reddit

r/mullvadvpn · 4y ago
u/DN9TP3

Join

[Guide] NextDNS + Mullvad (WireGuard) + DOH3 on iOS / iPadOS / macOS

Solved

Introduction

How to make NextDNS and Mullvad (WireGuard) work together, perfectly, is a question that has been asked hundreds of times and across many different forums. Today, the magic to make that happen comes together—with the added bonus of support for DoH3.

This guide has a difficulty level of **Medium**; and is bifurcated into two major sections, each with several steps. If you are unfamiliar with any of the steps below, please ask for help in the comments and someone will assist.

NextDNS steps:

1. Visit: https://apple.nextdns.io
   1. Enter your "*Configuration ID*."
   2. Enter your "*Device Name*."
   3. Enter your "*Device Model*."
   4. **Do not** "*Trust NextDNS Root CA*." [Unless you know what you are doing and are completely crazy].
   5. **Do not** enable "*Bootstrap IPs*." [Unless you know what you are doing and enjoy slow DNS resolution].
   6. **Do not** enable "*Sign Configuration Profile*." [As we will be editing it in a moment].
2. "*Download*" your shiny new *Configuration Profile*, which will be in your `Downloads` folder, as a file ending with `.mobileconfig` .
3. Inside that file, there will be one occurrence of the string `apple.dns.nextdns.io` . Replace that string with `doh3.dns.nextdns.io` .
   1. If one is comfortable with macOS's *Terminal* app, one option for effecting the above string replacement would be to execute: `sed -i.bak 's#apple.dns.nextdns.io#doh3.dns.nextdns.io#' ~/Downloads/NextDNS\ \([[:alnum:]]*\).mobileconfig` .
4. Install the edited *Configuration Profile*.

> The above steps will make it such that your iOS, iPadOS or macOS device will use NextDNS's *Device Identification* for *Analytics* and *Logs*; in addition to Apple's system-wide *Encrypted DNS*. [This works for both iOS/iPadOS 15/16 & macOS 12/13].

Mullvad (WireGuard) steps:

> **Note**: If you are using the *Mullvad* macOS app, instead of the *WireGuard* iOS/iPadOS/macOS app, you may replace steps 1-8 below by visiting `Settings > Advanced > Use custom DNS server` and specifying `0.0.0.0` and `::`.

