

DNS Privacy Test Servers

- [Public resolvers](#)
- [Experimental DNS Privacy Recursive Servers](#)
 - [DoH servers](#)
 - [DoT servers](#)
 - [Stubby](#)
 - [Servers run by the Stubby developers](#)
 - [Other servers with a 'no logging' policy](#)
 - [Servers with minimal logging/limitations](#)

Public resolvers



Public Resolvers: Several large organisations have announce DNS Privacy Servers - see [DNS Privacy Public Resolvers](#)

- [Quad9 \(9.9.9.9\)](#) and [Cloudflare \(1.1.1.1\)](#) offer DNS-over-TLS on port 853
- DOH servers are also currently listed on that page

Experimental DNS Privacy Recursive Servers

[Live Monitoring Dashboard](#)

[Live Traffic Graphs](#)

[Map of server locations](#)

DoH servers

These are currently listed on the [DNS Privacy Public Resolvers](#) page and also the list maintained [on the curl wiki](#). For any servers below with the note 'also does DoH' check these pages or the website of the service for the DoH endpoint.

DoT servers

The following servers are experimental DNS-over-TLS servers.



Note that they are experimental offerings (mainly by individuals/small organisations) with **no guarantees** on the lifetime of the service, service level provided. The level of logging may also vary (see the individual websites where available) - the information here about logging has not been verified. Also note that the single SPKI pins published here for many of these servers are subject to change (e.g on Certificate renewal) and should be used with care!!

Stubby

A YAML configuration file for Stubby containing a the details of these servers is provided with Stubby and [can be found here](#). This file enables only the subset of servers operated by the stubby/getdns developers by default, users can choose to enable any of the other servers by uncommenting the relevant section (occasionally the file lags this page).

Servers run by the Stubby developers

Hosted by	IP addresses	TLS Ports	Hostname for TLS authentication	Base 64 encoded form of SPKI pin (s) for TLS authentication (RFC7858)	TLSA record published	Logging	Software	Notes
1) The following are currently enabled in the default Stubby config file because they are run by the stubby/getdns developers and have no known issues.								
Surfnet	145.100.185.15 2001:610:1:40ba:145:100:185:15	853 443	dnsovertls. sinodun.com	62lKu9HsDVbyiPenApnc4sfmSYTHOVfFgL3pyB+cBL4=	Y	Traffic volume only	HAProxy + BIND 9.12	
Surfnet	145.100.185.16 2001:610:1:40ba:145:100:185:16	853 443	dnsovertls1. sinodun.com	cE2ecALeE5B+urJhDrJIVFmf38cJLAvqekONvjvpqUA=	Y	Traffic volume only	Nginx + BIND 9.12	
getdnsapi.net	185.49.141.37 2a04:b900:0:100::37	853	getdnsapi.net	foxZRnlh9gZpWnl+zEiKa0EJ2rdCGroMWm02gaxSc9Q=	Y	Traffic volume only	Unbound	

