Avoid traffic shaping by using ssh on port 443

Asked 16 years, 3 months ago   Modified 9 years, 10 months ago
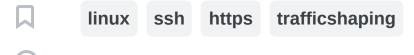
Viewed 6k times

6

I heard that if you use port 443 (the port usually used for https) for ssh, the encrypted packets look the same to your isp.
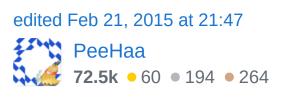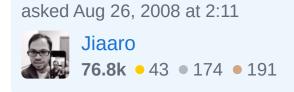
Could this be a way to avoid traffic shaping/throttling?

linux   ssh   https   trafficshaping

Share

Improve this question

Follow

edited Feb 21, 2015 at 21:47

PeeHaa
72.5k ● 60 ● 194 ● 264

asked Aug 26, 2008 at 2:11

Jiaaro
76.8k ● 43 ● 174 ● 191

3 Answers

Sorted by: Highest score (default) ⇕

I'm not sure it's true that any given ssh packet "looks" the same as any given https packet.

However, over their lifetime they don't behave the same way. The session set up and tear down don't look alike (SSH offer a plain text banner during initial connect, for one thing). Also, typically wouldn't an https session be short lived? Connect, get your data, disconnect, whereas ssh would connect and persist for long periods of time? I think perhaps using 443 instead of 22 might get past naive filters, but I don't think it would fool someone specifically looking for active attempts to bypass their filters.

Is throttling ssh a common occurrence? I've experienced people blocking it, but I don't think I've experienced throttling. Heck, I usually use ssh tunnels to bypass other blocks since people don't usually care about it.

Share   Improve this answer

Follow

answered Aug 26, 2008 at 2:21

jj33
7,633 ● 2 ● 40 ● 43

2   HTTP/1.1 sessions can be persistent. – user562374 Jan 31, 2011 at 19:50 ✎

443, when used for HTTPS, relies on SSL (not SSH) for its encryption. SSH looks different than SSL, so it would depend on what your ISP was actually looking for, but it is entirely possible that they could detect the difference. In

my experience, though, you'd be more likely to see some personal firewall software block that sort of behavior since it's nonstandard. Fortunately, it's pretty easy to write an SSL tunnel using a `SecureSocket` of some type.

In general, they can see how much bandwidth you are using, whether or not the traffic is encrypted. They'll still know the endpoints of the connection, how long it's been open, and how many packets have been sent, so if they base their shaping metrics on this sort of data, there's really nothing you can do to prevent them from throttling your connection.

Share Improve this answer

Follow

By filtering ssh input/output through a tunneler (didn't stunnel offer something like that?), you can prepend (and strip) unused HTTP headers with a CONNECT in front of the initial SSH handshake. – user562374 Jan 31, 2011 at 19:52

2

Your ISP is probably more likely to traffic shape port 443 over 22, seeing as 22 requires more real-time responsiveness.

Not really a programming question though, maybe you'll get a more accurate response somewhere else..

Share Improve this answer

Follow