Рекомендации по усилению защиты от обхода фильтрации

Общие рекомендации

1. Заблокируйте категорию **Прокси и анонимайзеры**.
2. Убедитесь, что **пользователи используют ограниченную учетную запись** в операционной системе. Использование ограниченной учетной записи и отсутствие доступа пользователей к учетной записи администратора лишает пользователей возможности удалить агент SkyDNS, установить стороннее программное обеспечение, изменить файл hosts или изменить сетевые настройки, в том числе возможности изменить адрес сервера DNS.
3. **Запретите доступ к другим DNS**. Если доступ в интернет осуществляется через шлюз или бытовой роутер, то, по возможности, запретите доступ к любым другим серверам DNS кроме 193.58.251.251 или кэширующего сервера DNS на вашем шлюзе/роутере. Для этого в настройках firewall на роутере запретите прохождение пакетов по протоколам TCP и UDP на порт 53 на любые IP-адреса, кроме 193.58.251.251.
4. **Запретите доступ к HTTP прокси серверам**. Для этого в настройках firewall на роутере запретите прохождение пакетов по протоколам TCP и UDP на наиболее популярные порты 3128 и 8080 на любые IP-адреса.
5. **Отключите опцию DNS Crypt** в браузерах, также эта опция может называться **Использовать безопасный DNS сервер**.

Рекомендации для администраторов корпоративных сетей

1. Настройте перенаправление DNS запросов на адрес серверов SkyDNS или на кэширующий сервер DNS в корпоративной сети.
2. Запретите доступ к внешним прокси серверам.
3. Ограничите доступ к сайтам с обращением к ним по прямому IP адресу, без ввода имени сайта.
4. Ограничьте пользователям возможность создавать и осуществлять подключения к неизвестным внешним серверам VPN.
5. Ограничьте пользователям возможность запускать стороннее программное обеспечение.
6. Ограничьте пользователям возможность подключать стороннее оборудование к рабочим станциям.

Revision #2
Created 22 November 2023 08:23:03 by Виктор
Updated 6 December 2023 05:37:21 by Виктор