CNS Solution

Carrier-Grade Caching DNS

Март 2020

сети и коммуникации
ВИНКО-Т

Значимость DNS

Критичный сервис

DNS – критически важная часть услуги доступа в Интернет.

Недостаточное качество **реализации DNS сервиса** влияет на клиентов также как и маршрутизатор сети теряющий пакеты: медленная или ненадежная работа DNS воспринимается как услуга доступа в Интернет низкого качества.

Результаты коммерческой эксплуатации решения CNS для Операторов Связи

- Исключение финансовых потерь из-за простоя
- Уменьшение стоимости обслуживания системы DNS
- Возможность оказывать дополнительные сервисы на базе решения CNS (фильтрация, безопасность, NXR)
- Повышение лояльности клиентов
- Сокращение количества необходимого оборудования
- Возможности диагностики CNS позволили выявить аномалии в поведении клиентов и оборудования

Типичные проблемы DNS у Операторов Связи

Избыточное количество оборудования

В силу низкой производительности обычно применяемого программного обеспечения у Операторов Связи с большим количеством абонентов часто используются десятки серверов для обслуживания DNS трафика.

Проблемы с производительностью программного обеспечения “затыкаются” увеличением количества серверов, использованием дорогостоящих балансировщиков нагрузки, разделением трафика от разных групп абонентов на разные кластера DNS серверов.

Большое количество оборудования усложняет диагностику и приводит к длительному решению возможных проблем.

Типичные проблемы DNS у Операторов Связи

Недостаточная функциональность программного обеспечения

Все современное программное обеспечение DNS с открытым кодом создавалось в расчете на некоего усредненного пользователя или как эталонная реализация той или иной спецификации RFC.

Ни в одной реализации программного обеспечения с открытым исходным кодом кеширующего DNS не реализованы функции, необходимые Операторам Связи, такие как: политики DNS, диагностика выполнения запросов в контексте сервера, механизм ограничения скорости запросов в расчете на единичных абонентов или групп абонентов, адаптивное проактивное кеширование, API, SNMP и других.

Отличия Anycast CNS от других решений

Функциональные отличия Anycast CNS от других реализаций кеширующих DNS серверов

	ISC BIND	NLnet Labs Unbound	PowerDNS Recursor	Anycast CNS
Высокая производительность в условиях трафика от более чем 1M/10M Абонентов	Нет/Нет	Нет/Нет	Да/Нет	Да/Да
Приоритезация запросов к значимым доменам	Нет	Нет	Нет	Да
Возможность журналировать все запросы и ответы от Абонентов и ответов к ним без потери производительности	Нет	Нет	Нет	Да
Возможность стриминга журнала запросов в Apache Kafka	Нет	Нет	Нет	Да
Возможность журналировать все запросы к авторитативным серверам и ответы от них без потери производительности	Нет	Нет	Нет	Да
Ответ из кэша при недоступности авторитативных северов для популярных доменов	Нет	Нет	Нет	Да
Ограничение скорости запросов от Абонентов	Нет	Нет	Нет	Да, можно гибко управлять лимитами на основе политик и групп Абонентов, подсетей, типа запроса и пр.

Отличия Anycast CNS от других решений

Функциональные отличия Anycast CNS от других реализаций кеширующих DNS серверов

	ISC BIND	NLnet Labs Unbound	PowerDNS Recursor	Anycast CNS
Поддержка разных представлений для клиентов (view)	Да	Нет	Нет	Да
Встроенные списки доменов	Через локальные зоны	Через локальные зоны	Через локальные зоны	Да
Встроенные списки IP-адресов	Да	Нет	Нет	Да
Возможность управлять DNS запросами через встроенные политики	Нет	Через медленные внешние политики на Python	Через LUA скрипты	Да
Возможность использовать встроенные списки доменов и адресов в правилах политик	Нет	Нет	Нет	Да
Интерактивная симуляция выполнения запроса от Абонента с полным диагностическим выводом	Нет	Нет	Нет	Да
Отчеты по DNS запросам вида TOP-100 авторитативных серверов с максимальным количеством потерь запросов	Нет	Нет	Нет	Да
Мониторинг SNMP	Нет	Нет	Нет	Да
Программный интерфейс API на полную функциональность	Нет	Нет	Нет	Да

