

Forum:[Hack Forums](#)

Thread: [How to prevent DNS leaks and choosing the right VPN](#)

G^aNNicus - December 29, 2014, 7:31 am

How to prevent DNS leaks when using a VPN

Alot of VPN users think they are safe, when using a VPN...but the reality is you have to download some extra protection software and adjust your computer settings, for your VPN to work without any leaks.

I'll explain some steps you can take to prevent DNS leaks.

First of all.

- How do u know when u have DNS leaks

1 Connect to your VPN

2 Visit this site [Leaktest](#)

3 Now take the Extended test

4 Determine if your DNS is leaking, if you are connected to an anonimity/privacy service and ANY of the servers listed below are from your ISP then your DNS is leaking (you should be able to recognize them based on the hostname and location)

Example

Here we have a DNS LEAK

Here we have NO DNS LEAKS

- What to do when you have DNS leaks

There are alot of solutions you can try to fix this, we are going to explain a couple of easy fixes.

1) Change your IP address to a static one

Disabling DHCP so when your router reboots your address will remain the same) as well as changing your preferred DNS servers to that of Googles or OpenDNS. Alot of people still use the DNS servers from their ISP...i would NOT recommend this ofcourse.

These are some of the DNS servers you can use

Google DNS Servers:

Preferred DNS server: 8.8.8.8

Alternate DNS server: 8.8.4.4

Open DNS Servers:

Preferred DNS server: 208.67.222.222

Alternate DNS server: 208.67.220.220

I will show u the instructions for Windows 7, alot of other OS's uses similar procedures.

First head on over to your Network and Sharing Center which is located on your Control Panel. Alternatively just hit Start and type Network and Sharing. Once there select Local Area Connection.

Then you want to go to Properties> Internet Protocol Version 4 (TCP/IPv4)> Properties.
I would also recommend to uncheck the Internet Protocol Version 6 (TCP/IPv6) box.

If you have never touched these settings then by default you will have an IP address automatically set for you by your router via DHCP (Dynamic Host Configuration Protocol) and the DNS servers that you will be using are those belonging to your ISP (Internet Service Provider). These are what we are going to change.

Note

That the choice of DNS servers that you use are completely up to you, although I suggest that you use other DNS servers than your ISP providers. If you are unsure as to what your IP address is currently, just hit the Windows key+R and type cmd into the Run box and hit enter. You will then get the command prompt window open. Now type ipconfig and hit enter. You will find your current IP address, Subnet Mask and Default Gateway (router address)

Now you have the information that you need, so now we can fill in the details.

In the first part of the Properties window select Use the following IP address button. This will now allow you to make the changes. My original IP address was 192.168.1.76 which I changed the last number to 18. The Subnet Mask will automatically be set for you when you click in the first box (in most cases this is 255.255.255.0) The Default Gateway is the address of your router.

If you find that you get an IP conflict error, simply change the last digit of your IP address to a different one, as another computer or device may be currently using that. This is another reason that I prefer to set static IP addresses on all of my devices where possible

For the DNS server details to be changed, select Use the following DNS server addresses button. I will be using the Google DNS servers. And as I have previous times stated, I suggest you DON'T use your ISP DNS servers.

Now hit OK>Close>Close

You can now test to see if you still have any DNS leaks by visiting the DNS Leak Test page [Leaktest](#)

Make sure that you are connected to your VPN and then run the test. You should hopefully not be able to see any information relating to your actual ISP.

If you still have DNS leaks ? Please continue on this journey

2) Executing BATCH file - Automatic Only apply's to OpenVPN

This is a very easy solution to prevent DNS leaks.

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

3) Manually clearing the DNS

Click the Start button.

Enter cmd in the Start menu search text box.

Right-click on Command Prompt and select Run as Administrator.

Type the following command and press Enter: ipconfig /flushdns

If the command was successful, you will see the following message:

Windows IP configuration successfully flushed the DNS Resolver Cache

Test again for DNS leaks!!!

Still no luck ?

4) DNS Crypt

DNSEncrypt is a piece of lightweight software that everyone should use to boost online privacy and security. It works by encrypting all DNS traffic between the user and OpenDNS, preventing any spying, spoofing or man-in-the-middle attacks.

You can download DNS crypt package here [DNSEncrypt](#)

It looks something like this

So, these are some easy ways to prevent DNS leaks, but there are other ways u won't even have to do one of these steps to prevent leaks, and it all starts with picking the RIGHT VPN provider. And that's very simple.

5) Use a VPN client with built in DNS leak protection

This is by far the easiest way, but unfortunately only a few VPN providers supply this option. Those that do include:

- Private Internet Access
- Mullvad
- TorGuard

But ofcourse u can choose your own VPN provider, where you feel comfortable with.
These clients also feature an Internet Kill Switch

Perhaps the simplest way to ensure that no programs access the internet except over VPN, is to use an 'internet kill switch' built into your providers VPN client. Choosing this setting in the client's Settings dialogue will prevent all traffic in and out of the computer in the event of a VPN fail.

