

Malware and Phishing Protection with DNS-Based Filtering

Anonyproz OpenVPN servers offers malware and phishing protection using DNS-based filtering on our private and secure DNS servers. Our OpenVPN system will detect and block all DNS requests to known malicious sites obtained from various user contributed sources such as malware and phishing sites as part of our service. This means that once connected to any of our OpenVPN server, any outgoing traffic to a known malicious site in our database will be blocked, thereby preventing the website from loading in your browser. Once connected to our servers, your default ISP DNS servers are automatically bypassed and you will be connected to the internet using our private DNS servers which are then forwarded to Google DNS servers to take advantage of its anycast routing technology to send users to the geographically closest data center.

How Does the DNS-Based Malware & Phishing Filtering Work?

Malware and phishing sites are typically hosted and used by cyber criminals to cause damage to a computer or network, disrupt system operations, gather sensitive personal information such as bank account logins, credit cards and social security numbers, send SPAM (SPAM zombies), or take control of your PC as part of a botnet network.

The most common way to get infected by a malware is by visiting the malware or phishing site, downloading files, downloading email attachments etc. Since all malware and phishing sites use DNS to translate their domain names into machine readable IP-addresses needed to locate the requested web-server on the Internet, it makes sense to block or filter them at the DNS level. The DNS works like a phone book such that each time your computer visits a web site; it needs to get the IP address of the site.

Thus by integrating our OpenVPN services with malware/botnet/phishing filtering, our subscribers obtain an extra layer of protection in combination with a secure anonymous and encrypted internet using OpenVPN strong encryption.

Once connected to our OpenVPN servers, access to these known malicious sites are automatically blocked at the DNS level (DNS sinkhole) thereby preventing the sites from loading in your browser. You will be automatically redirected to our malware alert page at: <http://184.22.136.125> when a DNS request is made for a malicious domain listed in our database. . Our custom DNS sinkhole system is currently blocking over 300,000 malicious domains.

To see these blocked domains, please go to our Malware DNS Sinkhole web portal at:
<https://www.anonyproz.com/dnssinkhole/>

To see how the DNS sinkhole works in practice, just connect to any our OpenVPN servers, open your browser and try and visit any of the domains listed on the DNS Sinkhole Web Portal using the link above.

The domain will be prevented from loading and you will be re-directed to our malware alert page at:
<http://184.22.136.125/>

Using the web portal, users are able to view the blocked domains, request domain delist, add new and suspected malicious domains for inclusion etc.

The following highlights the benefits of our new DNS system:

1. Integration malware, botnet and phishing protection.
2. Faster, reliable and more secure DNS
3. Faster DNS Queries via Google anycast routing DNS infrastructure
4. Custom and community generated malicious domain blocking