

Re: Reverse SSH tunnelling

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-09/0002.html>

From: Martin Menhart, B.Sc. – m-sys EDV-Dienstleistungen (m.menhart_at_m-sys.at)

Date: 09/01/04

Date: Wed, 01 Sep 2004 11:45:23 +0200

To: "focus-linux@securityfocus.com" <focus-linux@securityfocus.com>

I've done a lot ssh-tunneling (back an forth, cascaded-ssh-portforwarding ...) myself, because I think that allowing the the needed ports is better than to allow all ports, then restrict it to the ports needed. SSH-Tunnels ar also very easy to implement and straight-forward. You can "just do it", needing only an ssh-client at hand. I agree with Glynn in considering a "real" VPN for persistent server-to server-tunnels, although the reverse ssh-tunnelling has it's charm. Not everything is so easily done with this technique (broadcasting, udp, ...). Furthermore to implement a persistent server-to-server tunnel, implies some locking mechanism, that you have to maintain yourself, so I decided to look into VPNning myself and luckily found openvpn! I think openvpn is a good choice because of it's easy setup. Also it should be reasonably secure, since it relays on the security of ssl. It runs in userspace and utilizes one udp-port per connection. If you want to give this a try:

<http://openvpn.sourceforge.net/>

nice tunneling, martin.

Glynn Clements schrieb:

> *Raistlin Majere wrote:*

>

>

>> *I need some advice .. I have a situation where about fifty servers will*
>>*be located in fifty sites that cannot allow services to be hosted. These*
>>*servers will be in private network space behind firewalls. I can use*
>>*them to 'scp' files out to a common home base server, but sometimes I*
>>*need to access a command line console on these servers. I am thinking of*
>>*having a hourly cron job ssh out to my home base server and leaving that*
>>*tunnel open so that I can access that console, but am looking for the*
>>*specific way of doing this. Security os pf the utmost concern, so I need*
>>*some sort of encrypted tunnel, hence the thought of ssh, but I don't*
>>*know how to do this 'reverse' tunnel... I was also thinking of a 'free*
>>*swan' vpn tunnel ..*

>

>

> *If you have root on the remote systems, I would suggest using a real*

SecurityFocus Linux: Re: Reverse SSH tunnelling

- > *VPN rather than the sort of ad-hoc mechanisms which others have*
- > *suggested. The choice of exactly which VPN is likely to be determined*
- > *by what you can get through the firewall; e.g. if it only allows TCP,*
- > *then you will be limited to a PPP/SLIP-over-SSH/SSL type VPN.*
- >