DHCPv4 Configuration of IPsec Tunnel Mode HOWTO

Mario Strasser, mast@gmx.net v0.3.1, 27 August 2002

This HOWTO is part of the DHCP-Relay package and describes how to support the DHCPv4 Configuration of the IPsec Tunnel Mode with the FreeS/WAN IPSec Stack. After a short scenario overview, the installation and configuration of all involved parts (FreeS/WAN, DHCP-Relay and DHCP-Server) is explained. To keep things simple, only the needed changes on the IPSec and DHCP configuration are shown. Thus, it is assumed that FreeS/WAN and a DHCP-Server are already appropriately configured. For a installation from scratch the HOWTO includes a number of references to other documents.

Contents

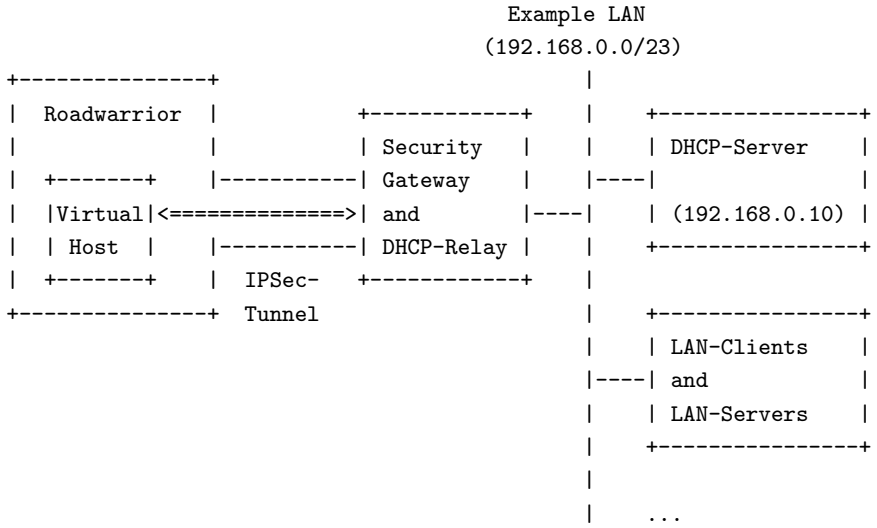
1 Introduction

In many remote access scenarios, a mechanism for making the remote host appear to be present on the local corporate network is quite useful. This may be accomplished by assigning the host a "virtual" address from the corporate network, and then tunneling traffic via IPsec from the host's ISP-assigned address to the corporate security gateway. In IPv4, the Dynamic Host Configuration Protocol (DHCP) provides for such a remote host configuration. The Internet-Draft <draft-ietf-ipsec-dhcp-13.txt> explores the requirements for host configuration in IPsec tunnel mode, and describes how DHCPv4 may be leveraged for configuration. This HOWTO describes the needed modifications of the FreeS/WAN IPSec configuration as well as of further needed parts, ex. the DHCP-Relay and DHCP-Server.

The latest version of this document can be found at <http://www.strongsec.com/freeswan/dhcprelay/>.

1.1 Scenario Overview

The configuration examples in the following sections are based on the following scenario:



- Roadwarrior
  - Gets its *real IP* address - which is used for Internet connectivity - from the DHCP-Server of the ISP. This happens independent from the mechanisms described in this HOWTO.
  - Gets its *virtual IP* (VIP) - which is used to access the *Example LAN* through the IPSec tunnel - from the DHCP-Server of the *Example LAN*.
- Security Gateway and DHCP-Relay
  - FreeS/WAN with applied X.509 patch (>= 0.9.14).
  - DHCP-Relay, forwarding from `ipsec0` to the DHCP-Server over `eth1`.
- DHCP-Server
  - DHCP-Server from the Internet Software Consortium (ISC), issuing leases to the LAN-Clients as well as to the VPN-Clients.
  - The address pool for the LAN-Clients is out of the 192.168.0.0/24 subnet and out of the 192.168.1.0/24 subnet for the VPN-Clients, respectively.