Other servers with a 'no logging' policy

Hosted by	IP addresses	TLS Ports	Host name for TLS authentication	Base 64 encoded form of SPKI pin(s) for TLS authentication (RFC7858)	TLS A record published	Logging	Software	Notes
Uncensored DNS	89.233.43.71 2a01:3a0:53:53::0	853	unicast.censurfridns.dk	wikE3jYAA6jQmXYTr/rbHeEPmC78dQwZbQp6WdrseEs=	Y	Traffic volume only		See https://blog.uncensoreddns.org/
Fondation RESTENA (NREN for Luxemburg)	158.64.1.29 2001:a18:1::29	853	kaitain.restena.lu	7ftvkA+UeN/ktVkovd/rPZ6mbkhV17/8HnFJlLa4=		Traffic volume only	Unbound	Configured with qname-minimisation, use-caps-for-id, aggressive-nsec, prefetch, harden-below-nxdomain and the newest auth-zone for local root zone caching.
Surfnet	145.100.185.18 2001:610:1:40ba:145:100:185:18	853	dnsvertls3.sinodun.com	5SpFz7JEPzF71hditH1v2dBhSErPUMcLPJx1uk2svT8=	Y	Traffic volume only	HAPROXY + BIND 9.12	Supports TLS 1.3 and TLS 1.2. Our initial stability problems are solved... see here for details .
Surfnet	145.100.185.17 2001:610:1:40ba:145:100:185:17	853	dnsvertls2.sinodun.com	NAXBESvpjZMnPWQcra2KFkHV/pDElJRKA3hLWogSg=	Y	Traffic volume only	Knot Resolver	
dkg	199.58.81.218 2001:470:1c:76d::53	85343	dns.cmrng.net	3IOHSS48KOc/zlkKGtl46a9TY9PPKDVGH3W2ZS4JZ0=5zFN3smRPuHlIM/8L+hANt99LW26T97RFHqHv90awjo=		None	Knot Resolver	See https://dns.cmrng.net/ Note that on port 443 this server can serve both HTTP 1.1 traffic (to securely access the nameserver credentials) on TLS connections and DNS-over-TLS on separate TLS connections due to some nifty, experimental demultiplexing of traffic, described here . Has some issues with DNSSEC responses - this is under investigation.
dns.larsdebruin.net (Previously dns1.darkmoon.is)	51.15.70.167	853	UPDATED on 30 Jan 2018 dns.larsdebruin.net	UPDATED on 30 Jan 2018 AAT+rHoKx5wQkWhxlfriybFocBu3RBrPD2/ySwlwmvA=		Traffic volume only	Unbound	
securedns.eu	146.185.167.43 2a03:b0c0:0:1010::e9a:3001	853	dot.securedns.eu	h3mufC43MEqRD6uE4lz6gAgULZ5/rigH/E+U+jE3H8g=		None	HaProxy + Bind	NOTE 1: SecureDNS has support for additional TLDs of OpenNIC, Emercoin, and Namecoin NOTE 2: While both secure.eu and dot.secure.eu are running pin only validation for dot.secure.eu will not work!
dns-tls.bitwiseshift.net	81.187.22.124 2001:8b0:24:24::24	853	dns-tls.bitwiseshift.net	YmcYWZU5dd2EobIZHNf1jTUPVS+uK3280YYCdz4l4wo=		None	Unbound	
ns1.dnsprivacy.at	94.130.110.185 2a01:4f8:c0c:3c03::2	853	ns1.dnsprivacy.at	vqVQ9TcoR9RDY3TpO0MTXw1YQLjF44zdN3/4PKLwtEY=		None	Unbound	See https://dnsprivacy.at/
ns2.dnsprivacy.at	94.130.110.178 2a01:4f8:c0c:3bfc::2	853	ns2.dnsprivacy.at	s5Em89o0kigwBF1gcXWd8zIATSWVXsJ6ecZfmBDTKg=		None	Unbound	
dns.bitgeek.in (India)	139.59.51.46	853	dns.bitgeek.in	FndaG4ezEBQs4k0Ya3xt3z4BjFEyQHd7B75nRyP1nTs=		Traffic volume only	Nginx + BIND	
Lorraine Data Network	80.67.188.188 2001:913::8	85343		WaG0kHUS5N/ny0labz85HZg+v+f0b/UQ73lZjFep0nM=		Traffic volume only	stunnel 4 + BIND	See https://ldn-fai.net/serveur-dns-recursif-ouvert/ (note, logging of IP address at stunnel no longer performed). A self-signed certificate is used, so SPKI pinning is must be used.
dns.neutopia.org	89.234.186.112 2a00:5884:8209::2	85343	dns.neutopia.org	wTeXHM8aczhRSi0cv2qOXkXInoDU+2C+M8MpRyT3O1=		No logging	Knot Resolver	
BlahDNS	108.61.201.119 2001:19f0:7001:1ded:5400:01ff:fe90:945b	85343	dot-jp.blahdns.com			No logging		https://blahdns.com/ NOTE1: Located in Japan. Also does DoH . NOTE2: Note that port 443 REQUIRES an authentication name UPDATED 22nd JAN 2018: note the authentication name has changed

