Removing OpenVPN Handshake and Authentication Settings

Kaneesha D. - 2021-05-14 - Application & Features

In order to continue to provide PIA users with an application that provides the best stable connection to the VPN, PIA has decided to eliminate PIA-specific patches to OpenVPN.

In preparation for this migration, we will be removing some settings within our Desktop and Mobile applications that will no longer be supported.

Removed Settings:

Setting	Old Choices	New Setting
Data Authentication	(GCM cipher): GCM (CBC or no encryption): SHA1, SHA256, None	(GCM cipher): GCM
Handshake	RAS2048, RSA3072, RSA4096, ECC-256k1, ECC-256r1, ECC-521	RSA4096

Additionally, the Data Encryption choice of “None” will no longer be available (other settings will still be supported).

Motivation:

As previously stated, we are eliminating PIA-specific patches to OpenVPN on both Desktop and Mobile PIA applications. The elimination of these patches will allow us to provide our users with several benefits, such as:

- Improved compatibility with manual connections
- Reduced risk of issues due to custom patches
- More responsive deployment of OpenVPN updates for future improvements and fixes

These specific PIA patches were originally created to allow our users to customize the applications Encryption and Authentication settings on a per-connection basis, which was not supported by OpenVPN at the time. However, OpenVPN 2.4 and later supports cipher negotiation as a standard feature, which supersedes most of the functionality of the PIA patches.

With that being said, we will be eliminating the Data Authentication and Handshake settings, as they are no longer as relevant as they were when the patches were introduced. We will use the most secure option going forward.

Data Authentication

Using the Data Authentication setting is only relevant when using a CBC cipher. When using a GCM cipher (the default in the Desktop and iOS application), data authentication is provided as part of the GCM construction itself.

When connecting to the VPN, GCM ciphers are preferred over CBC as they are much more efficient when AES acceleration is present. For systems without AES acceleration, we recommend that users connect over WireGuard, as the most efficient software alternative. (This includes Intel/AMD processors older than approximately 2013, ARM processors without AES extensions, etc.).

For the reasons mentioned above, we have decided to drop the support for CBC ciphers, as such PIA users will no longer be able to alter our application settings to connect over these ciphers starting PIA 3.11.0 for Mobile applications and PIA 2.9.0 for Desktop applications.

Handshake

Using the Handshake setting determines how the client authenticates the VPN server (it determines the server certificate used). This setting does not impact the throughput or performance of the VPN connection. The default setting was RSA-2048, but after eliminating this setting the PIA application will now use RSA-4096 (the strongest option) for all connections connecting over OpenVPN.

When connecting over the WireGuard protocol, the PIA application already uses the RSA-4096 certificate to authenticate the server.

If you have any questions or issues please contact PIA Support by submitting a ticket here.

Tags

Authentication

Handshake

OpenVPN

Settings