Network DDoS protection

Защита ИТ-инфраструктуры от сетевых угроз и DDoS-атак
на базе технологии DosGate

servicepipe

О Servicepipe

Servicepipe работает на рынке защиты более интернет-ресурсов 6 лет. На этапе становления компания фокусировалась на предоставлении услуг защиты провайдерам связи и дата-центрам. Эти сервисы строились на базе оборудования ведущих производителей Arbor Networks и F5 Networks, а в дальнейшем их число пополнили продукты российских компаний БИФИТ Митигатор, и Inoventica.

Работа с решениями разных производителей дала опыт интеграции и создания комплексных сервисов, знание сильных и слабых сторон имеющихся на рынке средств защиты, их возможностей и ограничений. Мы осознали, что идеальных продуктов не существует и приняли решение начать разработку собственных, а также сервисов на их базе.

Сейчас в команде Servicepipe более 50 специалистов в области построения и эксплуатации сетей передачи данных, разработки высоконагруженных решений, Data science, front и back-end разработки.

Мы разрабатываем решения, обеспечивающие доступность и безопасность онлайн-ресурсов и оказываем услуги на базе собственной распределённой инфраструктуры. Решения Servicepipe помогают очистить трафик клиентов и защитить их интернет-активы от внешних угроз различного типа – DDoS-атак, нежелательных ботов, попыток взлома и целевых атак.

Сервисы предоставляются как в виде полностью облачных сервисов, так и по гибридной схеме, с установкой компонент решения внутри ИТ-инфраструктуры клиентов.

Помимо этого, Servicepipe проводит аудиты защищенности, нагрузочное и стресс-тестирование, которые помогают заранее выявить актуальные уязвимости в сетевом периметре и приложениях, проверить работу имеющихся средств защиты, а также проверить и подготовить приложения к условиям высоких нагрузок.

Нашим продуктам доверяют

2GIS

Miran data-center

РоссельхозБанк

Почта Банк

DATALINE

okko

РБК

tutu

окб

Об угрозах для сетей и ИТ-инфраструктуры

Большинство сетевых атак сегодня успешно выводят из строя ИТ-системы компаний вне зависимости от часового пояса злоумышленника и типа атакуемой цели. Ситуация осложняется тем, что методы атакующих постоянно совершенствуются, из-за чего бизнес все чаще сталкивается не только с типовыми и автоматизированными атаками, но и со сложными интеллектуальными, а также с 0-day угрозами, против которых бессильны даже самые авторитетные ИБ-разработки.

DDoS-атаки на сетевую инфраструктуру (L3-L4)

Ежегодно одними из самых злободневных угроз для бизнеса в мировом киберпространстве становятся DDoS (Distributed Denial of Service) – распределенные атаки типа «отказ в обслуживании». В 2022 году ситуация сильно усугубилась для российских компаний, которые испытали на себе организуемые «кибердружинами» многовекторные DDoS-атаки, достигающие в объеме сотен гигабит вредоносного трафика.

Организуя DDoS-атаку, злоумышленники используют множество подконтрольных ему зараженных устройств и скомпрометированных компьютерных систем, обычно распределенных по географическому признаку. На этих мощностях генерируется огромное количество искусственных автоматизированных запросов, которые обрушивают целевую систему, исчерпывая лимит пропускной способности каналов связи и/или производительности сетевого оборудования.

- Лучшей аналогией атаки на каналы связи является автомобильная пробка, созданная умышленно с использованием нескольких транспортных средств.
- DDoS на сетевое оборудование можно сравнить с обслуживанием на кассе в магазине наглого покупателя, который влез без очереди с большой корзиной покупок – в этом случае у кассира физически нет возможности обслужить остальных посетителей, многие из которых просто уходят ни с чем.