1.2 Copyright

1.3 Disclaimer

Use the information in this document at your own risk. I disavow any potential liability for the contents of this document. Use of the concepts, examples, and/or other content of this document is entirely at your own risk.

All copyrights are owned by their owners, unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

You are strongly recommended to take a backup of your system before major installation and backups at regular intervals.

1.4 Credits

I would like to thank Dr. Andreas Steffen for proofreading and giving me support with the configuration files.

2 FreeS/WAN with X.509 Patch

2.1 Installation

If not already done, download the latest *FreeS/WAN release* <http://www.freeswan.org/> (*>= 1.98b*) and its dedicated *X.509 patch* <http://www.strongsec.com/freeswan/> (*>= 0.9.14*). To apply and install the patch follow the instructions given in the *X.509 Patch Installation and Configuration Guide* <http://www.strongsec.com/freeswan/install.htm>.

2.2 Configuration

In addition to the common transfer tunnels, an additional DHCP tunnel has to be configured, to transport the initial DHCP Traffic between the client and the gateway. This tunnel is only needed to negotiate the DHCP parameters and thus should be setup short-lived. Further, access should be restricted to protocol *udp* and ports *bootps (67)* and *bootpc (68)*, respectively. A sample configuration which should work in most cases is given below (the gateway is supposed to be *on the left*):

```
conn dhcp
        rekey=no
        keylife=30s
        rekeymargin=15s
        leftsubnet=0.0.0.0/0
        leftprotoport=udp/bootps
        rightprotoport=udp/bootpc
```

Some clients do not use this connection to renew their DHCP-lease, but use the normal data tunnel instead. If so, you have to allow the client to send its whole traffic over the gateway (leftsubnet=0.0.0.0/0) as the renew of DHCP-leases has to be done by broadcast under some circumstances! SSH Sentinel 1.3.X is known to be such a client. As this is only a internal feature, the client's configuration must be set to the correct subnet address, not to 0.0.0.0/0!

```
conn roadwarrior
        leftsubnet=192.168.0.0/23
        rightsubnetwithin=192.168.1.0/24

conn roadwarrior-sentinel
        leftsubnet=0.0.0.0/0
        rightsubnetwithin=192.168.1.0/24
```

The whole configuration file, including some general FreeS/WAN options, can be found in 6.1 (Section 6.1).

3 DHCP-Server

3.1 Installation

As DHCPv4 is a well defined standard, almost any DHCP-Server can be used as long as it supports the *DHCP Relay Agent Information Option*. However, I recommend the usage of the DHCP-Server released by the Internet Software Consortium (ISC): <http://www.isc.org/products/DHCP/>. More information can be found in the *DHCP mini-HOWTO* <http://www.tldp.org/HOWTO/mini/DHCP/> or the related `README` file.

3.2 Configuration

If the VPN-clients should not be given a IP out of the common address pool, either the *DHCP Relay Agent Information Option* or the *Gateway Address* can be used, to distinguish between VPN-clients and normal clients. The first contains the name of the ipsec device the request came from, the second is set to the gateway's IP address. The following sample shows how this may work. See 6.2 (Section 6.2) for a complete configuration file.

```
# vpn client class
class "vpn-clients" {
  match if option agent.circuit-id = "ipsec0";
}

subnet ... {
  ...

  # lan clients
  pool {
    deny members of "vpn-clients";
    ...
  }
```

```
  # vpn clients
  pool {
    allow members of "vpn-clients";
    ...
  }

}
```

General information about how to setup a DHCP-Server can be found either in the *DHCP mini-HOWTO* <http://www.tldp.org/HOWTO/mini/DHCP/> or in the man page of the DHCP-Server configuration file (*dhcpd.conf (5)*).

