

Questions on secure remote access to Fedora Core 2

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2006-10/msg00202.html>

- *From:* "C. J. Clegg" <reply.in.group@xxxxxxxxxx>
 - *Date:* Thu, 26 Oct 2006 01:27:01 -0400
-

I am somewhat new to Internet security solutions in general and Linux security in particular, though I have a fair amount of experience with Linux generally.

I am setting up a server with Fedora Core 2 (there are specific reasons why this server needs to run FC2 and not something newer like FC5/6). I want HTTP to be open to everyone. Everything else needs to be open only to certain trusted individuals via certain trusted hosts and needs to be locked up tight to everyone else. Right now, this is all controlled by hosts.allow and hosts.deny (hosts.deny contains ALL: ALL, hosts.allow enables access to ALL from four trusted hosts, and all servers are turned off except httpd, sshd, and ftpd).

The problem is that those certain trusted individuals all have DSL with dynamic IP addressing and so I would have to open up a whole netblock from their ISPs (Comcast) in order to be sure to allow them in.

Also, these people travel from time to time, and they need access from "wherever" while they're traveling. That's not currently available with the current setup.

What is the most secure method I can use to give these individuals access from wherever they are, while minimizing risk from intruders?

I've been reading up on Virtual Private Networks (VPN) over the last couple of days but it seems that they are mostly intended to link up two private LANs, not provide secure access to a publicly-visible server.

I have been told that I can enable only ssh (and not telnet or rlogin or ftp or etc.) and that trusted users can tunnel other protocols (e.g. ftp) under ssh. That sounds interesting but is that really the most secure way?

Anyway I am unclear on just what it is that makes ssh more secure than, say, telnet. If I set up sshd and someone has an ssh client on their computer, and they know a valid userID and password on my machine, then they're in just as easily with ssh as with telnet, near as I can see.

Questions on secure remote access to Fedora Core 2

As you can see I'm pretty short on clues when it comes to this security stuff, so if anyone can (a) suggest the most secure way to allow remote access and (b) point to a website or tutorial or two that I can study that tells all about (a), that would be a very big help and much appreciated.

Thanks.... CJ

.