К типам DDoS-атак на сетевой и транспортный уровни ИТ-инфраструктуры (L3-L4) относятся:

- UDP floods
- NTP amplification
- DNS amplification
- SYN flood
- Memcache amplification
- CharGEN amplification
- SSDP amplification
- SNMP amplification
- GRE-IP flood
- CLDAP amplification
- IP-Fragment attack
- Jenkins amplification
- TCP RST flood
- TCP ACK flood
- TCP connect flood
- ARMS (ARD) amplification

Используемые сегодня средства защиты от DDoS неплохо справляются со своей задачей, когда дело касается типовых автоматизированных угроз. Однако они пока несовершенны в отношении целевых интеллектуальных и 0-day атак из-за ограниченных наборов правил фильтрации и неспособности сдерживать сразу большое количество активных контрмер. При объемных или прикладных атаках эти инструменты неизбежно теряют в производительности, пропуская вредоносные запросы и блокируя легитимный трафик. Иными словами, будучи пригодными лишь для грубой очистки трафика, они способны противостоять лишь 50% DDoS-атак.

Привычные способы защиты от DDoS атак

1.Защита от DDoS на стороне Cloud и ISP провайдеров

Предоставляя услуги связи, облачные провайдеры и телеком-операторы не обеспечивают защиту от сетевых атак по умолчанию. Атаки на отдельных клиентов могут затрагивать сразу многих, поскольку за одним каналом связи могут находиться ресурсы сразу несколько компаний. Для провайдера становится невыгодно иметь дело с проблемными клиентами. Ему легче прекратить отношения с ними, чем выплачивать штрафы по SLA всем остальным и выделять значительные бюджеты на организацию защиты от сетевых угроз.

Тем не менее все больше провайдеров предоставляют различного рода услуги защиты, часто утверждая, что они могут справиться с атаками не только сетевого, но и прикладного уровня.

1. Подключение протокола BGP FlowSpec

Провайдеры и операторы связи способны снижать вредоносное воздействие сетевых DDoS-атак на клиентов, задействуя BGP FlowSpec – дополнительный протокол маршрутизации трафика на сетевом оборудовании. BGP FlowSpec поддерживает управление правилами фильтрации, которые позволяют или полностью отсечь пакеты определенного типа, присущие DDoS-атаке, или ограничить их прохождение по полосе (rate-limit).

Для применения этого метода защиты необходима глубокая экспертиза в сетевой безопасности, а также специализированное оборудование или ПО с поддержкой BGP FlowSpec.

Основными недостатками метода являются ограниченность функционала правил фильтрации, из-за которых реализуются достаточно грубые алгоритмы блокировки, следовательно, повышается вероятность блокировок легитимного трафика и реальных пользователей.

2. Динамическая маршрутизация Remote Triggered Black Hole

Объем DDoS может достигать 1ТБ в секунду и выше. С такими атаками не всегда справляются даже магистральные провайдеры. Направленный, как правило, на одного из клиентов, паразитный трафик забивает всю емкость канала на отдельном участке сети, за которым обычно находятся сразу несколько клиентов.

Провайдеры в данном случае могут пойти на крайнюю меру – полностью изолировать IP-адреса получателей и направить абсолютно весь поступающий к ним трафик по несуществующему маршруту. В результате атакованные адреса теряют доступность в том числе и для реальных пользователей.

3. Маршрутизация трафика по принципу Reroute

Представляет из себя защиту «по запросу». После начала DDoS-атаки в стандартный маршрут трафика «оператор-клиент» добавляется поставщик комплекса фильтрации, на стороне которого блокируется вредоносный трафик.

Первым существенным недостатком этого метода является фактическая задержка начала фильтрации за счет времени обновления таблиц маршрутизации BGP, которая занимает от 30 секунд до 15 минут. Пока происходит активация схемы reroute, пользователи не имеют доступа к атакуемому ресурсу, что уже делает атаку успешной.

Второй значительный минус – строгое ограничение по объему атаки, лимитированное возможностями каналов между оператором связи и комплексом фильтрации. При объемных атаках все сервисы, защищаемые по схеме reroute, становятся недоступны, поскольку фильтрация ограничивается пропускной способностью связующего канала (обычно до 100 Gbps).

1.4. Эксплуатация комплекса(ов) очистки сторонних производителей

Провайдеры могут заранее защитить свою сетевую инфраструктуру, установив решения по защите от DDoS-атак от сторонних поставщиков.