4 DHCP-Relay

4.1 Installation

Download the source archive from <http://www.strongsec.com/freeswan/dhcprelay/> then unpack, configure, compile and install it:

```
bash# tar -xvzf dhcprelay-X.Y.tar.gz
bash# cd dhcprelay-X.Y
bash# ./configure
bash# make
bash# make install
```

In case of troubles, the relay can be compiled in debugging mode by using the `-enable-debug` argument:

```
bash# ./configure --enable-debug
bash# make
bash# make install
```

The DHCP-Relay can be started, stopped, restarted and observed using the `/etc/init.d/dhcprelay` startup script as shown in the following example:

```
bash# /etc/init.d/dhcprelay start
Starting dhcprelay                      done
bash# /etc/init.d/dhcprelay status
Checking for service dhcprelay:         running
bash# /etc/init.d/dhcprelay stop
Shutting down dhcprelay                 done
```

To make the relay starting automatically on start-up, insert the service with the `insserv` or `chkconfig`tool:

```
bash# cd /etc/init.d/
bash# insserv dhcprelay
```

Be aware of the fact that FreeS/WAN *must* already be running when you start the relay and thus if you restart the FreeS/WAN service, the DHCP-Relay *must* be restarted, too!

4.2 Configuration

The DHCP-Server configuration file (`/usr/local/etc/dhcprelay.conf`) contains four items:

- `LOGFILE` sets the path to log-file of the relay.
- `DEVICES` is a comma separated list of ipsec devices the relay should listen on and must contain no spaces!
- `SERVERDEVICE` the device over which the DHCP-Server can be reached.
- `DHCPSERVER` defines the host name or the IP address of the responsible DHCP-Server. If no server is given, the packets are forwarded by broadcast.

It follows an example for one ipsec device and a known DHCP-Server, according to the 1.1 (overview scenario).

```
# DHCP-Relay configuration file

# Logfile
LOGFILE="/var/log/dhcprelay.log"

# IPSec devices (comma separated list including NO spaces)
DEVICES="ipsec0"

# The device over which the DHCP-Server can be reached
SERVERDEVICE="eth1"

# Hostname or IP Address of the DHCP-Server
DHCPSERVER="192.168.0.10"
```

4.3 Running the DHCP-Server and the DHCP-Relay on the same Host

Since release 0.3.1 of the DHCP-Relay this can easily be done by binding both, the relay and the server to the loopback device. Therefore, set

```
SERVERDEVICE="lo"
```

in the DHCP-Relay configuration file and add `lo` to the list of target devices when starting the DHCP-Server. For example:

```
bash# dhcpd lo eth1
```

Further, the DHCP-Server must be able to reply to request comming over the `lo` device, which are not out of the dedicated subnet (127.0.0.0/8). For the ISC DHCP-Server the `subnet` configurations must therefore be embedded into the `shared-network` statement:

```
...
shared-network vpn-networks {
  ...

  subnet 127.0.0.0 netmask 255.0.0.0 {
```

```
  }

  subnet 192.168.0.0 netmask 255.255.255.0 {
    ...
  }

  subnet 192.168.1.0 netmask 255.255.255.0 {
    ...
  }

  ...
}
```

See 6.3 (Section 6.3) for a complete configuration file.

5 Routing Issues

5.1 Using a Proxy ARP

If you have to use exactly the same subnet for the vpn-clients and the lan-clients, the vpn-gw must also work as an arp proxy. Therefore you have to enable arp proxy support in the kernel configuration and activate it with:

```
echo 1 > /proc/sys/net/ipv4/conf/ethX/proxy_arp
```

For further details see the *Linux Advanced Routing and Traffic Control HOWTO* <http://lartc.org/howto/lartc.bridging.html>

5.2 Using a different Subnet for the VPN-Clients

If you have to distinguish between vpn-clients and lan-clients in some cases, split your network (virtually) in two parts:

- use 192.168.0.0/23 for the whole lan
- use 192.168.0.0/24 for the vpn-clients
- use 192.168.1.0/24 for the lan-clients
- if the vpn-gw is not your default gw, add a rule to the default gw which forwards all 192.168.0.0/24 traffic to the vpn-gw.
- use 192.168.0.0/23 for access restrictions where both lan- and vpn-clients are accepted
- use 192.168.0.0/24 for access restrictions where only the vpn-clients are accepted
- use 192.168.1.0/24 for access restrictions where only the lan-clients are accepted

