

Re: OpenSwan – Linux VPN to Linux VPN

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2006-06/msg00283.html>

- *From:* Tauno Voipio <tauno.voipio@xxxxxxxxxxxxx>
 - *Date:* Tue, 13 Jun 2006 15:04:59 GMT
-

walt750@xxxxxxxxxx wrote:

I am trying to use 2 linux servers to bridge or route ip. I have tried using OpenSwan and OpenVPN and cannot get it to work.

The setup is as follows:

```
InternalNet(10.0.0.0/8) > Linux(216.XXX.XXX.1) > Internet <
Linux(70.XXX.XXX.1) < Internal Net (192.168.XXX.XXX)
```

OpenSwan has the problem of not setting up the routing correctly on either sub-network

The routing always comes up work even though the ipsec.conf file seems to be configured correctly.

The routing on the remote comes up as:

```
10.0.0.0/8 gw 70.XXX.XXX.XXX when it should be 10.68.0.0/8 gw
216.XXX.XXX.XX1.
```

I want to be able to use all the resources on the host network. Has anyone gotten OpenSwan to work?

I can get some of it to work changing the routes manually. But I shouldn't have to do that.

3 days at it already I'm getting dizzy.

Thanks in advance.

It seems to me that you are having difficulties with the addresses in a VPN tunnel.

There are 4 IP addresses associated with a VPN tunnel:

– the public address (outside) at the left end,

Re: OpenSwan – Linux VPN to Linux VPN

- the public address (outside) at the right end,
- the private address (inside) at the left end,
- the private address (inside) at the right end.

In your case, the addresses are

- left outside: 216.xxx.xxx.1,
- right outside: 70.xxx.xxx.1,
- left inside: a private address, maybe in another RFC 1918 subnet,
- right inside: a private address, maybe in another RFC 1918 subnet.

You have to think about the IP packet travel in a VPN:

1. A host in the left local subnet sends a packet for the right local subnet (here: 10.x.y.z → 192.168.u.w),
2. The left router knows that the packet is destined via the tunnel, and routes it into the tunnel inside address,
3. The VPN daemon gets the packet via the tunnel pseudo-interface, encrypts it, and creates a packet to the public network,
4. The left router sends the wrapped, encrypted packet to the right router,
5. The right router receives the wrapped packet, decrypts it and feeds it to the network via the tunnel pseudo-interface,
6. The routing in the right router knows how to route the packet to the ultimate destination host in the local network.

The reverse direction is traversed in the same way, but opposite direction.

You need routes set up: