What does military-grade encryption in VPN mean?

When researching which VPN provider to choose, you may have come across many services that claim to use military-grade encryption. But what exactly does this mean? What Is Military Grade Encryption and Do You Need It?

The term "military grade" encryption is used a lot these days, to the point where it seems a bit contrived. Is military-grade encryption really a real feature, and if so, are VPN providers really using it for their service?

When VPN providers refer to "military-grade" encryption, they're usually referring to AES, or more specifically, AES-256.

AES, or Advanced Encryption Standard, has been around for more than 20 years and was adopted by the US government in the early 2000s. There are 3 main types of AES encryption: 128-bit, 192-bit, and 256-bit. The higher the number of bits, the longer the encryption key.

AES-128 and AES-192 are used to encrypt certain types of data, but 256-bit definitely dominates in popularity.

Over the past few years, AES-256 has been widely adopted by cybersecurity companies, such as VPN and password manager service providers. The US Army, NASA and many other important agencies use AES-256, simply because it is one of the best encryption standards available today.

AES-256 is a type of symmetric encryption that uses a 256-bit key. This form of encryption is highly resistant to Brute Force attacks and is nearly impossible to crack.

AES-256, like all other AES encryption protocols, has never been cracked. It has been hypothesized that AES-256 encryption will take over a trillion years to crack, and other AES protocols take a similarly large amount of time. SCRAMBOX reported in 2016 that it will take more than 2 trillion years for AES-256 to be cracked, so we can rest assured that it is a long time before this encryption standard is broken (unless some kind of more likely new technologies emerge).

Do all VPN providers use AES-256 encryption?

In short, no. Not all VPN providers on the market use AES-256 encryption. There are different encryption protocols available for VPN services to use with AES-256, but this encryption standard is the most commonly offered (mainly for the reasons discussed above).

It's important to check what encryption protocol your potential VPN service uses before signing up, so you know how your data is protected.

However, many of the most popular VPN services today use AES-256, including:

1. ExpressVPN
2. NordVPN
3. PortonVPN
4. IPVanish
5. VyprVPN
6. PureVPN
7. Hide.me
8. CyberGhost
9. Windscribe
10. TunnelBear
11. Mozilla VPN
12. PrivadoVPN

While many free VPN providers also offer the AES-256 standard, some opt for other standards in exchange for free service. For example, ZoogVPN's free plan uses AES-128 encryption (while its paid plan offers AES-256). This is still a secure protocol, but differs from AES-256 in terms of encryption key length.

It seems like AES-256 is a hugely popular encryption standard among VPN providers, but is this what you really need? Should only services be selected that properly use AES-256 encryption?

Do you need military grade encryption?

If you're a regular Internet user, going online to stream shows, talk to friends, shop, and do the like, you probably don't need military-grade AES-256 encryption. from your VPN provider. After all, there's a reason why it's called military grade. This encryption standard is used to protect highly confidential information held by government agencies.

But this doesn't mean using AES-256 is a bad idea. Your private data still needs to be protected and if you have the option of accessing this high level of encryption, why not use it? As stated earlier, today there are even a lot of free VPN packages that offer AES-256 encryption, so you don't need to spend too much money to protect your data.

If you're still wondering why other security protocols have been abandoned in favor of AES-256, it's because there's a marketing aspect here that benefits VPN companies. Since AES-256 is considered military grade, it is a big plus when VPN providers advertise their services. The phrase "military grade" sounds pretty impressive.

AES-256 gives you the highest level of security

AES-256 is by no means the only secure encryption standard available, but it is still the top choice for cybersecurity companies and government agencies. So, if the VPN provider you choose is offering you this extremely secure form of encryption, there's no reason why you shouldn't enjoy it.