Отличия Anycast CNS от других решений

Функциональные отличия Anycast CNS от других реализаций кеширующих DNS серверов

	ISC BIND	NLnet Labs Unbound	PowerDNS Recursor	Anycast CNS
Поиск и выборка запросов от Абонентов через модификаторы поиска	Regex	Regex	Regex	Да
Поиск и выборка запросов к авторитативным серверам через модификаторы поиска	Нет	Нет	Нет	Да
Разделение GLUE и AUTH данных	Нет	Нет	Нет	Да
Защита от спуфинга через повторение первого запроса	Нет	Нет	Нет	Да
Конфигурация полностью построенная на основе объектов	Нет	Нет	Нет	Да
Защита от ошибок синтаксиса в конфигурации	Нет	Нет	Нет	Да
Адаптивные тайм-ауты при обращении к внешним серверам	Нет	Нет	Нет	Да
Счетчики “плохих” запросов	Нет	Нет	Нет	Да
Прагматичное распределение нагрузки к внешним серверам, во избежание их перегрузки	Нет	Нет	Нет	Да
Встроенная поддержка DNS over TLS	Нет	Да	Нет	Да
Встроенная поддержка DNS over HTTPS	Нет	Нет	Нет	Да

Улучшаем работу DNS через внедрение CNS

Кейс №1: Сокращаем количество оборудования

Для обслуживания 4M запросов в секунду при пятидесятипроцентной нагрузке оборудования необходимо всего четыре сервера CNS в защищенной от сбоев конфигурации. Этого достаточно для обслуживания жителей небольшой страны в 40M Абонентов на одном кластере CNS.

Типовая архитектура решения CNS предполагает балансировку нагрузки через equal-cost multi-path routing схему и не требует балансировщиков нагрузки.

Получаем более простую и производительную архитектуру кеширующего DNS, защищенную от сбоев по аппаратному обеспечению и электропитанию.

Улучшаем работу DNS через внедрение CNS

Кейс №2: Сводим в один кластер DNS всех клиентов

Решение CNS не испытывает никаких трудностей при обслуживании большого количества клиентов, даже в случае существенно различающейся характеристики нагрузки от них. Оптимизированные структуры кеша и алгоритмы работы делают невозможным его “вымывание” одними клиентами в ущерб другим. Чем больше трафика обслуживает решение CNS, тем меньшую задержку обработки запросов получают его клиенты.

Получаем лучшее качество обслуживания клиентов за счет большей наполненности кеша DNS и как следствие лучшего Cache Hit Ratio.

Улучшаем работу DNS через внедрение CNS

Кейс №3: Выполняем требования Минкомсвязи

Минкомсвязи в 2019 году утвердило требования к операторам связи и интернет-сервисам, выполняющим функции DNS. Такие сервисы должны будут в течение года хранить информацию о пользователях и обеспечивать время отклика не более 100 мс.

Решение CNS полностью отвечает требованиям приказа Минкомсвязи №510 от 16.09.2019 и может быть развернуто на всех Абонентах за считанные дни.

Получаем соблюдение нового законодательства при помощи родного для протокола DNS программного обеспечения, улучшая, а не ухудшая качество облуживания Абонентов.

Улучшаем работу DNS через внедрение CNS

Кейс №4: Избавляемся от промежуточных сетевых экранов

Решение CNS позволяет гибко управлять DNS трафиком для клиентов через механизм политик, выполнять ограничение скорости для единичных клиентов или групп клиентов. “Плохие” запросы обрабатываются на ранних этапах и не вредят производительности решения CNS. Для любых манипуляций с трафиком DNS достаточно встроенных механизмов решения.