Однако большинство провайдеров обходятся единственным узлом фильтрации, расположенным в определенной локации, что кратно увеличивает время обработки пакета и создает единую точку отказа.

Для оптимальной маршрутизации безопасного трафика необходима децентрализованная географически распределенная сеть из нескольких центров очистки. Узлы фильтрации должны быть зарезервированы на случай ЧС. В противном случае пожар в дата-центре, отключение всех лучей питания или повреждение магистральной сети могут вывести из строя всю систему защиты.

2. On Premise – ПАК и/или ПО

Несмотря на заявленную эффективность, существующие решения, встраиваемые/устанавливаемые локально на инфраструктуре заказчика, имеют ряд недостатков:

Во-первых, в процесс внедрения программно-аппаратных комплексов закладывается время на поставку, установку и обучение сотрудников, которого явно нет у компании, находящейся под атакой.

Во-вторых, и софт, и ПАК нуждаются в администрировании. Если решение приобретается у дистрибьютора, а не у вендора, помощь с внедрением может оказаться неполноценной, а в процессе эксплуатации многие вопросы заказчика скорее всего останутся без ответа.

1. Решения NETSCOUT Arbor

На протяжении длительного времени компании живут в контексте мультивекторных атак, эксплуатирующих сразу несколько протоколов для эффективного поражения цели.

Решения, основанные на технологиях Arbor, не способны параллельно отрабатывать сразу большое количество атак или атаки большого объема. Все из-за того, что в момент атаки с ростом активных контрмер растет и нагрузка на систему защиты. Встречаясь со сложными современными атаками, такие системы неизбежно теряют производительность и деградируют.

Также из-за скудного количества контрмер и ограничений в количестве активных правил фильтрации отсутствует возможность гибко и тонко настраивать профили защиты. В конечном итоге это приводит к тому, что правила фильтрации влияют на трафик пользователей, вызывая постоянную деградацию сервисов.

Важно учитывать, что чем больше инженеры имеют в распоряжении контрмер и/или правил, тем точнее они смогут настроить профиль защиты, что позволит эффективно бороться даже с мультивекторными атаками.

2. Next Generation Firewall (NGFW)

Защита от DDoS не является профилем решения NGFW. Несмотря на то, что в нем имеются модули фильтрации, в большинстве случаев они крайне нестабильны и непроизводительны. NGFW способен отфильтровать не более 50% популярных DDoS-атак. Ключевое его предназначение – в защите и контроле доступа внутреннего сетевого контура на небольших объемах трафика.

3. Решения с открытым исходным кодом (Open Source)

Бесплатный софт с открытым исходным кодом, опубликованный на популярных репозиториях, не способен отвечать актуальной конъюнктуре и требованиям информационной безопасности. Open Source разработки не тестируются и в основном не используются на сетевых контурах крупных компаний. Более того, разработчики таких решений не несут за них ответственность, поэтому эффективность работы таких решений, как и поставка обновлений, ничем не гарантированы. Для их эксплуатации требуется собственный штат высококвалифицированных разработчиков и инженеров, которые будут дорабатывать

ПО под меняющиеся условия и задачи. В рамках защиты ресурсов одной компании это, как правило, экономически неэффективно.

4. Решения от провайдеров защиты

Линейка продуктов защиты от мультивендорных или мультисервисных провайдеров и дистрибьюторов обычно не строится на их собственных разработках. Для них защита от DDoS не является ключевым профилем. Поэтому реализуемые провайдерами решения кратно страдают по эффективности перед профильными.

Кроме того, провайдеры зачастую не способны организовать действительно качественное внедрение и сопровождение сервисов, а также часто используют устаревшие продукты с ограниченным функционалом.

Для вендора разработка и совершенствование собственных продуктов и технологий, а также моделей их поставки – приоритетная задача.