6 Example Configuration Files

6.1 ipsec.conf

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

config setup
        # THIS SETTING MUST BE CORRECT or almost nothing will work;
        # %defaultroute is okay for most simple cases.
        interfaces=%defaultroute
        klipsdebug=none
        plutodebug=none
        plutoload=%search
        plutostart=%search
        uniqueids=yes
        dumpdir=/root

conn %default
        keyingtries=3
        ikelifetime=3h
        keylife=1h
        disablearrivalcheck=no
        # --- RSA authentication using certificates
        authby=rsasig
        # --- left: this server
        left=%defaultroute
        leftid=@gw.company.net
        leftcert=gwCert.der
        leftupdown=/usr/local/lib/ipsec/updown.x509
        # --- right: roadwarrior
        right=%any
        rightrsasigkey=%cert
        # --- preferred encryption algorithms
        esp=aes128,3des
        # --- load connections automatically at startup
        auto=add

conn dhcp
        rekey=no
        keylife=30s
        rekeymargin=15s
        leftsubnet=0.0.0.0/0
        leftprotoport=udp/bootps
        rightprotoport=udp/bootpc

conn roadwarrior
        leftsubnet=192.168.0.0/23
        rightsubnetwithin=192.168.1.0/24

conn roadwarrior-sentinel
        leftsubnet=0.0.0.0/0
```

```
        rightsubnetwithin=192.168.1.0/24
```

6.2 dhcpd.conf

```
# common server options
ddns-update-style none;

# vpn client class
class "vpn-clients" {
  match if option agent.circuit-id = "ipsec0";
}

# example net
subnet 192.168.0.0 netmask 255.255.254.0 {

  option domain-name "example.net";
  option domain-name-servers ns1.example.net, ns2.example.net;
  option routers gw.example.net;
  option netbios-name-servers ads.example.net;

  # lan clients
  pool {
    deny members of "vpn-clients";
    range 192.168.0.50 192.168.0.254;
    default-lease-time 7200;
    max-lease-time 14400;
  }

  # vpn clients
  pool {
    allow members of "vpn-clients";
    range 192.168.1.50 192.168.1.254;
    default-lease-time 3600;
    max-lease-time 7200;
  }

}
```

6.3 dhcpd.conf - DHCP-Server and Relay on the same host

```
# common server options
ddns-update-style none;

# vpn client class
class "vpn-clients" {
  match if option agent.circuit-id = "ipsec0";
}

# example net
shared-network vpn-networks {
```

```
  option domain-name "example.net";
  option domain-name-servers ns1.example.net, ns2.example.net;
  option routers gw.example.net;
  option netbios-name-servers ads.example.net;

  # local
  subnet 127.0.0.0 netmask 255.0.0.0 { }

  # lan clients
  subnet 192.168.0.0 netmask 255.255.255.0 {
    deny members of "vpn-clients";
    range 192.168.0.50 192.168.0.254;
    default-lease-time 7200;
    max-lease-time 14400;
    option subnet-mask 255.255.255.0;
  }

  # vpn clients
  subnet 192.168.1.0 netmask 255.255.255.0 {
    allow members of "vpn-clients";
    range 192.168.1.50 192.168.1.254;
    default-lease-time 3600;
    max-lease-time 7200;
    option subnet-mask 255.255.255.0;
  }

}
```

6.4 dhcprelay.conf

```
# DHCP-Relay configuration file

# Logfile
LOGFILE="/var/log/dhcprelay.log"

# IPSec devices (comma separated list including NO spaces)
DEVICES="ipsec0"

# The device over which the DHCP-Server can be reached
SERVERDEVICE="eth1"

# Hostname or IP Address of the DHCP-Server
DHCPSERVER="192.168.0.10"
```