What Encryption Can I Use?

Kaneesha D. - 2018-05-29 - in Frequently Asked Questions

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 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**

Data authentication: **SHA1**

Handshake: **RSA-2048**

All Speed No Safety

Data encryption: **None**

Data authentication: **None**

Handshake: **ECC-256k1**

Maximum Protection

Data encryption: **AES-256**

Data authentication: **SHA256**

Handshake: **RSA-4096**

Risky Business

Data encryption: **AES-128**

Data authentication: **None**

Handshake: **RSA-2048**

 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.

AES-128

Advanced Encryption Standard (128-bit) in CBC mode.
This is the *fastest* encryption mode.

Blowfish

Blowfish (128-bit) in CBC mode.

AES-256

Advanced Encryption Standard (256-bit) in CBC mode.

None

No Encryption. None of your data will be encrypted. Your login details **will** be encrypted. Your IP will still be hidden. This may be a viable option if you want the best performance possible while only hiding your IP address. This would be similar to a SOCKS proxy but with the benefit of not leaking your username and password.

 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. If you are not worried about active attackers you can turn off Data Authentication.

SHA1

HMAC using Secure Hash Algorithm (160-bit).
This is the *fastest* authentication mode.

Blowfish

Blowfish (128-bit) in CBC mode.

SHA256

HMAC using Secure Hash Algorithm (256-bit).

None

No Authentication. None of your encrypted data will be authenticated. An active attacker could potentially modify or decrypt your data. This would not give any opportunities to a passive attacker.

 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 v1.2 to establish this connection. All our certificates use SHA512 for signing.

RSA-2048

2048bit Ephemeral Diffie-Hellman (DH) key exchange and 2048-bit RSA certificate for verification that the key exchange really happened with a Private Internet Access server.

RSA-3072

Like RSA-2048 but 3072-bit for both key exchange and certificate.

RSA-4096

Like RSA-2048 but 4096-bit for both key exchange and certificate.

ECC-256k1

Ephemeral Elliptic Curve DHkey exchange and an ECDSAcertificate for verification that the key exchange really happened with a Private Internet Access server. Curvesecp256k1 (256-bit) is used for both. This is the same curve that Bitcoin uses to sign its transactions.

ECC-256r1

Like ECC-256k1 but curveprime256v1 (256-bit, also known as secp256r1) is used for both key exchange and certificate.

ECC-521

Like ECC-256k1 but curvesecp521r1 (521-bit) is used for both key exchange and certificate.

 Warnings

We display a warning in 3 cases:

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

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 them. 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 less places to hide a backdoor.

[†] There is strong evidence that a random number generator which 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 which 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 the 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.

Tags

Encryptions

Related Pages

- Should I change the encryption settings of my VPN?