

Technical requirements and installation

[Order now](#) | [Download](#) | [FAQ](#)

Technical requirements

- Operating systems: Debian 9+ (amd64), Ubuntu 18+ (amd64)
- Real ip address on server interface
- Domain name for the server
- **PUQVPNCP v1.2**
- Installed packages **strongswan strongswan-pki libstrongswan-extra-plugins**

Installation

We issue all commands after logging into the SSH terminal window as the root user.

```
apt-get update  
apt-get upgrade  
reboot
```

```
apt-get install strongswan strongswan-pki libstrongswan-extra-plugins -y
```

Checking installed packages

Checking the strongSwan

```
dpkg -s strongswan-starter
```

Output should look similar to this:

```
Package: strongswan-starter
Status: install ok installed
Priority: optional
Section: net
Installed-Size: 610
Maintainer: strongSwan Maintainers <pkg-swan-devel@lists.alioth.debian.org>
Architecture: amd64
Source: strongswan
Version: 5.9.1-1+deb11u3
Depends: adduser, libstrongswan (= 5.9.1-1+deb11u3), lsb-base (>= 3.0-6), debconf (>= 0.5) |
debconf-2.0, libc6 (>= 2.27)
Pre-Depends: init-system-helpers (>= 1.54~)
Recommends: strongswan-charon
Conflicts: openswan
Conffiles:
 /etc/apparmor.d/usr.lib.ipsec.stroke 3ddc2d056db9435ba0d421678308bee3
 /etc/init.d/ipsec a7b2d9de5749ee0bebcd6ac3f9fee732
 /etc/ipsec.conf 01485a8658db82dd781f9229f4151661
 /etc/ipsec.secrets d8e074734da10d2ec7bcd9913263d717
 /etc/strongswan.d/charon/stroke.conf effb1b5bc46a7c849754fada75bae0d2
 /etc/strongswan.d/starter.conf 2ba2784c18e268e34cec179d90e38437
Description: strongSwan daemon starter and configuration file parser
 The strongSwan VPN suite uses the native IPsec stack in the standard
 Linux kernel. It supports both the IKEv1 and IKEv2 protocols.
.
 The starter and the associated "ipsec" script control the charon daemon from
 the command line. It parses ipsec.conf and loads the configurations to the
 daemon.
Homepage: http://www.strongswan.org
```

Checking the IPsec Version

```
ipsec version
```

Output should look similar to this:

Linux strongSwan U5.9.1/K5.10.0-10-amd64
University of Applied Sciences Rapperswil, Switzerland
See 'ipsec --copyright' for copyright information.

Checking the pki

pki

Output should look similar to this:

```
strongSwan 5.9.1 PKI tool
loaded plugins: test-vectors pkcs11 tpm aes rc2 sha2 sha1 md5 mgf1 random x509 revocation
pubkey pkcs1 pkcs7 pkcs8 pkcs12 dnskey sshkey pem openssl gcrypt af-alg gmp curve25519 hmac
drbg curl
usage:
  pki --acert    (-z)  issue an attribute certificate
  pki --dn       (-d)  extract the subject DN of an X.509 certificate
  pki --gen       (-g)  generate a new private key
  pki --issue     (-i)  issue a certificate using a CA certificate and key
  pki --keyid    (-k)  calculate key identifiers of a key/certificate
  pki --pkcs12   (-u)  PKCS#12 functions
  pki --pkcs7    (-7)  PKCS#7 wrap/unwrap functions
  pki --print     (-a)  print a credential in a human readable form
  pki --pub       (-p)  extract the public key from a private key/certificate
  pki --req       (-r)  create a PKCS#10 certificate request
  pki --self      (-s)  create a self signed certificate
  pki --signcrl  (-c)  issue a CRL using a CA certificate and key
  pki --verify    (-v)  verify a certificate using the CA certificate
  pki --help      (-h)  show usage information
```

Revision #6

Created 13 December 2022 08:47:30 by Ruslan

Updated 16 October 2023 08:58:13 by Yuliia Noha