

Re: stunnel, cgi-proxies, Tera Term, shell accounts

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2002-03/0570.html>

From: laertes-no-spam@cotse.net

Date: 03/27/02

Date: Tue, 26 Mar 2002 18:44:34 -0500 (EST)

From: <laertes-no-spam@cotse.net>

I'm no guru, but you might want to check the features available to members of www.cotse.com. They seem to approximate what you're looking for.

A. Melon wrote:

> *Here's one for the gurus.*

>

> *I've been experimenting with trying to setup stunnel and cgi-proxies to facilitate the setup of my own remote proxy and to be able to access pop3 servers via a SSL link. I have my own W98/NT/Linux systems, but I am trying to get the W98 setup working, however the higher level theory should be the same for all platforms.*

>

> *Scenario*

> -----

> *The problem is that I want to be able to use POP3 to pick up my email from a remote POP3 server without my ISP being able to*

> *snoop on my connection. The problem is that even though email clients such as OE6 do offer POP3S/SMTPS many email suppliers*

> *do not offer POP3S. In addition, it would be a security compromise if you connected to a POP3S server without a SSL tunnel,*

> *because your ISP (upon an FBI order) could track your a/c by simply contacting the POP3S supplier and by using their*

> *respective IP tracking logs, they can determine which a/c was accessed at a particular precise time, and hence they can find*

> *out who you are! A SSL tunnel is the best option of decreasing such an attack. Enter stunnel and similar tunnelling*

> *techniques. stunnel and ssh will enable me to setup a SSL tunnel between my client and a remote server would be ideal. The*

> *problem is however that stunnel works great if the other end of the tunnel connects to the POP3 server directly, however you*

> *need to install a stunnel server at the other end of the pipe, so*

obviously as normally one does not have access to the POP3

> *server this is not possible.*

>

> *So, to overcome this, you need a shell account to an intermediary server where you setup a stunnel server. So the link is*

> *something like this:*

>

> *W32/Linux client running QS/OE/Eudora/Pine <-->SSL tunnel (stunnel client)*

<-->stunnel server (intermediate server) <--data

> *not encrypted in this link-->final server (POP3)*

>

> *The problem is that the vast majority of the unix servers (intermediate) offering FREE shell accounts DO NOT ALLOW traffic*

> *to be routed out of their server from your shell a/c unless you pay for the service. The problem with paying for the*

> *service is that you have to disclose your details and hence this is a security risk (see the APAS posting on digi-cash for*

> *more details on this).*

>

> *Setup Details and Questions*

> -----

> *Q1 – I have setup stunnel under W98 and the 1st question is that when you run stunnel -c (client mode) the program runs and*

> *disappears. I have tried placing an entry in ..RunServices registry key and also created a Task but despite the process*

> *being executed, I do not see it in the Running Tasks list (^-alt-del).*

Am I missing something, shouldn't I see a stunnel

> *process running in the task list or do I need to use a WinTop program to see it?*

>

> *Q2 – What is the use of a Shell Account if you are not allowed to route out of it to another server? OR AM I*

> *misinterpreting this? If I can find a server which will enable me to install stunnel in my Shell Account, do you think it*

> *is feasible to assume that they will let a user have a process such as stunnel run in the background for the duration of*

> *your connection? Does anyone know of a reliable FREE Shell Account service which will enable me to run stunnel?*

>

> *Q3 – Failing stunnel, is there a way to do the above using ssh (openSSH or Tera Term TTSSH?). Does anyone have any*

> *experience in setting up a SSL tunnel to an intermediary server and then collect mail through it or run ftp through it? As*

> *ftp uses 2 channels for communicating stunnel does not support it, how do they implement ftps then? and how can I achieve*

> *this using open source s/w such as OpenSSL. I am aware of the commercial products.*

>

> *Q4 – I also wish to be able to surf the web through my stunnel pipe by running http through it. If this is not possible, I thought of setting up a CGI-Proxy (SSL preferably) to facilitate web browsing, essentially this*

would create my own anonymizer service. Again does anyone have experience with any good CGI-proxies to facilitate anonymous surfing. I am looking into JAP and Delegate proxies. Again, has anyone successfully implemented the latter and can they offer any tips with regards the remote intermediary Shell Account server setup.

>

> *Q5* – *On a general note, TTSSH came with a warning that there is a problem with the IDEA cipher when used with their product. See complete details at <http://www.kb.cert.org/vuls/id/315308>. TTSSH suggest not using the IDEA cipher to overcome this. My question is that when you generate a RSA PGP key using PGP 6.5.8 it specifies that it is IDEA. Could someone clarify for me that if you disable IDEA in TTSSH will you still be able to use your RSA key/certificate? OR am I missing some vital theory?*

>

> *TIA*

- *Next message:* Jason: "Re: Tunnelling via SSL anonymously to connect to remote host(s)"
- *Previous message:* chuck: "Re: SSH Server under Windows"
- *In reply to:* (deleted message) A. Melon: "stunnel, cgi-proxies, Tera Term, shell accounts"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]