



The Linux IKEv2 VPN Solution!

- Fast tunnel setup (4 instead of 9 IKE messages)
- Mixed authentication (RSA/PSK or EAP)
- Virtual IP assigned from address pool
- Automatic narrowing of traffic selectors

```
#ipsec.secrets for rw carol
carol@strongswan.org : \
    PSK "FpZAZqEN6Ti9sqt4ZP5EWcqX"
```

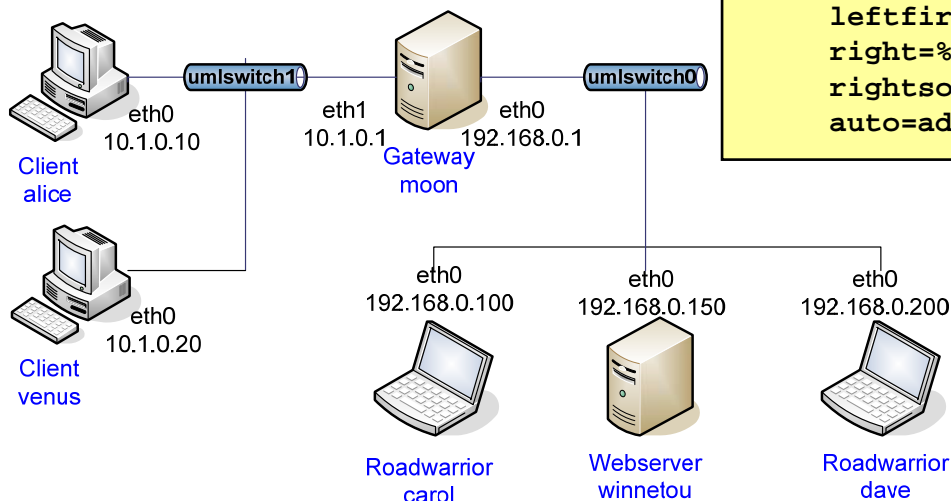
```
#ipsec.conf for roadwarrior carol
conn home
    keyexchange=ikev2
    authby=psk
    left=%defaultroute
    leftsourceip=%config
    leftid=carol@strongswan.org
    leftfirewall=yes
    right=192.168.0.1
    rightid=@moon.strongswan.org
    rightsubnet=10.1.0.0/16
    auto=start
```

```
#ipsec.secrets for gateway moon
: RSA moonKey.pem

carol@strongswan.org : \
    PSK "FpZAZqEN6Ti9sqt4ZP5EWcqX"

dave@strongswan.org : \
    PSK "jVzONCF02ncsgislmIXeqhGN"
```

```
#ipsec.conf for gateway moon
conn rw
    keyexchange=ikev2
    authby=rsasig
    left=%defaultroute
    leftsubnet=10.1.0.0/24
    leftcert=moonCert.pem
    leftid=@moon.strongswan.org
    leftfirewall=yes
    right=%any
    rightsourceip=10.3.0.0/16
    auto=add
```



strongSwan IKEv1 & IKEv2 features

- Runs on Linux 2.6 kernels using the native NETKEY IPsec stack
- Fast connection startup and periodic update using ipsec starter
- Automatic insertion and deletion of IPsec-policy-based firewall rules
- Strong AES, 3DES, Serpent, Twofish, or Blowfish encryption
- NAT-Traversal (RFC 3947) and support of static and dynamic virtual IPs
- Dead Peer Detection (DPD, RFC 3706) takes care of dangling tunnels
- Authentication based on X.509 certificates (RSA) or preshared keys (PSK)
- Generation of a default self-signed certificate during first program startup
- Retrieval and local caching of Certificate Revocation Lists via HTTP or LDAP
- Full support of the Online Certificate Status Protocol (OCSP, RFC 2560).
- CA management (OCSP and CRL URIs, default LDAP server)
- Powerful IPsec policies based on wildcards or intermediate CAs
- Group policies based on X.509 attribute certificates (RFC 3281)
- Optional storage of RSA private keys and certificates on a smartcard (IKEv1)
- Smartcard access via standardized PKCS #11 interface (IKEv1)
- XAUTH authentication in conjunction with IKEv1 Main Mode
- Mixed RSA/EAP authentication (IKEv2)
- Automatic assignment of virtual IP addresses from an address pool (IKEv2)

Our services

- We develop add-ons for strongSwan tailored to your specific needs, e.g. XAUTH, EAP-AKA, and EAP-SIM client or server modules with RADIUS or LDAP access. Major companies all over the globe have chosen strongSwan for their hardware or software security solutions.
- We assist you in defining and setting up your optimized VPN solution. Corporate and campus networks with thousands of VPN clients connecting to a strongSwan gateway are known to work flawlessly without intermission.