

Forum:[Hack Forums](#)

Thread: [Extra protection while on a VPN : DNS leak protection](#)

Meow - September 23, 2014, 10:06 am

When using an anonymity or privacy service (VPN), it is extremely important that all traffic originating from your computer is routed through the anonymity network.

If any traffic leaks outside of the secure connection to the network, any adversary monitoring your traffic will be able to log your activity.

Under certain conditions, even when connected to the anonymity network, the operating system will continue to use its default DNS servers instead of the anonymous DNS servers assigned to your computer by the anonymity network. DNS leaks are a major privacy threat since the anonymity network may be providing a false sense of security while private data is leaking.

I see that a few VPN providers have implemented DNS leak protection to their client, however many clients do not.

3 basic steps to fix it :

1. Before connecting to the VPN, set static IP address properties if you are using DHCP
2. After connecting, remove DNS settings for the primary interface
3. After disconnecting, switch back to DHCP if necessary or reapply original static DNS servers

Solution #1 - Automatic

If you are using OpenVPN on Windows then a fully automated solution is available.

Download [dnsfixsetup.exe](#)

After installation, when you connect to a VPN server, a batch file will be run executing the 3 steps above.

Three scripts are generated for each OpenVPN configuration file;

Configfilename_pre.bat - executed when you initiate the connection but before the connection is established - Calls pre.vbs - If any active DHCP adapters exist, switch to static

Configfilename_up.bat - executed when the connection is established - Calls up.vbs - Clear the DNS servers for all active adapter except the TAP32 adapter

Configfilename_down.bat - executed after the connection is disconnected - Calls down.vbs - Reconfigure adapters back to their original configuration

Solution #2 - Manually clearing the DNS

1. Open the command prompt (cmd.exe) as an administrator.
2. Before connecting identify the name of the connected network interface. In the case below it is "Local Area Connection"

Quote:netsh interface show interface

3. Connect to the VPN. Once connected proceed to the next step.
4. Flush the DNS resolver cache

Quote:ipconfig /flushdns

5. Disable the DNS configuration for the Interface identified in Step 1

Quote:netsh interface IPv4 set dnsserver "Local Area Connection" static 0.0.0.0 both

6. Test for DNS leak [HERE](#)
7. After disconnecting, reconfigure the adapter to renew the previous DNS settings

Quote:netsh interface IPv4 set dnsserver "Local Area Connection" dhcp

8. Once again, flush the DNS resolver cache.

Quote:ipconfig /flushdns

And you are done.

Just saw this on another site and wanted to share with you guys, hope you enjoyed. ?

AllBlack - September 23, 2014, 10:23 am

No offense to your method, but why not have an alternative method that also works for Linux and Macs?

Here is a thread I made for Windows users on PIA about DNSCrypt. (Not the garbage version by OpenDNS.)

https://www.privateinternetaccess.com/forum/index.php?p=/discussion/3999/how-to-use-dnscrypt-on-windows-#Item_1

It is entirely free and open sourced. And the servers are linked in too, with a detailed list showing what each supports and does not support. And if it has not changed in a few days, the only server they have that logs is OpenDNS. So do not use OpenDNS.

Note that every time you connect to a new network or VPN, or disconnect from a VPN you will need to close the DNSCrypt program and reopen it and again select all adapters it shows you and then select your server. And if you use a VPN, most of the time it will not support IPv6, so avoid the IPv6 DNS servers.

I hope this helps people. And Linux and Mac instructions are on the DNSCrypt homepage. Good day everyone.