Защищённый DNS-хостинг

servicepipe

ОТКАЗОУСТОЙЧИВОСТЬ И ЗАЩИТА DNS ОТ DDOS-АТАК
И АНОМАЛЬНЫХ НАГРУЗОК.

Зачем защищать DNS

Атаки на DNS — по-прежнему одна из самых разрушительных киберугроз. Поскольку если из-за DDoS-атаки произошёл сбой в работе DNS, то даже при подключенной эшелонированной защите IT-инфраструктуры и приложений сервисы не будут доступны для пользователей и сотрудников.

Чтобы DNS-сервер не стал точкой отказа, рекомендуем защищённый DNS-хостинг, подключаемый вариативно: как основной (Primary DNS) или резервный (Secondary DNS).

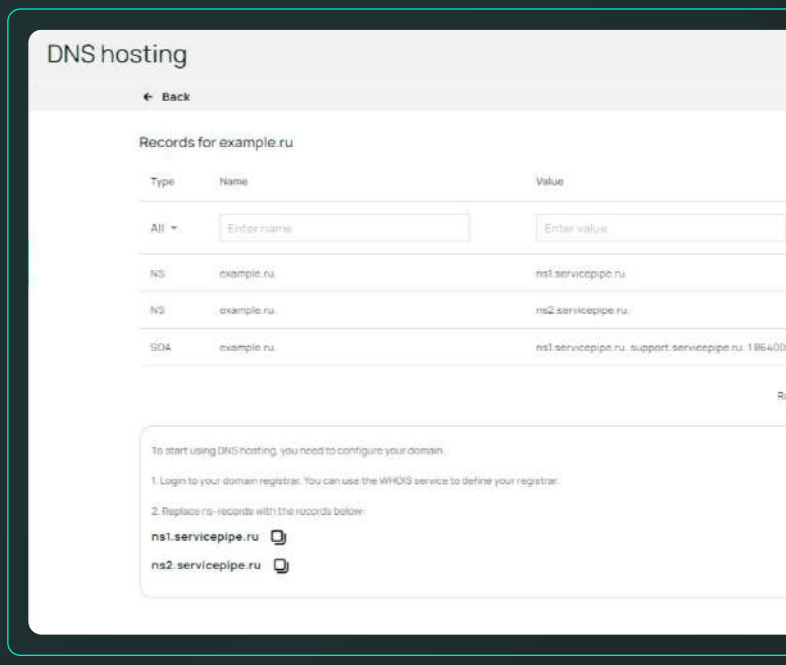
Т БАНК ökko ОНЛАЙН ТРЕЙД.РУ точка ЦРПТ

Primary DNS

Как работает

Подключая основной DNS-хостинг в Servicepipe, вы делегируете домен, указывая как авторитетные наши NS-серверы.

И в дальнейшем сами управляете DNS-зоной в личном кабинете Servicepipe, внося изменения в DNS-записи.



Для кого предназначен

Подключить защищённый основной DNS в Servicepipe мы рекомендуем всем, кто хочет быть уверен в защищённости авторитетных DNS-серверов.

Кроме того, использование нашего DNS-хостинга Servicepipe как основного упрощает подключение защиты от DDoS и ботов для сайта, веб-приложения и API.

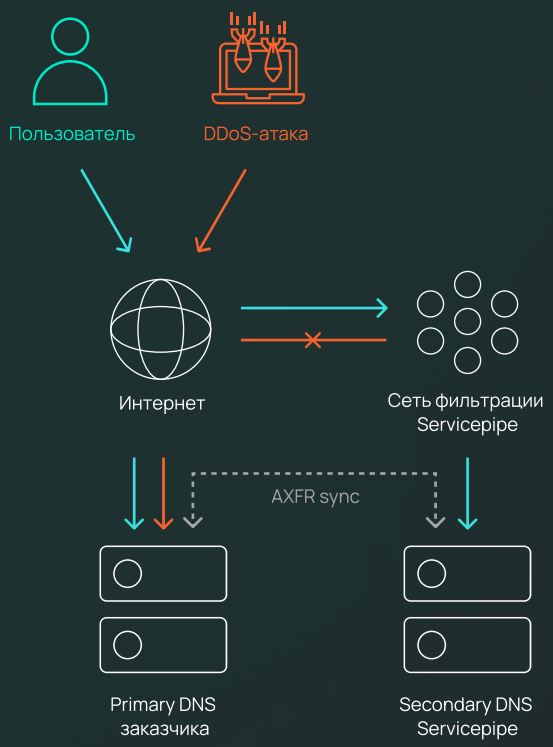
Secondary DNS

Как работает

Резервный DNS подключается параллельно вашему основному DNS-серверу.

При недоступности основного, резервный DNS продолжает принимать запросы пользователей и отдавать последний актуальный статус доменной зоны.

Secondary DNS не только блокирует паразитные запросы, но и забирает на себя часть избыточного легитимного трафика DNS. Нагрузка между основным и дублирующим DNS-серверами балансируется по алгоритму round-robin.



Для кого предназначен

Защищённый резервный DNS мы рекомендуем всем, кто хочет гарантировать отказоустойчивость онлайн-ресурсов за счёт подключения второго DNS-провайдера.

Почему защищённый DNS-хостинг Servicepipe

Защищённость от DDoS-атак по умолчанию благодаря системе DosGate	Отказоустойчивость DNS-сервера за счёт распределённой архитектуры	Резервирование программных и физических компонентов в каждой локации	Сертифицированные дата-центры Tier III	<10 минут на подключение

Истории защиты

точка

Когда весной 2022 года массово заливали мусорным трафиком ресурсы российских банков, ЦОДы и веб-хостингов в «Точке» решили дополнительно защитить свои DNS-серверы.

«Во время известных атак на Рег.ру проблем с DNS у нас не было, но наши DNS-серверы находились в тех же ЦОДах, что и вся наша инфраструктура.
А во время атак на ЦОДы мусорным трафиком заливало наши файрволы.
Поэтому мы подняли резервный DNS Servicepipe, чтобы он был не в нашей сети, а снаружи. Теперь используем защищённый DNS, который для нас ещё резервный.
Зоны и NS-записи обслуживаем сами».

Антон Казанцев
архитектор ИБ

Интернет-аптека

Необходимость в защищённом DNS-сервере возникла во время первой масштабной DDoS-атаки на nic.ru. Тогда от неё пострадали многие пользователи. Но при втором падении nic.ru из-за DDoS атака на DNS хостинг-провайдера осталась для клиентов интернет-аптеки незамеченной.

«Использование Secondary DNS помогло нам сохранить работоспособность сервисов при повторной атаке на nic.ru».

Директор по информационной безопасности
онлайн-аптеки

Сколько стоит DNS-хостинг

от **20 000** рублей.

в минимальный пакет включено до 20 зон.

servicepipe

Защищённый DNS-хостинг — это гарантия стабильной доступности и отказоустойчивости ваших онлайн-ресурсов, а также удобство подключения продуктов защиты Servicepipe в будущем.

Оставьте заявку на подключение или свяжитесь с нами, чтобы обсудить технические детали и получить дополнительные материалы о продукте.

welcome@servicepipe.ru +7 (495) 374-62-65 servicepipe.ru