Получаем единый механизм управления безопасностью DNS, исключаем фрагментацию ответственности между разными отделами за работоспособность решения.

Улучшаем работу DNS через внедрение CNS

Кейс №5: Упрощаем и стандартизируем диагностику

Решение CNS позволяет проводить диагностику DNS запросов в контексте сервера без потери производительности. Любая диагностика запросов требует только лишь встроенных средств. Помимо встроенной диагностики выполнения запросов есть возможность инспектировать содержимое кеша сервера, включая сведения о том с какого авторитативного внешнего сервера были получены и закешированы данные. Все запросы от клиентов и все запросы самого CNS на внешние сервера журналируются без снижения производительности.

Получаем быструю, простую и достоверную диагностику.

Улучшаем работу DNS через внедрение CNS

Кейс №6: Разворачиваем дополнительные сервисы

Решение CNS позволяет организовывать на своей основе дополнительные сервисы.

Примером такого сервиса может быть фильтрация вирусных доменов.

Получаем более лояльных клиентов и зарабатываем на предоставлении дополнительного сервиса.

Улучшаем работу DNS через внедрение CNS

Кейс №7: Удерживаем трафик DNS запросов Абонентов от перетекания в Google

Решение CNS имеет встроенную поддержку DNS over TLS (DoT) и DNS over HTTPS (DoH).

Эти стандарты набирают популярность в программном обеспечении для мобильных устройств и в веб-браузерах. В последних версиях Android теперь будет пытаться создать DoT-сессию, прежде чем использовать незашифрованный DNS-сеанс.

Кроме того, и Google, и Mozilla объявили, что будут поддерживать DoH в следующих версиях Chrome и Firefox.

Улучшаем работу DNS через внедрение CNS

Кейс №7: Удерживаем трафик DNS запросов Абонентов от перетекания в Google

Google, в частности, заявил, что в Chrome они попытаются использовать DoH-сервер, если он может быть обнаружен в локальной сети, а также упростят пользователям выбор другого сервера, который поддерживает DoH, если DoH у текущего провайдера недоступен. Очень вероятно, что в конечном итоге Google Chrome начнет предупреждать пользователей об отсутствии поддержки DoH у текущего оператора, что может привести к массовому уводу DNS-трафика от службы DNS оператора к OTT-провайдеру, в частности к Google.

Улучшаем работу DNS через внедрение CNS

Кейс №7: Удерживаем трафик DNS запросов Абонентов от перетекания в Google

Mozilla уже заявляла, что их цель - перевести всех своих пользователей в один из надежных провайдеров (OTT), поддерживающих DoH, которые поддерживают строгие требования конфиденциальности. Единственный способ стать частью этого списка - запустить DoH-совместимую службу DNS.

Если оператор связи не развернет DoT/DoH службы DNS, то большая часть трафика DNS будет маршрутизироваться вне его сети. Результатом будет не только отсутствие видимости DNS, но и ухудшение взаимодействия с пользователем с точки зрения задержки и производительности, а так же снижение лояльности Клиентов.

Ключевые характеристики решения CNS

Возможности конфигурации

Вся конфигурация CNS целиком построена на объектах и взаимоотношениях между объектами.

Конфигурация на объектах дает широкие возможности, такие как простое создание сложных политик обработки трафика или использование миллионов представлений (view) для клиентов.

Конфигурация сохраняется в “in memory” легковесной базе данных с регулярными чекпоинтами на файловую систему.

Ключевые характеристики решения CNS

Адаптивные тайм-ауты

А что если авторитативный DNS сервер, к которому привязался наш кеш по RTT перестал отвечать?

В случае ISC BIND тайм-аут наступит только через 5 секунд.

В случае CNS: тайм-аут через 2 x RTT. Например для сервера, у которого мы фиксировали RTT в 20 миллисекунд время ожидание перед запросом другого сервера составит всего 40 миллисекунд.

