What Encryption Can I Use?

Travis - 2022-06-29 - Encryption

Private Internet Access uses the open-source, industry-standard OpenVPN to provide you with a secure VPN tunnel. OpenVPN has many options when it comes to encryption.

Our users are able to choose what level of encryption they want on their VPN sessions. We try to pick the most reasonable defaults and we recommend most people stick with them. That being said, we like to inform our users and give them the freedom to make their own choices.

Suggested Encryption Settings
Default Recommended Protection

- Data encryption: AES-128-GCM
- Data authentication: GCM
- Handshake: RSA-4096

Maximum Protection

- Data encryption: AES-256-GCM
- Data authentication: GCM
- Handshake: RSA-4096

Data Encryption:

This is the symmetric cipher algorithm with which all of your data is encrypted and decrypted. The symmetric cipher is used with an ephemeral secret key shared between you and the server. This secret key is exchanged with the Handshake Encryption. All PIA OpenVPN connections use Advanced Encryption Standard encryption variants.

AES-128-GCM

- GCM provides higher security at some performance cost, while a 128-bit key provides a faster but less secure connection.

AES-256-GCM

- GCM provides higher security at some performance cost, while a 256-bit key provides a more secure but slower connection.

What's the difference between AES-CBC and AES-GCM?

Data Authentication:
This is the message authentication algorithm with which all of your data is authenticated. This is only used to protect you from active attacks.

GCM Cipher

- GCM is defined for block ciphers with a block size of 128 bits.
- Modern throughput rates with high speeds achievable on inexpensive hardware.

Handshake Encryption

This is the encryption used to establish a secure connection and verify you are really talking to a Private Internet Access VPN server and not being tricked into connecting to an attacker's server. We use TLS v1.3 to establish this connection. All our certificates use SHA512 for signing.

RSA-4096

- 4096-bit Ephemeral Diffie-Hellman (DH) key exchange and 4096-bit RSA certificate for verification that the key exchange really happened with a Private Internet Access server.

Warning about Elliptic Curves

The recent NSA revelations have raised concerns that certain or possibly all Elliptic Curves endorsed by US standards bodies may have backdoors allowing the NSA to more easily crack. There is no proof of this for curves used with signing and key exchange† and there are experts who think this to be unlikely. We, therefore, give users the option but display a warning anytime you select an Elliptic Curve setting. We also included the less standard curve secp256k1, which is what Bitcoin uses, was generated by Certicom (a Canadian company) instead of NIST (as the other curves were), and seems to have fewer places to hide a backdoor.

† There is strong evidence that a random number generator that uses ECC was backdoored but it was not widely used.

Glossary

Active Attacks

An active attack is one where an attacker gets "between" you and the VPN server, in a position where they can modify or inject data into your VPN session. OpenVPN was designed to be secure against active attackers as long as you are using both data encryption and data authentication.

Passive Attacks

A passive attack is one where an attacker simply records all data passing over the network

but does not modify or inject any new data. An example of a passive attacker is an entity that performs the dragnet capture and storage of all network traffic but does not interfere with or modify it. As long as you are using data encryption your OpenVPN session is secure against passive attackers.

Ephemeral Keys

Ephemeral keys are encryption keys that are generated randomly and only used for a certain amount of time, after which they are discarded and securely erased. An ephemeral key exchange is a process by which these keys are created and exchanged. Diffie-Hellman is an algorithm used to perform this exchange. The idea behind ephemeral keys is that once you are done using them and they are thrown away, no one will ever be able to decrypt the data which they were used to encrypt, even if they eventually got full access to all the encrypted data and to both the client and the server.

- You choose 'None' for Data Encryption
- You choose 'None' for Data Authentication
- You choose an ECC (Elliptic Curve Cryptography) option

Tags

Encryptions