

Re: freebsd vpn server behind nat dsl router

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-03/msg00009.html>

- *From:* Tom Judge <tom@xxxxxxxxxxxx>
 - *Date:* Thu, 08 Mar 2007 07:59:24 +0000
-

Robert Johannes wrote:

On Wed, 7 Mar 2007, Tom Judge wrote:

<SNIP/>

Looking into adding nat-t to ipsec as we speak.

I would suggest you go with Yvan's suggestion of doing away with gif and adding the nat-t support to ipsec. Alternatively you could use a UDP/TCP based vpn solution such as openvpn (in ports and <http://openvpn.net/>) which will be fully compatible with you nat setup, openvpn will also be tolerant to remote end points changing ip address half while the vpn link is active, comes in hand when used in combination with a dynamic dns service).

As far as openvpn goes, I looked into it in October or Nov. last year, and it seemed not to be very scalable; I have 6 different offices that all need to connect and chat with each other, and it didn't seem like openvpn would allow for this to happen. I didn't investigate it much beyond that when I learned that.

There are no problems with connecting 6 sites together with openvpn, you could either run separate instances of openvpn for each site or using the correct configuration option that specifies all clients can talk to each other via the server. However I would have though that you would want each site to have a link to every other site directly, in which case a openvpn server at each site is you best option, with a number of clients if you use ospf/bgp you will be able to easily maintain your routing table with all these links and be able to survive a link failure as the traffic will get routed via another site rather than directly to its destination.

It would be advisable to use a routing protocol such as ospf even if you decide to use IPSec as is simplifies the maintenance of the routing table, and allows new sites to be added easily and quickly.

Just my 2p

Re: freebsd vpn server behind nat dsl router

Tom

freebsd-security@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"