Клиент получит ответ в 125 раз быстрее, если он в этой ситуации обслуживался решением CNS!

Ключевые характеристики решения CNS

Адаптивное проактивное кеширование

А что если задержка к авторитативному DNS серверу составляет 500 миллисекунд и TTL у запрашиваемой популярной у клиентов записи установлен в 60 секунд?

В случае ISC BIND раз в 60 секунд клиенты обращающиеся за этой записью будут ждать до 500 дополнительных миллисекунд, перед тем как получить ответ.

В случае CNS задержки перед ответом не будет, так как CNS проактивно перекеширует популярный у клиентов домен, до того как он исчезнет из кеша по TTL.

Ключевые характеристики решения CNS

Обслуживание устаревших данных из кеша

А что если авторитативные сервера, обслуживающие популярный у клиентов домен перестали отвечать?

В случае ISC BIND клиенты будут получать код ответа SERVFAIL, после того как данные по записи устареют вследствие превышения TTL.

В случае CNS клиенты будут получать последние доступные на момент работоспособности авторитативного сервера данные. Для того, чтобы клиенты не кешировали такие ответы CNS будет их отдавать с TTL 0.

Ключевые характеристики решения CNS

Встроенная поддержка DNS over TLS (DoT) и DNS over HTTPS (DoH).

Решение CNS имеет встроенную поддержку DNS over TLS (DoT) и DNS over HTTPS (DoH).

В случае CNS клиенты будут получать лучшую производительность DoH и DoT, чем на DNS решениях, которые поддерживают данные протоколы только с помощью стороннего программного обеспечения (stunnel, nginx).

Встроенная в CNS поддержка DoT/DoH делает возможным журналировать трафик таких клиентов, сохраняя их IP-адреса и порты, а так-же выполнять встроенную диагностику, в отличии от других решений без нее.

Ключевые характеристики решения CNS

Журналирование всего трафика

Сохраняются все DNS запросы от пользователей к сервису и от сервиса к авторитативным серверам. Потоковая трансляция данных с оборудования на внешний агрегатор.

Для выгрузки информации из журнала можно использовать модификаторы поиска.

Возможна выгрузка данных журнала в Apache Kafka.

Не влияет на производительность!

Ключевые характеристики решения CNS

SNMP мониторинг и диагностика со стороны Оператора

Решение CNS поддерживает мониторинг своего состояния по протоколу SNMP.

Инспектирование содержания кеша одной командой с выводом имени домена и относящихся к нему записей, включая данные о том с какого авторитативного сервера была получена информация, оказавшаяся впоследствии в кеше.

Симуляция выполнения DNS запроса с трассировкой внутренних состояний обработки и принудительной рекурсией.

