configure Privileged Account Protection:

1. Go to the **BOT MITIGATION > Bot Mitigation** page.
2. Select **Edit** under **Options** next to the URL policy for which you want to configure Privileged Account Protection.
3. On the **Edit URL Policy** page, scroll down to the **Account Protection** section and do the

following:
   1. **Enable User Account Profiling** – When set to **Yes**, Privileged Account Protection is enabled and parameters, such as a user's geolocation, user agent, network, are evaluated for the client before allowing the request.
   2. **Allowed Deviation** – Set the deviation to **Low**, **Medium** or **High**. When **Allowed Deviation** is set to **Low** and the risk score of the client exceeds the low deviation threshold, an ATO_DEVIATION_LOW_EXCEEDED attack is raised, and a notification with violation parameters is sent to the admin on the configured Webhook.
   3. **Webhook for Profile Deviation** – Specify the Webhook to receive notifications about the violations that occurred from the client. Webhook configuration can be any HTTPS application endpoint where notification messages can be sent using HTTP POST. Apart from the Webhook notification, a separate notification will be sent to admin’s email address or Slack channel, if configured.
   4. **Webhook Passphrase Option** - Select how you want to send the passphrase (**Header**, **Parameter** or **Not Required**) to the Webhook endpoint. Based on the option selected, the passphrase is sent through the header or query parameter in the name value pairs.
   5. **Passphrase Name** - Specify the name of the passphrase to be used in the name value pair.
   6. **Passphrase Value** - Specify the value of the passphrase to be used in the name value pair.
4. Specify values for other parameters as required and click **Save**.

Figures