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

- 2022-08-10 - Encryption

We recently incorporated AES-GCM encryption as an encryption option for updated installations and default encryption for new installs and we will continue to add this feature in all applications.

AES-GCM is a more secure cipher than AES-CBC, because AES-CBC, operates by XOR'ing (eXclusive OR) each block with the previous block and cannot be written in parallel. This affects performance due to the complex mathematics involved requiring serial encryption. AES-CBC also is vulnerable to padding oracle attacks, which exploit the tendency of block ciphers to add arbitrary values onto the end of the last block in a sequence in order to meet the specified block size.

The Galois/Counter Mode (GCM) of operation (AES-128-GCM), however, operates quite differently. As the name suggests, GCM combines Galois field multiplication with the counter mode of operation for block ciphers. The counter mode of operation is designed to turn block ciphers into stream ciphers, where each block is encrypted with a pseudorandom value from a “keystream”. This concept achieves this by using successive values of an incrementing “counter” such that every block is encrypted with a unique value that is unlikely to reoccur. The Galois field multiplication component takes this to the next level by conceptualizing each block as its own finite field for the use of encryption on the basis of the AES standard. Additionally, AES-GCM incorporates the handshake authentication into the cipher natively and, as such, it does not require a handshake.

AES-GCM is written in parallel which means throughput is significantly higher than AES-CBC by lowering encryption overheads. Each block with AES-GCM can be encrypted independently. The AES-GCM mode of operation can actually be carried out in parallel both for encryption and decryption. The additional security that this method provides also allows the VPN to use only a 128-bit key, whereas AES-CBC typically requires a 256-bit key to be considered secure.

CBC ciphers were removed in May of 2021. Information based on this decision can be found here.

You are able to use GCM ciphers (such as aes-128-gcm) on any of our OpenVPN ports. Simply change the cipher, and also add the line 'ncp-disable' to your config file.

Although AES-256-GCM is available, it is costly from a computational standpoint at this time and should be used with other practices and methods to ensure

enhanced security and privacy.