Ключевые характеристики решения CNS

Поведение при вирусных атаках

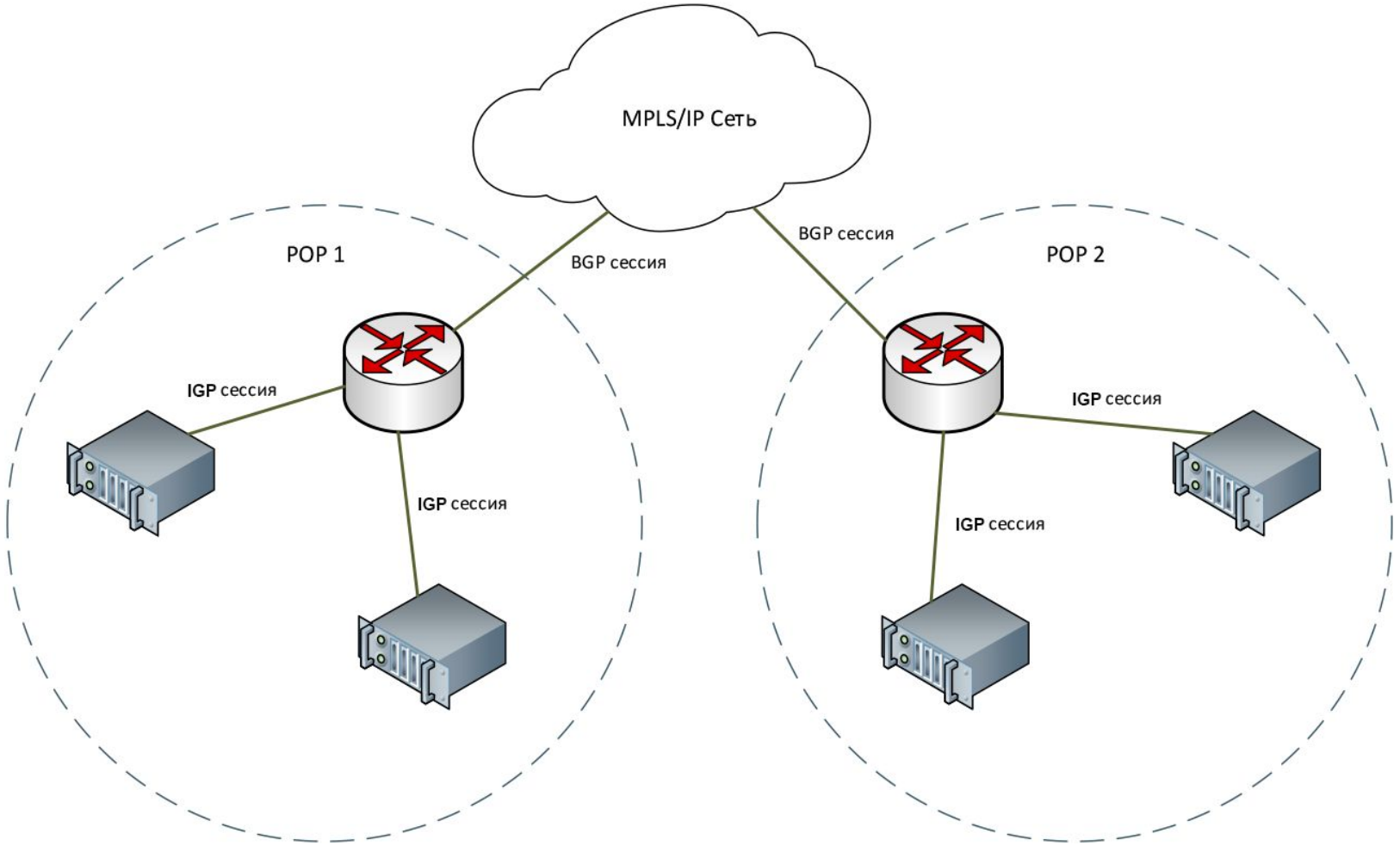
CNS спроектирован работать в условиях постоянных аномалий клиентских запросов.

Гибкая обработка очередей запросов, LRU. “Плохо сформированные запросы” отвергаются на ранней стадии.

Специальная реализация защиты от Chinese Water Turtle атак на DNS.

Ключевые характеристики решения CNS

Схема типовой архитектуры решения с резервированием в двух ДЦ



Ключевые характеристики решения CNS

Проактивная поддержка производителя

Решение CNS при соответствующей настройке отправляет телеметрию производителю.

Производитель в курсе операционного состояния сервиса и может прогнозировать производительность, видеть ошибки и оказывать сервис до того как случится что то, что могут заметить клиенты!