Unfortunately this is a feature that we don't see often enough, and of the providers we have reviewed so far, only the following offer this feature:

- Private Internet Access
- Mullvad

Ok, i think its time to rap things up in here, hopefully your DNS leaks are fixed, and u feel comfortable browsing the internet.

Hope u enjoyed this!!!!

Credits:

www.dnsleaktest.com

www.bestvpn.com

www.techfleece.com

Bucked - December 29, 2014, 11:12 am

Really nice tutorial, this will help a lot of people who dont know how to change their dns

G^aNNicus - December 29, 2014, 11:22 am

Thank you i hope it will be useful for alot of people

ubnt123 - December 30, 2014, 7:13 am

So i tested my vpn and its showed 1 host name belong to my ISP,i did the 1st step and changed to static IP ,scanned it again and its clear ,ithat's enough and mean my ISP have no chance to do any MITM ?

Very helpful information this thread must keep alive,Thanks.

Richard "The Lionheart" - December 30, 2014, 7:51 am

Really nice tutorial m8. Well done.

G^aNNicus - December 30, 2014, 3:32 pm

(Dec 30, 2014 08:13 AM)ubnt123 Wrote: [\[CITE\]](#) So i tested my vpn and its showed 1 host name belong to my ISP,i did the 1st step and changed to static IP ,scanned it again and its clear ,ithat's enough and mean my ISP have no chance to do any MITM ?

Very helpful information this thread must keep alive,Thanks.If there isn't ANY information about your country or ISP, then you have NO leaks

I don't know which VPN u have, but im positive ur good. Don't worry bout MITM

(Dec 30, 2014 08:51 AM)Richard "The Lionheart Wrote: [\[CITE\]](#) Really nice tutorial m8. Well done. Thanks

jakedav - December 30, 2014, 3:53 pm

So handy! Great tut dude!!

Commenting as bookmark!!

G^aNNicus - December 31, 2014, 3:19 am

Thank you for the kind words jakedav

Profatssor - January 5, 2015, 2:19 am

(Dec 29, 2014 08:31 AM)????? 3??l??? ?????? Wrote: [\[CITE\]](#) Alot of VPN users think they are safe, when using a VPN...but the reality is you have to download some extra protection software and adjust your computer settings, for your VPN to work without any leaks.

I'll explain some steps you can take to prevent DNS leaks.

Vouch for this. I had a dns leak with the VPN I was using and was able to fix it.

The VPN I am using uses openvpn and the website mentioned in the post had a download (cannot post link due to <50 posts) that automatically solved the issue for openvpn.

Thanks for making me aware of this and I really do suggest that people check for dns leaks!

G^aNNicus - January 5, 2015, 4:57 am

Thanks for the vouch glad you found it useful.

EvilMo - January 6, 2015, 3:18 pm

Thanks! This is exactly the information i needed. Thanks m8!

G^aNNicus - January 7, 2015, 10:35 am

No problem, glad i could assist you.

Pr0m3th3us - January 10, 2015, 1:31 pm

thank you very much for this, for some reason I can't get a connection to the Internet after I change my IP, so I figured I had to disable DHCP on my router but when I did that it locked up and I had to actually hold the reset button for once....lame. So any ideas?

Edit: I do believe i have figured it out, im still using my router as a DHCP server for the rest of my devices connected to it, i just set my PC's IP out of its range and shortened the range of the DHCP server.

G^aNNicus - January 11, 2015, 2:15 pm

Okay, so everything is resolved Lord Foolber ?

Pow3r - January 12, 2015, 7:03 am

This is sticky worthy. I hope it does get stickied.

G^aNNicus - January 12, 2015, 7:07 am

Thank you, glad you liked it.

I hope it gets stickied someday.

G^aNNicus - January 14, 2016, 11:00 am

Yup thats right i'm bumping my own thread. I believe it can help alot of people how to be safe and choosing the right VPN.

kpr1337 - January 15, 2016, 10:01 am

ty for this tutorial is very helpful for me

G^aNNicus - January 15, 2016, 10:17 am

No problem, glad it helped you.

saharmagic - August 10, 2016, 8:52 am

Thankyou for sharing this news ,it could provide us more privacy.

ProfessorGeng - August 16, 2024, 10:34 pm

thank you for the tutorial , it helps a lot

6eRePeY7 - August 22, 2024, 3:41 pm

Thank you for your help. You make me feel comfortable.

Hosting Farmer - *August 25, 2024, 9:23 am*

Very interesting, thank you.

shang0 - *January 27, 2025, 8:42 pm*

very helpful did not know this thank god ii have mullvad