1. Visit: https://mullvad.net/en/account/#/wireguard-config/
2. Generate and download a *WireGuard Configuration File*.
3. Edit the *WireGuard Configuration File*.
4. For "*DNS servers*", specify: `0.0.0.0/32, ::/128`
5. For "*Allowed IPs*", specify: `0.0.0.1/32, 0.0.0.2/31, 0.0.0.4/30, 0.0.0.8/29, 0.0.0.16/28, 0.0.0.32/27, 0.0.0.64/26, 0.0.0.128/25, 0.0.1.0/24, 0.0.2.0/23, 0.0.4.0/22, 0.0.8.0/21, 0.0.16.0/20, 0.0.32.0/19, 0.0.64.0/18, 0.0.128.0/17, 0.1.0.0/16, 0.2.0.0/15, 0.4.0.0/14, 0.8.0.0/13, 0.16.0.0/12, 0.32.0.0/11, 0.64.0.0/10, 0.128.0.0/9, 1.0.0.0/8, 2.0.0.0/7, 4.0.0.0/6, 8.0.0.0/5, 16.0.0.0/4, 32.0.0.0/3, 64.0.0.0/2, 128.0.0.0/1, ::1/128, ::2/127, ::4/126, ::8/125, ::10/124, ::20/123, ::40/122, ::80/121, ::100/120, ::200/119, ::400/118, ::800/117, ::1000/116, ::2000/115, ::4000/114, ::8000/113, ::1:0/112, ::2:0/111, ::4:0/110, ::8:0/109, ::10:0/108, ::20:0/107, ::40:0/106, ::80:0/105, ::100:0/104, ::200:0/103, ::400:0/102, ::800:0/101, ::1000:0/100, ::2000:0/99, ::4000:0/98, ::8000:0/97, ::1:0:0/96, ::2:0:0/95, ::4:0:0/94, ::8:0:0/93, ::10:0:0/92, ::20:0:0/91, ::40:0:0/90, ::80:0:0/89, ::100:0:0/88, ::200:0:0/87, ::400:0:0/86, ::800:0:0/85, ::1000:0:0/84, ::2000:0:0/83, ::4000:0:0/82, ::8000:0:0/81, ::1:0:0:0/80, ::2:0:0:0/79, ::4:0:0:0/78, ::8:0:0:0/77, ::10:0:0:0/76, ::20:0:0:0/75, ::40:0:0:0/74, ::80:0:0:0/73, ::100:0:0:0/72, ::200:0:0:0/71, ::400:0:0:0/70, ::800:0:0:0/69, ::1000:0:0:0/68, ::2000:0:0:0/67, ::4000:0:0:0/66, ::8000:0:0:0/65, 0:0:0:1::/64, 0:0:0:2::/63, 0:0:0:4::/62, 0:0:0:8::/61, 0:0:0:10::/60, 0:0:0:20::/59, 0:0:0:40::/58, 0:0:0:80::/57, 0:0:0:100::/56, 0:0:0:200::/55, 0:0:0:400::/54, 0:0:0:800::/53, 0:0:0:1000::/52, 0:0:0:2000::/51, 0:0:0:4000::/50, 0:0:0:8000::/49, 0:0:1::/48, 0:0:2::/47, 0:0:4::/46, 0:0:8::/45, 0:0:10::/44, 0:0:20::/43, 0:0:40::/42, 0:0:80::/41, 0:0:100::/40, 0:0:200::/39, 0:0:400::/38, 0:0:800::/37, 0:0:1000::/36, 0:0:2000::/35, 0:0:4000::/34, 0:0:8000::/33, 0:1::/32, 0:2::/31, 0:4::/30, 0:8::/29, 0:10::/28, 0:20::/27, 0:40::/26, 0:80::/25, 0:100::/24, 0:200::/23, 0:400::/22, 0:800::/21, 0:1000::/20, 0:2000::/19, 0:4000::/18, 0:8000::/17, 1::/16, 2::/15, 4::/14, 8::/13, 10::/12, 20::/11, 40::/10, 80::/9, 100::/8, 200::/7, 400::/6, 800::/5, 1000::/4, 2000::/3, 4000::/2, 8000::/1`
   1. **Note**: The above CIDR ranges were derived by visiting the WireGuard AllowedIPs Calculator and—on that page—setting *Allowed IPs* to `0.0.0.0/0, ::/0` and setting *Disallowed IPs* to `0.0.0.0/32, ::/128` .
6. In the *WireGuard app*, create a new *WireGuard tunnel* from your *WireGuard Configuration File*.
   1. **Note**: Due to a bug in the macOS *WireGuard* app's UI, you will not be able to "*Add Empty Tunnel*", nor will you be able to "*Edit*" an existing tunnel; You must instead have edited your *WireGuard Configuration File* first, and then "*Import Tunnel(s) from File*." [This bug is not present in the *WireGuard* app on iOS/iPadOS].
7. Enable *On-Demand* [Wi-Fi or cellular; Any SSID] and activate your new *WireGuard tunnel*.
8. Restart your device.
9. Visit: https://test.nextdns.io
   1. `status` should be: `ok`
   2. `protocol` should be: `DOH3` or `DOH`
      1. **IMPORTANT NOTE**: NextDNS features *foundational* support for DOH3. Currently, DOH is the default; DOH3 *is not*. When explicitly using the `doh3.dns.nextdns.io` endpoint, DOH3 will be leveraged *when available*; otherwise, DOH will be leveraged. This means that—at this time—when visiting `test.nextdns.io` , you should expect to see either `DOH3` *or* `DOH` ; instead of only `DOH3` . Similarly, when visiting the `my.nextdns.io` *Logs* tab and hovering over a row's lock symbol, you should expect to see either `DNS-over-HTTP/3` *or* `DNS-over-HTTPS` ; instead of only `DNS-over-HTTP/3` . [1][2]

> The above steps will make it such that your new *WireGuard tunnel* uses the NextDNS *Configuration Profile* that you installed. It achieves this by explicitly setting the DNS servers to `0.0.0.0/32` [which is not the same as 127.0.0.1/32] for IPv4, and to `::/128` for IPv6. Then, we allow the entire IPv4 and IPv6 address spaces to transit the tunnel, except for the two aforementioned device-local IPs.

