

## Re: Establishing a site-to-site ipsec connection

**Source:** <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2003-05/0002.html>

---

**From:** John SMith (*Jsmith\_at\_hotlink.com*)

**Date:** 04/30/03

Date: Wed, 30 Apr 2003 16:50:09 GMT

Nico,

In my opinion, FreeSwan works best for site to site VPNs – I do not use it for client VPNs so the passwords "shared secrets" are static for each connection. Thier is nothing to hack (unless they take over your tunnel server) since the secret is tied to the VPN end Point. Natting is not that unusuall in a firewalled situation – which assuradly your tunnel server would be doing firewalling even if you have other firewalls behind it. If you want to place it in a DMZ then pay for the IPs to subnet a routable address class and put your tunnel server on the DMZ without NAT in front of it. You would likely want to secure what activity is permitted over the tunnel anyway so it sould have IPTABLE rules.

If your tunnel server is hacked than you have bigger problems anyway. Why steal the secrets and attempt difficult man in the middle attack when they can tcpdump you ipsec interfaces and lunch further attacks from that box or create thier own VPN connections as they choose? Hopefully you secured that box like it had the keys to your Porsche inside Which means you log everything off to a logging server, build a custom kernel, strip it of anything usefull, and implement change management tools and procedures).

–the configurations are usually site specific – but the tunnell server would have to have a routable internet address bound to it. – Why use a NAT hardware solution anyway when you can have a software firewall/NAT, and VPN solution that can adapt to your environment with more flexibility?

FreeSwan is an industrial grade IPSEC solution – All IPSEC implementations are not NAT friendly because NAT does not support protocol 57 (IPSEC) unless they stray from the RFC specs. Some vendors will wrap IPSEC in TCP to get around this for client access – those vendors usually are not for free and that is not standard IPSEC.

Try POPTOP for Mobile users – it is a bit more friendly to NAT because it uses PPTP (but better implementation than MS).

–John

Nico Kadel-Garcia wrote:

> *John SMith wrote:*

>

>> *Natting is OK if it is done on the same box as the Tunnell server not  
>> after it.*

>

>

> *Then that NAT box is running the tunneling services? Forget it! My NAT  
> is a \*hardware\* NAT, shared by my family or workgroup, not a Linux box  
> with which I'm going to tunnel.*

>

>> *Our Natting implementation is rather simple due to our needs. We have  
>> to simply provision connectivity to third parties in more or less for  
>> individual services not whole network connections. So we nat those  
>> services onto the public addresses in our DMZ which are iptabled and  
>> IPseced to our third parties and vice versa if required. We use IKE  
>> for key management. Because it is more widely supported and easily  
>> maintained.*

>>

>> *Regarding the secrets? Yes they are in clear text. We watch very  
>> closely! Tripwired and custom IPTABLE watch daemons to detect changes  
>> in filters and of course IDS sensors everywhere – even on the IPSEC  
>> tunnels.*

>

>

> *Unfortunately, too many users want to use the same password for their  
> user account as for their VPN. And keeping it in clear text on the  
> client is \*begging\* for it to be stolen by anyone with physical access  
> to the box. So once the client is hacked, the attackers now have VPN  
> access to your internal network.*

>

> *Not good.*

>