The New Linux IKEv2 VPN Solution!

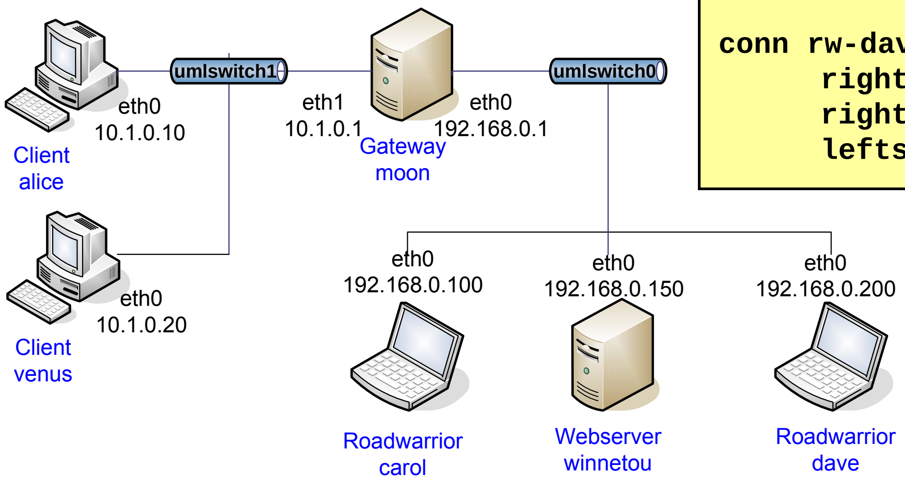
- Fast tunnel setup (4 instead of 9 IKE msgs)
- Automatic narrowing of traffic selectors
- Mixed authentication (RSA/PSK or EAP)
- Virtual IP via configuration payload

```
#ipsec.secrets for rw carol

: RSA carolKey.pem "nH5ZQEWtku0RJ"
```

```
#ipsec.secrets for gw moon

: RSA moonKey.pem
```

```
#ipsec.conf for roadwarrior carol

conn home
     keyexchange=ikev2
     left=%defaultroute
     leftsourceip=%config
     leftcert=carolCert.pem
     leftid=carol@strongswan.org
     leftfirewall=yes
     right=192.168.0.1
     rightid=@moon.strongswan.org
     rightsubnet=10.1.0.0/16
     auto=start
```

```
#ipsec.conf for gateway moon

conn %default
     keyexchange=ikev2
     left=%defaultroute
     leftcert=moonCert.pem
     leftid=@moon.strongswan.org
     leftfirewall=yes
     right=%any
     auto=add

conn rw-carol
     rightid=carol@strongswan.org
     rightsourceip=10.3.0.1
     leftsubnet=10.1.0.0/24
     lefthostaccess=yes

conn rw-dave
      rightid=dave@strongswan.org
      rightsourceip=10.3.0.2
      leftsubnet=10.1.0.20/32
```



www.strongswan.org

Institute for
Internet Technologies
and Applications

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, RCF 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)

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.

EIN INSTITUT DER

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Prof. Dr. Andreas Steffen
Institute for Internet Technologies and Applications
Oberseestrasse 10
CH-8640 Rapperswil
✉ andreas.steffen@hsr.ch ☎ +41 76 340 25 56