

How Is Website Blocking Implemented?

DNS tampering

DNS tampering occurs when Internet Service Providers (ISPs) interfere with the DNS resolution for a particular hostname, preventing you from accessing it (e.g. by returning the wrong IP address).

HTTP blocking

HTTP blocking occurs when an ISP **interferes with the connection between your computer and the server hosting the website** you're trying to access.

This can be implemented by intercepting your HTTP request (in some cases, redirecting you to a block page) or by closing the connection (thereby preventing the normal exchange between your computer and the server of the website).

IP blocking

IP blocking occurs when Internet Service Providers (ISPs) **block connections to the IP address** of a website.

SNI-based filtering

SNI is an extension for the TLS protocol (used for websites hosted on HTTPS), designed to specify what hostname the encrypted connection should be established with.

As the SNI field is unencrypted, ISPs are able to see if you are trying to access a banned website and restrict access (for example, by closing the connection).

Censorship that is **informed by the SNI field** is characterised as SNI-based filtering.

Detection method	Blocking method					
	Closing the connection (RST or FIN)	Packet dropping	Traffic throttling	MITM	Bad HTTP response	Bad DNS answer
Destination IP (+ port)	✓	✓	✓	✓		
Domain in DNS query						✓
HTTP Host header	✓	✓	✓	✓	✓	
SNI field in TLS handshake	✓	✓	✓	✓		