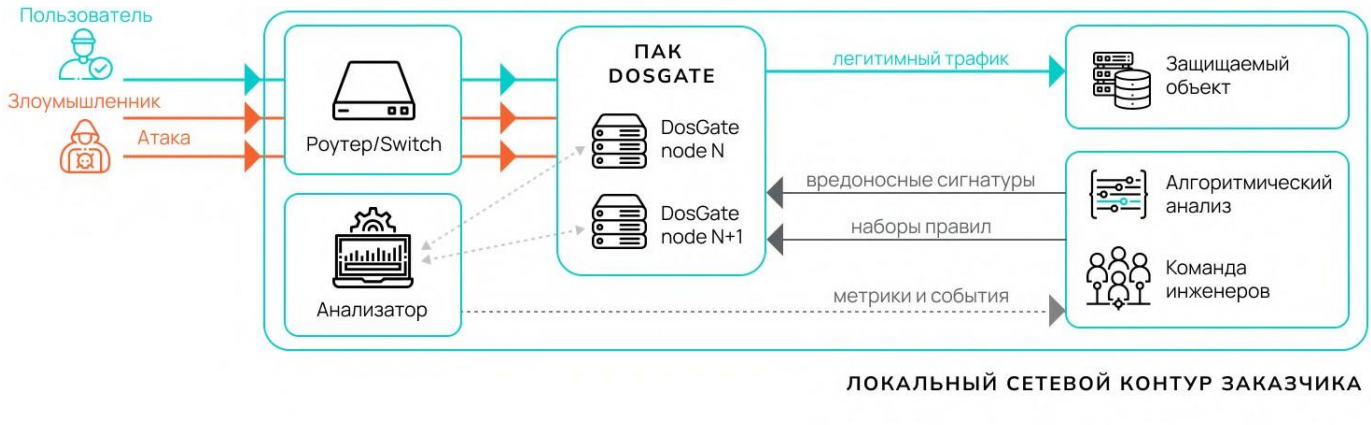
Servicepipe DosGate

При разработке продукта для защиты ИТ-инфраструктуры команда Servicepipe изначально отталкивалась от существующих на рынке решений, таких как NETSCOUT Arbor и «Периметр». Они послужили «референсом» при создании продукта DosGate, который за два года разработки с нуля стал нашим видением эволюции всех существующих на рынке аналогичных решений.

DosGate создавался как in-house-решение для собственных нужд компании. Сегодня продукт защищает сетевую инфраструктуру крупных компаний, в том числе телеком-операторов, дата-центров и финансовых организаций.

DosGate защищает приложения, сервисы, а также сетевой и транспортный уровни сети от переполнения вредоносным трафиком, предотвращая недоступность ресурсов вследствие DDoS-атак. Продукт позволяет оперативно подключать правила фильтрации трафика по схеме IP-транзита и обеспечивать доступность всех ИТ-ресурсов, расположенных за ним, включая каналы связи, сетевое и серверное оборудование. Решение спроектировано для работы в высокопроизводительной инфраструктуре и способно обрабатывать трафик до 400 Гбит/с и 200 млн. пакетов в секунду на серверной платформе в 1 юнит.

Алгоритмический анализ DosGate



DosGate имеет возможность поддерживать одновременную работу большого количества правил фильтрации – до 150 тыс. различных профилей защиты, в рамках каждого из которых можно настроить до 1000 разных правил. Таким образом, вся система способна единовременно удерживать до 150 млн уникальных активных правил в режиме Always-on.

Продукт DosGate отличается высокой производительностью, стабильностью работы, возможностью кластеризации и свободной интеграции, а также уникальным конструктором правил, который позволяет создавать высокоточные контрмеры за считанные минуты. Программно-аппаратные комплексы могут формировать большие кластеры размером в сотни Gbps.

Верификация пакетов и расширенный конструктор правил

Расширенный конструктор позволяет создавать наборы правил, которые поочередно верифицируют каждый отправленный в сторону сервисов клиента пакет, отдельно авторизуя каждого клиента и сервис, к которому он обращается. Это позволяет превентивно отрабатывать свыше 99% даже самых сложных DDoS-атак.

Не теряя в производительности, продукт DosGate способен взаимодействовать с сетевыми пакетами как DPI-система. Это позволяет ИБ-администраторам полноценно работать с конструктором правил и самостоятельно, без ограничений, создавать контрмеры, использование которых невозможно в подобных сторонних решениях без разработки и поставки вендорских обновлений.

