

Re: Need VPN Firewall security advice

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2004-08/0223.html>

From: P Gentry (*rdgentry1_at_cablelynx.com*)

Date: 08/21/04

Date: 21 Aug 2004 11:18:57 -0700

Anthony Ewell <aewell@gbis.com> wrote in message news:<2onr96Fcgmh2U3@uni-berlin.de>...

- > *Hi All,*
- >
- > *I am about to put a port forward in my IPTABLES*
- > *firewall to allow a remote Windows laptop to*
- > *run a VNC on a desktop inside my firewall.*
- >
- > *The port forward checks to remote end's IP address,*
- > *protocol type, and port before doing the forward.*
- > *the VPN required a password in addition to the key.*
- > *The user is very good about keeping the password*
- > *separate from the laptop, in case it gets stolen.*
- > *(The password is really, really nasty!) To break*
- > *in, a thief would need both the password and the IP*
- > *address of the distant end.*
- >
- > *Question: at this point in my description, do*
- > *you all feel comfortable with what I am planning?*

Probably not -- the VNC connect password is encrypted (barely) but all subsequent traffic passes unencrypted. Will compression be enough to discourage the bad guys? Your call. At least check into using SSH or SSL (stunnel) to provide end-to-end encryption of all traffic. SSL with certificates provides reasonable authentication security as well ;~)

- > *If so, on to my next question. When the rest*
- > *of the remote user figure out how the above works,*
- > *they will want it too. Problem: the rest of them*
- > *are on dynamic addresses. This would mean that*
- > *I would have to open up the firewall to access*
- > *a great deal of additional IP addresses.*

This wouldn't even help if the "inside" IPs are on a private network ,ie., out 10.x, 172.16.x, or 192.168.x friends. Provides a great excuse for why not everyone can have VNC access ;~) Just play dumb re: tunneling schemes!

> *A thief would only need the password. And those*
> *annoying port scanner would be able to make contact*
> *the desktop's VPN (the password guessing would start*
> *in earnest). The idea of doing this give me*
> *hives! :(*
>
> *Does anyone know of a secure way to handle these*
> *dynamic IP remote users?*
>
> *Many thanks,*
> *--Tony*
> *awell@gbis.com*

Agree with WG that you should make someone higher up make that call and accept responsibility. Part of that is for you to formally draw up access/security plans and get a signature -- bet that cuts down on the number of people clamoring for this nifty new feature.

Go slow, get familiar with the product and the risks involved and start researching `_secure_` access now -- plan for the day that someone higher up says, "Just do it!"

my 2 c's,
prg
email above disabled