Congrats on your leak-free, kill-switched, system-wide, NextDNS DoH3, Mullvad (WireGuard) VPN!


```
{
        "status": "ok",
        "protocol": "DOH3",
        "profile": "[redacted]",
        "client": "[redacted]",
        "srcIP": "[redacted]",
        "destIP": "[redacted]",
        "anycast": false,
        "server": "vultr-atl-1",
        "clientName": "unknown-doh3",
        "deviceName": [redacted]
        "deviceID": "[redacted]"
}
```


Output from https://test.nextdns.io

STATUS
Active (On-Demand)

INTERFACE
Name [redacted]
Public key [redacted]
Addresses [redacted]
Listen port [redacted]
DNS servers 0.0.0.0/32, ::/128

PEER
Public key [redacted]
Endpoint [redacted]
Allowed IPs 0.0.0.1/32, 0.0.0.2/31, 0.0.0.4/30, 0.0.0.8/29, 0.0
Data received 544.02 MiB
Data sent 35.94 MiB
Latest handshake 02:13 minutes ago

ON-DEMAND ACTIVATION
On-demand Wi-Fi or cellular
SSIDs Any SSID

Active iOS WireGuard tunnel

```
dnscheck.tools - test your dns resolvers

results    more

Hello! You're accessing the Internet from:

  QuadraNet
    [redacted]

  QuadraNet Enterprises LLC
    [redacted]

Your dns resolvers are:

  Anexia
    [redacted]
      ptr: dns.nextdns.io
    [redacted]
      ptr: dns.nextdns.io

Great! Your dns responses are authenticated:

  DNSSEC using ECDSA P-256 (PASS)
    Correct signature: connected
    Invalid signature: not connected
    Expired signature: not connected
    Missing signature: not connected

  DNSSEC using ECDSA P-384 (PASS)
    Correct signature: connected
    Invalid signature: not connected
    Expired signature: not connected
    Missing signature: not connected

  DNSSEC using Ed25519 (PASS)
    Correct signature: connected
    Invalid signature: not connected
    Expired signature: not connected
    Missing signature: not connected
```

Output from https://dnscheck.tools

Manage WireGuard Tunnels

[redacted]

Interface: [redacted]
Status: Active, On-Demand Enabled
Public key: [redacted]
Addresses: [redacted]
Listen port: [redacted]
DNS servers: 0.0.0.0/32, ::/128
Disable On-Demand and Deactivate

Peer: [redacted]
Endpoint: [redacted]
Allowed IPs: 0.0.0.1/32, 0.0.0.2/31, 0.0.0.4/30, 0.0.0.8/29, 0.0.0.16/28,...
Data received: 3.42 MiB
Data sent: 782.80 KiB
Latest handshake: 1 minute, 57 seconds ago

On-Demand: Wi-Fi or ethernet
SSIDs: Any SSID

Edit

Active macOS WireGuard tunnel

75 · 42 · 214

ninehat · 4y ago
How to install mobileconfig file from filesapp?

3 more replies

NmAmDa · 4y ago
Hi, Thank for this guide. I tried following it but using adguard home mobileconfig instead of nextdns. It works with wireguard if I make DNS values in config values take '0.0.0.0/32, ::/128' but with mullvad app, letting custom dns '0.0.0.0' and '::' does not connect to the dns server. Do you have an idea what could be the problem?

DN9TP3 OP · 4y ago
Hi, thank you for the question. Can you try it with AdGuard Home and the WireGuard app, and let me know if it works like that? Later today, I'll test with AdGuard Home and the Mullvad app, and I'll see what's going on.

4 more replies

atat_sa_putut · 4y ago · Edited 4y ago
Hey! Thanks for the guide, helped me to get Proton VPN with NextDNS on iOS. Basically I'm doing exactly what you said, but with the wireguard config file generate from Proton.

I do have a problem though. With NextDNS I can see that some queries come from my real IP and ISP. So they don't make it through the VPN tunnel. DNS leak test results from here are fine, but my IP leaks in the NextDNS logs.

Any ideas why?

Edit: it's my ipv6 address that gets revealed, and only through cell data. Ipv4 is that of my VPN, but ipv6 seems to be that of the cell tower I'm connected to.

DN9TP3 OP · 4y ago
Hiya!

In order to avoid *potential* result-caching issues, I would only consider results to be reliable if a leak is shown from a *brand new*, *single-use*, *private* browser tab. Also, I would look for confluence between dnsleaktest.com and other similar sites: ifconfig.io, ifconfig.me, www.whatismyip.com, dnscheck.tools, mullvad.net/en/check, browserleaks.com/ip, test-ipv6.com and ipv6-test.com.

Have you tested to see if you can reproduce the behavior that you observed with the Mullvad iOS app, as opposed to the iOS WireGuard app?

I would also double check your WireGuard configuration, ensuring, for example, that `Addresses` , `DNS servers` and `Allowed IPs` have the expected IPv6 values. And I would also double check your NextDNS Configuration File's configuration against both your NextDNS-provided values and developer.apple.com/documentation/devicemanagement/dnssettings/dnssettings.