BlahDNS	159.69.19 8.101 2a01:4f8: 1c1c: 6b4b::1	8 53 4 43	dot- de. blah ns. com			No logging		https://blahdns.com/ NOTE1: Located in Frankfurt. Also does DoH . NOTE2: Note that port 443 REQUIRES an authentication name
Go6Lab	2001:67c: 27e4::35	8 53	privac ydns. go6la b.si	g5lqtW Hia/plKqWU /Fe2Woh4+7MO3d0JY qYJpjiYAw=		No logging	Unb ound	
Tenta	99.192.18 2.200, 66.244.15 9.200	8 53	iana. tenta. io			Traffic volume only	Tenta	https://tenta.com/privacy-policy
Tenta	99.192.18 2.100, 66.244.15 9.100	8 53	openn ic. tenta. io			Traffic volume only	Tenta	NOTE: Uses OpenNIC Root!
dns.233py.com	Various, see notes	8 53	dns. 233py .com			No logging	Unb ound + DO HC /S	https://dns.233py.com (Chinese language version) Shanghai (Eastern China): 47.101.136.37/ edns.233py.com Chongqing (Western China): 118.24.208.197/ wdns.233py.com Beijing (North China): 114.115.240.175/ ndns.233py.com Guangzhou (Southern China): 119.29.107.85/ sdns.233py.com NOTE: Blocks ads and trackers. Also support DoH (see website)
Secure DNS Project by PumpleX	51.38.83.1 41 2001: 41d0:801: 2000::d64	8 53	dns. oszx. co	P /Auj1pm8MiUpelxGcrE uMJOQV+pgPY0MR4 awpclvT4=		No logging		https://dns.oszx.co NOTE1: Also does DoH and dnscrypt NOTE2: Performs ad blocking
Foundation for Applied Privacy	37.252.18 5.232 2a00: 63c1:a: 229::3	8 53 4 43	dot1.a pplied privac y.net		Y	Only aggre gated logging , no PII	unb ound	https://appliedprivacy.net/services/dns/ NOTE: Also does DoH and has an .onion endpoint
ibksturm.synology.me	178.82.10 2.190	8 53	ibkstu rm. synolo gy.me			No logging	ngin x + unb ound	https://github.com/ibksturm/dnscrypt-switzerland NOTE: Also does DoH and dnscrypt no filters, opennic root copy
DNS Warden	116.203.7 0.156 2a01:4f8: 1c1c: 75b4::1	8 53	dot1. dnswarden. com			No logging	dnsd ist	DETAILS UPDATED 18th Mar 2019 Website is a work in progress: dnswarden.com NOTE1: These servers have ad and tracker blocking with return of NXDOMAIN for bad domains. NOTE2: Also supports OpenNIC TLDs. Also does DoH .
DNS Warden	116.203.3 5.255 2a01:4f8: 1c1c: 5e77::1	8 53	dot2. dnswarden. com			No logging	dnsd ist	

Servers with minimal logging/limitations

These servers use **some logging**, self-signed certs or no support for Strict mode.

Hosted by	IP addresses	TLS Ports	Hostname for TLS authentication	Base 64 encoded form of SPKI pin(s) for TLS authentication (RFC7858)	TLSA record published	Logging	Software	Notes
NIC Chile	200.1.123. 46 2001: 1398:1:0: 200:1:123: 46	853	dnsotls. lab.nic.cl	pUd9cZpbm9H8ws0tB5 5m9BXW4TrD4GZfBAB 0ppCziBg=	Y	Yes, for research purposes	Unbound	Details updated 18th Sept - now uses Let's encrypt cert
OARC	184.105.1 93.78 2620:ff: c000:0:1: 64:25	853	tls-dns-u. odvr.dns- oarc.net	pOXrpUt9kgPgbWxBFF cBTbRH2heo2wHwXp1f d4AEVXI=		Yes, see OARC website	Unbound	See OARC website NOTE: As of June 2017 this server does not support Strict Mode because it does not offer the correct cipher suites to match RFC7525 recommendations.
Rubyfish Internet Tech	115.159.1 54.226 47.99.165. 31	853	dns. rubyfish. cn	DBDigy3zDS7TN /zbQOmjZ0qW+qbRVz IsDKSsTwSxo=		Yes, see rubyfish website (only chinese version now)	Unbound	115.159.154.226/ ea-dns.rubyfish.cn use upstream located in Hongkong/Japan to resolve domains poisoned by the China-GFW47.99.165.31/ uw-dns.rubyfish.cn use upstream located in US-West.