

Forum:[Hack Forums](#)

Thread: [vpn-tor-vpn](#)

mrus3r - May 7, 2023, 12:30 pm

Hi,
I saw that best privacy is using vpn-tor-vpn. But really I would like to understand how.
I'm really new to this.
I normally use VPN and sometimes TOR.

If I use VPN then I connect to TOR and this is clear, but I do not understand how I can open another VPN due to the fact that the TUN interface is busy with original VPN.

Somebody can explain this to me?

Thanks

blipblop - May 7, 2023, 4:07 pm

Do not trust any vpn, there are some that are considered quite good like proton, they promise that there are no loggers on their servers, but if you do criminal things, only use Tor

BigDap - May 7, 2023, 8:03 pm

Don't listen to the above comment: TOR nodes, 40% of them (exit), are owned by the United States Government, this means your un-encrypted data will be seen by them - ALWAYS use VPN -> TOR -> WEB-PROXY when browsing with TOR. Find a VPN company that has RAM only servers and doesn't log data, the web-proxy is just there to hide the fact that you're using TOR, from the website you connect to.

Everyone in the route will know you're on a VPN, and what your real IP is - thus you need a VPN.

DO not listen to people who say "only use tor, its safe" - nothing is safe.

canine - May 7, 2023, 9:39 pm

(May 7, 2023 08:03 PM)BigDap Wrote: [\[CITE\]](#) Don't listen to the above comment: TOR nodes, 40% of them (exit), are owned by the United States Government, this means your un-encrypted data will be seen by them - ALWAYS use VPN -> TOR -> WEB-PROXY when browsing with TOR. Find a VPN company that has RAM only servers and doesn't log data, the web-proxy is just there to hide the fact that you're using TOR, from the website you connect to.

Everyone in the route will know you're on a VPN, and what your real IP is - thus you need a VPN.

DO not listen to people who say "only use tor, its safe" - nothing is safe.

You're stressing a VPN, but now you have to trust that the provider you're using truly doesn't keep any logs of any kind. Like you said--nothing is safe. Tor bridges are also a thing instead of a web proxy if you're trying to hide Tor from your ISP.

Something that might be helpful for OP to read:

<https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN>

BigDap - May 7, 2023, 9:41 pm

(May 7, 2023 09:39 PM)canine Wrote: [\[CITE\]](#) You're stressing a VPN, but now you have to trust that the provider you're using truly doesn't keep any logs of any kind. Like you said--nothing is safe. Tor bridges are also a thing instead of a web proxy if you're trying to hide Tor from your ISP.

Something that might be helpful for OP to read:

<https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN>

I wasn't mentioning bridges because well, everyone knows about that. but still - the exit node has all your traffic decrypted, the same for your home-net. anyone can do DPI at your router or the exit node and see what's going on. TOR is safe, if used right.

canine - May 7, 2023, 9:51 pm

(May 7, 2023 09:41 PM)BigDap Wrote: [\[CITE\]](#) I wasn't mentioning bridges because well, everyone knows about that. but still - the exit node has all your traffic decrypted, the same for your home-net. anyone can do DPI at your router or the exit node and see what's going on. TOR is safe, if used right.

Doesn't the exit node just know the destination you're trying to access? I thought someone would have to compromise all of the nodes involved to get a clear picture of who you are and what you're requesting from a server since they all have their own encryption keys.

BigDap - May 7, 2023, 9:52 pm

(May 7, 2023 09:51 PM)canine Wrote: [\[CITE\]](#) Doesn't the exit node just know the destination you're trying to access? I thought someone would have to compromise all of the nodes involved to get a clear picture of who you are and what you're requesting from a server since they all have their own encryption keys. honestly, not sure. ive always been told the exit node receives information un-encrypted, which is why a VPN is needed in-front of the TOR connection, that and to prevent the ISP from snooping.

mrus3r - May 11, 2023, 3:32 pm

thanks guys for your suggestions!

lullabye - May 13, 2023, 10:30 pm

(May 7, 2023 09:51 PM)canine Wrote: [\[CITE\]](#) Doesn't the exit node just know the destination you're trying to access? I thought someone would have to compromise all of the nodes involved to get a clear picture of who you are and what you're requesting from a server since they all have their own encryption keys.

Just the control of entry and exit node is enough, to fully deanonymize u, and we have to remember https vs http/telnet etc

(May 7, 2023 12:30 PM)mrus3r Wrote: [\[CITE\]](#) Hi,
I saw that best privacy is using vpn-tor-vpn. But really I would like to understand how.
I'm really new to this.
I normally use VPN and sometimes TOR.

If I use VPN then I connect to TOR and this is clear, but I do not understand how I can open another VPN due to the fact that the TUN interface is busy with original VPN.

Somebody can explain this to me?

Thanks

TOR isn't a vpn it's a routing protocol they aren't mutually exclusive

Whether you want to use a vpn or not is a debated topic, in the end like another member said you have to trust the VPN provider not to share or log your data, also it depends on your threat model.

canine - May 14, 2023, 5:49 am

(May 13, 2023 10:30 PM)lullabye Wrote: [\[CITE\]](#) Just the control of entry and exit node is enough, to fully deanonymize u, and we have to remember https vs http/telnet etc

Yeah it's best to try and only use .onion sites when on the tor network in the first place. More onion hosts and non commercial nodes would do help things.

??CU?I??™ - May 14, 2023, 8:09 am

(May 7, 2023 08:03 PM)BigDap Wrote: [\[CITE\]](#) Don't listen to the above comment: TOR nodes, 40% of them (exit), are owned by the United States Government, this means your un-encrypted data will be seen by them - ALWAYS use VPN -> TOR -> WEB-PROXY when browsing with TOR. Find a VPN company that has RAM only servers and doesn't log data, the web-proxy is just there to hide the fact that you're using TOR, from the website you connect to.

Everyone in the route will know you're on a VPN, and what your real IP is - thus you need a VPN.

DO not listen to people who say "only use tor, its safe" - nothing is safe.

I completely agree with this. Most of the Exit nodes are controlled by agencies.

BigDap - May 14, 2023, 1:15 pm

(May 14, 2023 08:09 AM)Security Analyst Wrote: [\[CITE\]](#) I completely agree with this. Most of the Exit nodes are controlled by agencies.

thanks - i had read that and heard that during a defcon series. and then again on cyber gurillia, and then some friends pointed it out, too.

ylove1960 - May 28, 2023, 9:42 am

Which of the best vpn

dontaskmewhy22 - May 28, 2023, 2:13 pm

Opsec isn't just about obscuring network, need to obscure device data too. cross referencing will get you caught much faster than network

Jee098 - May 29, 2023, 2:29 am

I want to anonymise my RAT connection, such that the rat doesn't point to my real Ip. Can I use vpn-Tor Or something similar for this?

Since only a single vpn is not enough and also I need a static Ip.