Web Filtering Bypass Prevention

Common recommendations:

1. Block the **Proxies & Anonymizers** category.
2. Block the **Firefox/Chrome Secure DNS** feature in the **VPN and Proxy** section of AppBlocker.
3. Make sure that all of your **users have restricted operating system rights**. If a user has no administrator rights, it will be impossible for them to delete the SafeDNS Agent, install any VPN/proxy, change the "hosts" file, or change the DNS server in the network settings.
4. **Prohibit access to any other DNS.** If devices connect to the internet via a gateway or router, prohibit access to all DNS servers, except the SafeDNS public DNS servers. We recommend excluding the **195.46.39.0/24** network as well, as this is a whole SafeDNS network. If you are using a caching server in your corporate network, exclude its address instead.
5. **Prohibit access to HTTP proxies.** To do that, restrict packet transfer to all IP addresses by TCP and UDP protocols on ports **3128** and **8080** in the firewall settings of your router.
6. **Prohibit access to DNS over TLS.** To do that, restrict packet transfer to all IP addresses, except SafeDNS network **195.46.39.0/24**, on TCP port **853**.
7. **Disable IPv6 protocol.** Even though SafeDNS does support IPv6 addresses, we generally recommend disabling this protocol on your router or in the network settings of your device. Please note, that this will not have any effect on the quality of your internet connection.

Recommendations for system administrators:

1. Set up DNS requests rerouting to the SafeDNS public DNS server or to the caching server of your corporate network.
2. Prohibit access to any external proxy servers.
3. Restrict direct access to any website via its IP address.
4. Restrict connection to unknown external VPN servers.
5. Restrict running any unknown application.
6. Restrict using any unknown hardware.

Revision #3
Created 28 August 2022 23:17:50
Updated 2 October 2023 17:06:33 by Val Redman