What to Do if Your IP is Blacklisted by DNSBL

If you are using a public static IP address, then an IP address being in the blacklists may mean that bot activity, participation in DDoS attacks, or spam mailing has been recorded in your network.

The presence of a dynamic IP address from the "home" IP address ranges of providers in blacklists is generally normal, because malicious activity in this case may not be coming from your network.

Steps to Follow When on Blacklist

1. Find out the reason for getting into the DNSBL list. Often the service names a specific virus or network worm and its features - the ports used, and protocols. Follow the service recommendations.
2. Activate the intrusion prevention system on your gateway. Analyze the logs and the presence of requests to the botnet command centers.
3. Check all computers in your network with an antivirus. Make sure that the antivirus protection is activated, the databases are updated (as a rule, viruses interfere with updating databases or the work of antivirus software).
4. After treating infected computers, send a message to the DNSBL service with a request to exclude your IP from the blacklist.

SafeUTM

Our solution has all the functionality that provides maximum protection from spam bots, and botnet clients, and the prevention of viral activity in your network.

A 40-day trial version is available for up to 10,000 users.

Get SafeUTM

Revision #5
Created 27 August 2022 22:23:14 by Val Redman
Updated 30 March 2023 06:55:16