In order to streamline, some folks make the decision to disable IPv6 entirely. It's trivial to disable IPv6 on a Mac and many routers; it's slightly more involved to disable IPv6 on iOS: sunknudsen.com/privacy-guides/how-to-disable-ipv6-on-ios-cellular-only-and-macos.

[redacted]

Unbreakable2k8 · 4y ago
Seems to work randomly, when I switch from wifi to mobile or on multiple refreshes it's either DOH or DOH3. Don't know what to make of this. This is without the VPN.

I made a custom profile with DOT for my iPhone and that is more stable.

1 more reply

View more comments

People also ask about

- WireGuard DNS settings for iOS
- WireGuard split tunneling with TP-Link Omada
- WireGuard throughput for TP-Link routers
- Best practices for maximizing VPN privacy
- How to troubleshoot common Mullvad VPN issues

r/ControlD · 1y ago
I tested the top free DNS ad blocking services with the default configuration...
21 upvotes · 27 comments

r/xprivo · 1mo ago
Mullvad's public DNS is shutting down. Here are privacy-friendly alternatives...
206 upvotes · 48 comments

r/nextdns · 21d ago
New security option
54 upvotes · 13 comments

r/mullvadvpn · 4y ago
Is there any reason I shouldn't be using the Wireguard app on iOS/MacOS vs the Mullvad app?
2 upvotes · 11 comments

r/degoogle · 1mo ago
Mullvad Is Shutting Down Its Public Encrypted DNS Servers and Sponsorin...
1.6K upvotes · 176 comments

r/Piracy · 1mo ago
Mullvad VPN axes its public encrypted DNS service to sponsor Quad9 instead
682 upvotes · 104 comments

r/nextdns · 1mo ago
🚨 New NextDNS Early Access security features are live
273 upvotes · 41 comments

r/mullvadvpn · 9mo ago
Comparing Mullvad and NordVPN's ad-blocking capabilities
10 upvotes · 11 comments

r/mullvadvpn · 10mo ago
How effective is Mullvads adblock DNS?
11 upvotes · 12 comments

r/pihole · 9mo ago
Why isn't there much talk about Mullvad's DNS servers?
38 upvotes · 15 comments

r/PrivacyGuides · 4y ago
Mullvad, Quad9 or NextDNS as DNS server?
33 upvotes · 22 comments

r/mullvadvpn · 3y ago
Mullvad DNS vs NextDNS
3 upvotes · 4 comments

r/nextdns · 3y ago
NextDNS vs Mullvad DNS
3 upvotes · 19 comments

r/dns · 5mo ago
Mullvad dns
77 upvotes · 21 comments

r/DataHoarder · 1mo ago
Mullvad VPN axes its public encrypted DNS service to sponsor Quad9 instead
706 upvotes · 48 comments

r/mullvadvpn · 4mo ago
Mullvad silently rolled back their mitigation for static IPs, defaulting to 3...
81 upvotes · 39 comments

r/mullvadvpn · 19d ago
Websites keep blocking me even with a VPN? I bought Mullvad VPN subscription still doesnt work.
21 upvotes · 41 comments

r/WireGuard · 5y ago
Benefits between using official MullvAd vpn and wire guard customer setup?
6 upvotes · 2 comments

r/mullvadvpn · 10mo ago
How do the 4 Mullvad VPN WireGuard Obfuscation Techniques Hide my VPN Use From an ISP if the ISP...
22 upvotes · 19 comments

r/mullvadvpn · 3mo ago
After being a mullvad user for a bit, here's what I have to say
26 upvotes · 27 comments

r/dns · 10d ago
Why did Mullvad have to shut down? It was the best privacy and ad blocking DNS out there. 😭😭😭
41 upvotes · 40 comments

r/mullvadvpn · 5mo ago
Issues with Mullvad DNS lately? Sites barely loading
39 upvotes · 43 comments

r/mullvadvpn · 4mo ago
Switching to mullvad soon
46 upvotes · 41 comments

r/mullvadvpn · 2mo ago
It's becoming increasingly difficult to continue using Mullvad
189 upvotes · 96 comments

r/nextdns · 1mo ago
New hidden security features found in NextDNS strings and API
141 upvotes · 17 comments

VIEW POST IN
日本語
简体中文
See more

TOP POSTS
Reddit
reReddit: Top posts of September 5, 2022
Reddit
reReddit: Top posts of September 2022
Reddit
reReddit: Top posts of 2022