FreeSwan – VPN mit großer Sicherheit

- Kurzakte –

Server:

Installation	
• Installation des Pakets freeswan (IPsec Implementation: ermöglicht VPNs) aus Paketgruppe Productivity/Networking/Security nach /usr/sbin/ipsec • Installation und Start auf beiden beteiligten Rechnern	
Konfiguration	
/etc/ipsec.conf	• Hauptkonfigurationsdatei • ein globaler Abschnitt für die allgemeine Funktion • weiter existiert für jede zu erzeugende VPN-Verbindung ein eigener Bereich • Datei ist bei beiden Partnern identisch
/etc/ipsec.secrets	• Ablage der Schlüssel für die Authentifizierung • werden vom Daemon Pluto genutzt • Angabe des öffentlichen Schlüssels im Verbindungsparameter <leftrsasigkey>
ipsec rsasigkey *Bitanzahl*	• Erzeugen eines neuen RSA-Schlüssels • als Bitanzahl sollte man 1024 oder 2048 benutzen
Start als Stand-Alone-Dienst	
/etc/init.d/ipsec rccipe (nur bei SuSE)	• start | stop | restart | status - startet manuell
insserv ipsec (nur SuSE)	• Einfügen des Startskriptes in den Standard-Runlevel • alternativ über den Runlevel-Editor im Yast
Funktionskontrolle	
ifconfig ipsec0	• Betrachten der virtuellen Schnittstelle
route	• Sichten der eingetragenen Routen
Dokumentation	
http://www.freeswan.org ipsec(8), ipsec_pluto(8), ipsec_auto(8), ipsec.secrets(5), ipsec_atoaddr(3), ipsec_atosubnet(3)	

Erstellt von Dr. Jörg Meese www.doc-systems.de

/etc/ipsec.conf

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

# More elaborate and more varied sample configurations can be found
# in FreeS/WAN's doc/examples file, and in the HTML documentation.

# basic configuration (Einleitung des globalen Abschnitts)
config setup
        # THIS SETTING MUST BE CORRECT or almost nothing will work;
        # %defaultroute is okay for most simple cases.
        # interfaces="<virtuelle Schnittstelle>=<Schnittstelle> <...>"  je VPN eine Schnittstelle
        interfaces=%defaultroute
        # Debug-logging controls:  "none" for (almost) none, "all" for lots.
        klipsdebug=none
        plutodebug=none
        # Use auto= parameters in conn descriptions to control startup actions.
        # plutoload="<Verbindung1> <…>"       z.B. plutoload=vpn    (analog bei plutostart)
        plutoload=%search
        plutostart=%search
        # Close down old connection when new one using same ID shows up.
        uniqueids=yes
        # Enable NAT-Traversal
        #nat_traversal=yes
# defaults for subsequent connection descriptions
# (these defaults will soon go away)
conn %default
        keyingtries=0
        disablearrivalcheck=no
        authby=rsasig
        leftrsasigkey=%dnsondemand
        rightrsasigkey=%dnsondemand
# Abschnitt einer VPN-Verbindung mit beliebigem Namen z.B conn vpn
# connection description for opportunistic encryption
# (requires KEY record in your DNS reverse map; see doc/opportunism.howto)
conn me-to-anyone
        left=%defaultroute
        right=%opportunistic
        keylife=1h
        rekey=no
        # for initiator only OE, uncomment and uncomment this
        # after putting your key in your forward map
        #leftid=@myhostname.example.com
        # uncomment this next line to enable it
        #auto=route
# sample VPN connection
conn sample
        # Left security gateway, subnet behind it, next hop toward right.
        left=10.0.0.1
        leftsubnet=172.16.0.0/24
        leftnexthop=10.22.33.44
        # Right security gateway, subnet behind it, next hop toward left.
        right=10.12.12.1
        rightsubnet=192.168.0.0/24
        rightnexthop=10.101.102.103
        # To authorize this connection, but not actually start it, at startup,
        # uncomment this.
        #auto=add
        # Select allowed cipher/hash algorithms
        #ike=aes128-sha-modp1536,aes128-sha-modp1024,aes128-md5-modp1536,aes128-md5-modp1024,3des-
sha-modp1536,3des-sha-modp1024,3des-md5-modp1536,3des-md5-modp1024
        #esp=aes128-sha1,aes128-md5,3des-sha1,3des-md5
```

ipsec.conf zum Beispiels-VPN

```
# globaler Abschnitt
config setup
        # virtuelle Schnittstelle ist ippp0
        interfaces=“ipsec0=ipp0“
        # kein Debugging des Kernel-Codes
        klipsdebug=none
        # kein Debugging des Key-Generators pluto
        plutodebug=none
        # den Keygenerator pluto verwenden
        pluto=yes
        Pluto für die Verbindung namens vpn laden
        plutoload=vpn
        Pluto für die Verbindung namens vpn starten
        Plutostart=yes

# Konfiguration der virtuellen Verbindung namens vpn
conn vpn
        # Einrichtung eines IP-IP-Tunnels
        type=tunnel
        # automatischer Start von pluto
        auto=start
        # Schluesselaustausch per IKE
        keyexchange=ike
        # Authentifizierung mit ESP
        auth=esp
        # Lebensdauer eines keys beträgt 2 Stunden
        keylife=2h
        # Anzahl der Verbindungsversuche unbeschränkt
        keyingtries=0
        # eigene externe IP-Adresse (linkeSeite)
        left=200.0.24.1
        # der nächste Router auf dem Weg zur rechten Seite
        leftnexthop=200.0.24.100
        # lokales Netz der linken Seite
        leftsubnet=192.168.17.0/24
        # offizielle Adresse der rechten Seite
        right=200.0.24.2
        # der nächste Router auf dem Weg zur linken Seite
        rightnexthop=200.0.4.200
        # lokales Netz der rechten Seite
        rightsubnet=192.168.18.0/24
```

/etc/ipsec.secrets zum Beispiels-VPN

```
# Beispiel für einen RSA-Schlüssel für 192.168.17.2
# aka host2.hamburg.de
@host2.hamburg.de: rsa {
...
}

# Beispiel für einen Text als Geheimnis
# host2 aus hamburg tauscht Geheimnis mit host2 aus berlin aus
@host2.hamburg.de @host2.berlin.de:
        PSK „unser Geheimnis“
```