Множество сценариев применения

Расширенный конструктор правил предоставляет множество сценариев использования DosGate. Помимо классического сценария – в качестве инструмента защиты от DDoS-атак – также возможно использование:

- в качестве полноценного высокопроизводительного сетевого брандмауэра, глобального файрволла, инструмента защиты магистральной сети или конкретных сервисов от DDoS;
- в качестве дополнительного более мощного узла фильтрации или offload решения для комплексов WAF, анти-бот систем или иных вышестоящих систем очистки;
- в качестве классификатора входящего сетевого трафика.

Широкая поддержка приложений и протоколов

В момент активации DosGate команда инженеров на стороне заказчика получает в распоряжение полноценный набор правил фильтрации, заранее подготовленных под различные цели защиты. Предустановленные наборы правил содержат готовые контрмеры, которые уже реализованы поверх конструктора правил и способны обеспечивать точечную защиту от атак, включая особо организованные нападения политически мотивированных «кибердружин».

Команда собственного R&D центра Servicepipe непрерывно обновляет и совершенствует набор контрмер, интегрируя и поставляя их в режиме конвейерной разработки CI/CD. Ежедневно по всем локальным комплексам очистки заказчиков распространяются автоматические обновления, содержащие в себе новые наборы правил. Модульная архитектура решения позволяет централизованно и без перебоев для сетевого трафика поставлять обновления вредоносных и легитимных сигнатур.

Высокая скорость срабатывания

За счет реализации собственных разработок команда Servicepipe добилась возможности мгновенной активации правил фильтрации в рамках ПО DosGate с момента обнаружения вредоносной сигнатуры в трафике. Это кратно снижает время деградации сервисов клиента до момента активации очистки. У большинства поставщиков активация защиты занимает от 10 секунд до нескольких минут.

Высокая производительность и отказоустойчивость архитектуры

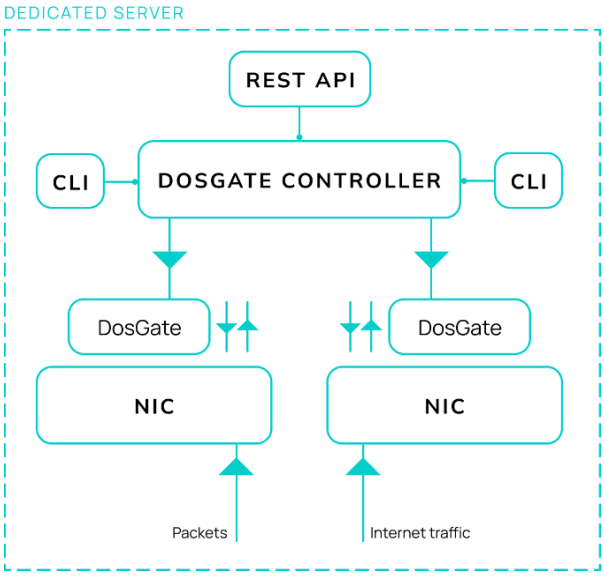
Узлы фильтрации, расположенные в РФ и Европе, имеют общую канальную производительность более 1 Tbps. Большая часть сети очистки, в том числе принимающая на себя клиентский трафик, находится на территории РФ.

Географическое распределение усиливает готовность к атакам любого объема и типа, генерируемым не только из-за рубежа, но также с территории РФ и ближнего зарубежья.

Это гарантирует исключительный уровень доступности инфраструктуры очистки SP DosGate даже при тяжелых распределенных атаках.

Вся сетевая инфраструктура и комплексы очистки полностью резервируются. Дублируются все элементы системы: питание, каналы связи, а также само оборудование, маршрутизаторы и коммутаторы.

Модульная архитектура решения позволяет организовать независимые друг от друга профили защиты с индивидуальной производительностью, что гарантирует отказоустойчивость всей системы.



