Which encryption/auth settings should I use for ports on your gateways?

Jeremy C. - 2019-05-07 - in Questions

These are the protocol, encryption cipher, auth hash and CA settings that should be used for ports on our gateways in a stock OpenVPN setup. The CRL is not necessary, but we recommend using it to prevent connecting to a discontinued server. The settings here do not apply for any of the PIA apps.

We recommend using ports 1198, 1197, 502 and 501 with AES encryption. We also generally recommend using our OpenVPN configuration files if possible.

You are also able to use GCM ciphers (such as AES-128-GCM) on all of these ports. Simply change the cipher, and also add the line '**ncp-disable**' to your config file.

To download the root CA certificate or CRL, right-click on the name and select "**Save link as**".

Port	Protocol	Encryption	Auth Hash	Root CA	CRL
53	UDP	BF-CBC	SHA1	ca.crt	crl.pem
80	TCP	BF-CBC	SHA1	ca.crt	crl.pem
110	TCP	BF-CBC	SHA1	ca.crt	crl.pem
443	TCP	BF-CBC	SHA1	ca.crt	crl.pem
501	**TCP**	**AES-256-CBC**	**SHA256**	ca.rsa.4096.crt	crl.rsa.4096.pem
502	**TCP**	**AES-128-CBC**	**SHA1**	ca.rsa.2048.crt	crl.rsa.2048.pem
1194	UDP	BF-CBC	SHA1	ca.crt	crl.pem
1197	**UDP**	**AES-256-CBC**	**SHA256**	ca.rsa.4096.crt	crl.rsa.4096.pem
1198	**UDP**	**AES-128-CBC**	**SHA1**	ca.rsa.2048.crt	crl.rsa.2048.pem
8080	UDP	BF-CBC	SHA1	ca.crt	crl.pem

Port	Protocol	Encryption	Auth Hash	Root CA	CRL
9201	UDP	BF-CBC	SHA1	ca.crt	crl.pem

If you encounter warnings while connecting to our gateways, please see this article which explains what may be going on.

Tags

Authoriziation settings

Encryptions