Исследование распространенности в РФ поддержки EDNS

Автор: А. Венедюхин, ведущий аналитик Технического центра Интернет (при участии Координационного центра доменов .RU/.РФ)

Краткое описание

Речь идёт о согласованном прекращении поддержки резолверами "обходных механизмов", позволяющих сейчас работать с DNS-серверами, которые не отвечают на запросы с EDNS. Согласованность состоит в том, что разработчики самых распространённых резолверов (BIND, PowerDNS, Knot, Unbound) договорились синхронизировать выпуск новых версий, в которых "обходные механизмы" отключены. Дата: 1 февраля 2019 года.

Так как DNS, независимо от объявления flag days, всё равно меняется медленно, то каких-то внезапных массовых "отключений сайтов" в связи с данным нововведением не ожидается. Локальные проблемы - возможны, но их можно упредить.

Подробности

EDNS - набор расширений для оригинального протокола DNS, позволяющий дополнить его рядом полезных функций, например: увеличение размера ответа; передача списков опций, поддерживаемых сервером или клиентом-резолвером; и так далее. Среди ключевых моментов, на которые, например, ссылается ISC (в контексте BIND), возможность использования в EDNS сигналов DNS-cookie. Эти сигналы могут применяться для противодействия DDoS-атакам. Кроме того, поддержка EDNS необходима для работы DNSSEC.

Изменения, о которых идёт речь, коснутся только ситуации, когда резолвер не получает никакого ответа на запрос, отправленный с EDNS. Такое возможно в следующих случаях:

1) авторитативный сервер игнорирует запросы, не укладывающиеся в "классический" формат (встречается весьма редко, обычно, в "самодельных" системах, так как все распространённые программные пакеты DNS-серверов - EDNS поддерживают). В этом случае - считается, что авторитативный сервер настроен некорректно, так как он должен прислать тот или иной ответ, например, сообщение об ошибке;

2) запросы или ответы фильтруются промежуточными узлами. Обычно, это разнообразные межсетевые экраны. Фильтроваться могут либо запросы/ответы, превышающие определённую длину (типовые для UDP 512 байтов), либо запросы/ответы, которые содержат дополнительные флаги. Первый вариант, с ограничением по длине, напрямую к EDNS не относится, но, тем не менее, работе протокола препятствует. Второй вариант - непосредственно связан с EDNS, так как работает "по DNS-заголовкам", однако на практике этот вариант вряд ли встречается. Фильтрация DNS-пакетов может использоваться в составе мер противодействия DDoS-атакам. Основная особенность здесь в том, что корректно работающий резолвер и корректно работающий авторитативный сервер всё равно не могут провести обмен данными в рамках протокола, так как им мешает промежуточный фильтр.

Ранее резолверы использовали дополнительные "обходные механизмы", позволявшие преодолеть сбой и "договориться" с неверно настроенным или недоступным по EDNS авторитативным сервером. Эти механизмы сводятся к повтору DNS-запросов, но с другими сочетаниями параметров, в том числе, без EDNS. После наступления "переломного дня" (01.02.2019) новые версии резолверов перестанут пытаться "договориться", а станут считать авторитативный сервер, от которого не был получен ответ на запрос с EDNS, нерабочим, соответственно, перестанут к нему обращаться. В этом и состоит "переломный момент" DNS flag day.

Такое поведение подразумевает, что каждый авторитативный сервер должен быть доступен для корректных DNS-запросов, отправляемых с EDNS, и сервер должен отвечать на такие запросы. Из этого не следует, что сервер должен полностью поддерживать EDNS: если сервер отвечает корректным пакетом с кодом DNS-ошибки ("Ошибка формата"), то в этом случае резолвер всё же попробует повторить запрос без EDNS. В частности, такое поведение заявлено для Unbound и BIND. То есть ужесточается только обработка отсутствия какого-либо ответа - в таком случае резолвер не пытается отправить запрос без EDNS. Но с практической точки зрения ситуация эквивалентна повсеместному внедрению EDNS, так как устранение "особенностей" обработки EDNS-пакетов там, где эти "особенности" внедрены преднамеренно, проще всего реализовать, внедрив данную технологию в полной мере.

Что нужно сделать

Нововведение не является критическим в масштабах Рунета. Во-первых, проблемы с потерями и блокированием EDNS довольно редки. Во-вторых, на проблемных направлениях ещё должны обновиться резолверы. Что касается авторитативных серверов, то большинство (по числу зон) уже так или иначе поддерживает работу с EDNS-пакетами, поэтому здесь массовой недоступности узлов для конечных пользователей ожидать не следует. Если где-то и остались несовместимые "самодельные" решения либо старые версии типового ПО, то им следует доработать программный код или обновить пакеты.

Особенность данной ситуации в том, что существенную роль играет сетевой транспорт и его настройка. То есть факторы, которые к DNS относятся косвенно, и исправить их обновлением ПО DNS нельзя. Здесь, в теории, возможна ситуация, когда крупный провайдер доступа обновит резолверы, но не поменяет настройки прохождения пакетов, соответственно, его конечные клиенты останутся без службы DNS (ситуация теоретическая, потому что такой провайдер уже должен был бы отмечать дефекты в работе DNS на своих сетях). Поэтому, для исключения возможных аварий, требуется участие провайдеров доступа, служб NOC, обеспечивающих прохождение пакетов DNS "в обе стороны" - и на стороне клиентов (рекурсивных резолверов), и на стороне автортитативных серверов. Такое участие состоит в проверке правил межсетевых экранов и подобного программно-аппаратного обеспечения: пакеты EDNS, при штатной работе сети, не должны блокироваться (если тотальное блокирование всё же необходимо, то следует отправлять на адрес источника пакета сообщение DNS о неверном запросе).