Ключевые характеристики решения CNS

API

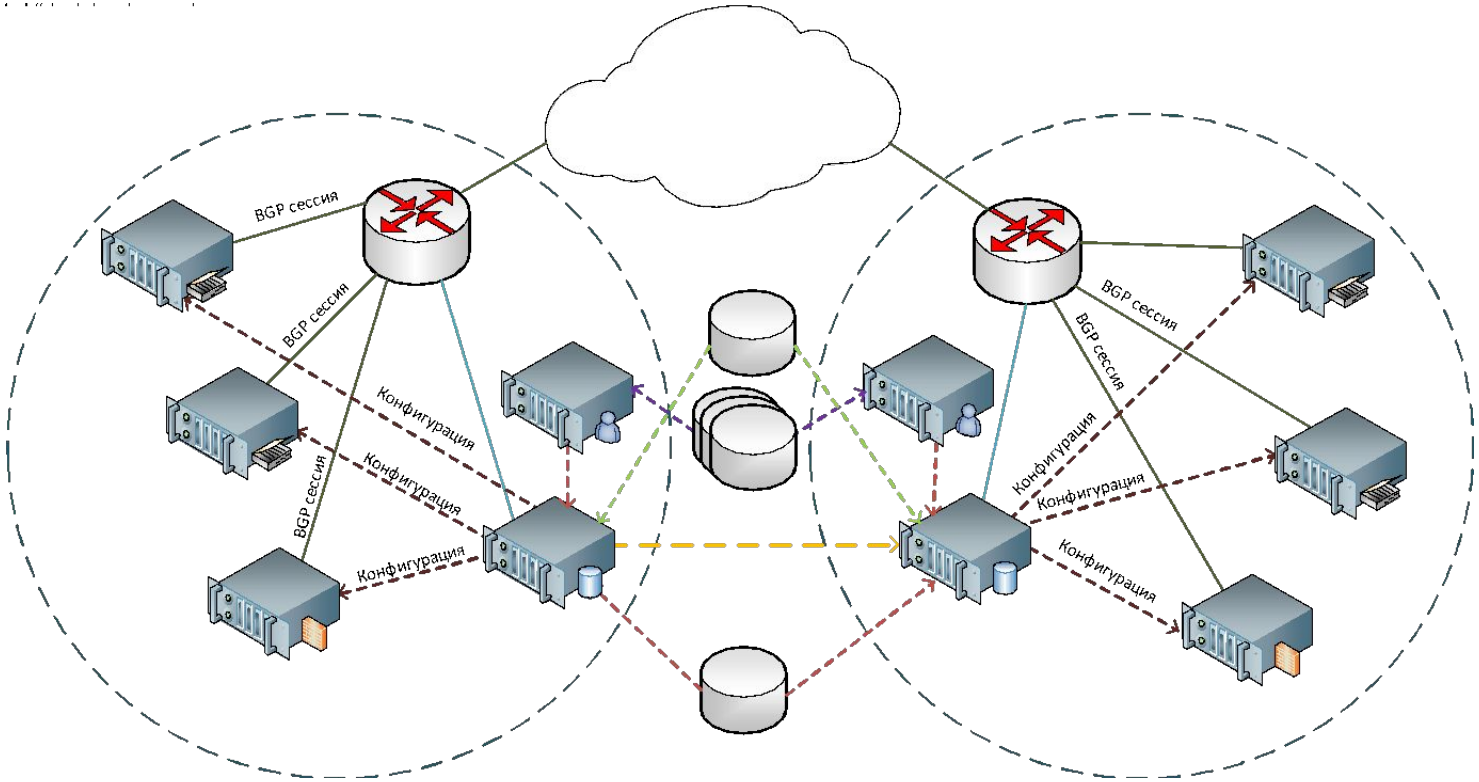
API на всю функциональность.

Поддержка Python, Perl, Java, .NET

Ключевые характеристики решения CNS

Дополнительные сервисы

Фильтрация вирусных доменов и “Персональный Интернет”.



Развертывание решения CNS

PoC

Мы готовы показать преимущества нашего решения в вашей сети, предоставим и настроим демонстрационное оборудование для тестов или опытной эксплуатации.

Развертывание решения CNS

Осознанный выбор!

Выбрав CNS вы увеличите и защитите свои доходы, предложив клиентам лучшие услуги!

Thank You

сети и коммуникации
ВИНКО-Т