Простая и свободная интеграция

DosGate свободно подключается к другим решениям через API, легко разворачивается на одном оборудовании параллельно с любыми другими решениями, работает вкупе с известными анализаторами трафика и имеет готовые схемы интеграции в различные сетевые инфраструктуры. Система не резервирует под себя сетевые интерфейсы или процессорные мощности, параллельно назначая себе самый высокий приоритет на случай полноценной загрузки процессора. Это позволяет запускать другие решения на оборудовании, выделенном под комплекс очистки на базе DosGate, включая программы для работы с сетевым трафиком (например, веб-сервера или приложения для балансировки трафика).

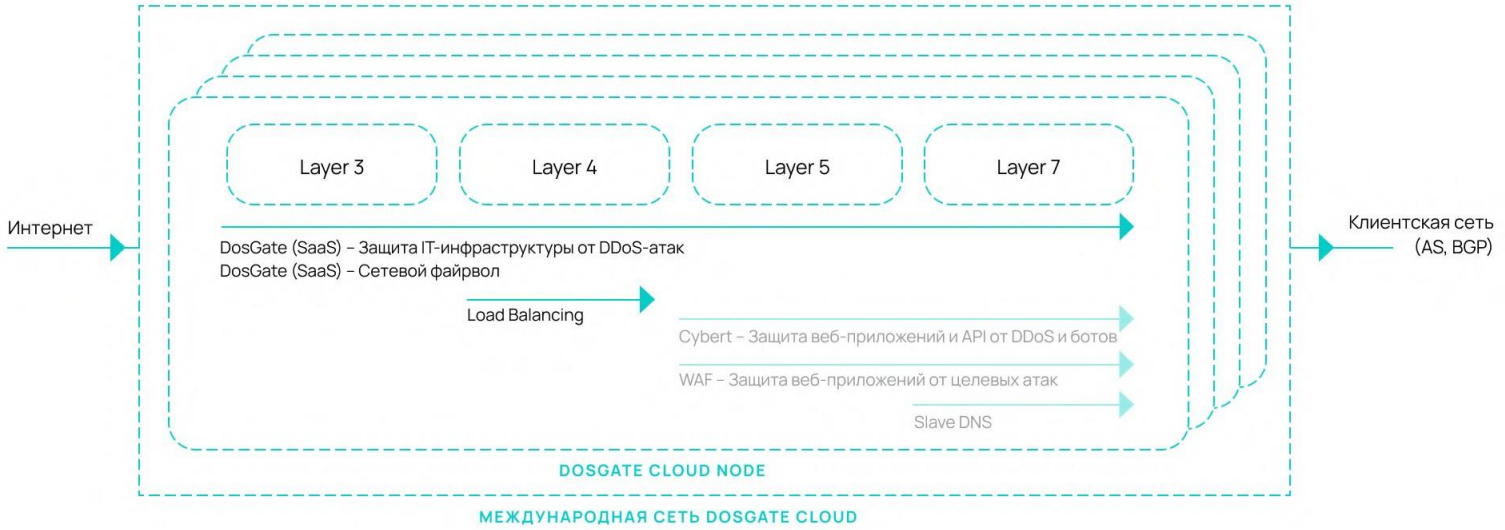
Варианты поставки и внедрения

Реализуя собственные решения и разработки, мы способны реализовать любые форматы их поставки и внедрения:

1. подключение заказчиков к облачному сервису:
   - с использованием общих ресурсов платформы фильтрации Servicepipe
   - организовать изолированные и выделенные ресурсы в рамках платформы фильтрации Servicepipe с возможности самостоятельного управления
2. установка DosGate в инфраструктуре заказчика в формате локального решения:
   - в виде программного обеспечения на оборудование заказчика
   - в виде программно-аппаратного комплекса
3. реализация гибридных схем, сочетающих упомянутые выше модели

Cloud protection

Базовым вариантом приобретения DosGate является подключение к облачной услуге защиты от DDoS-атак. В этом случае Servicepipe выполняет для клиента роль поставщика доступа в Интернет. Для фильтрации DDoS-атак системе требуется только входящий трафик, но по желанию клиент может маршрутизировать трафик симметрично.

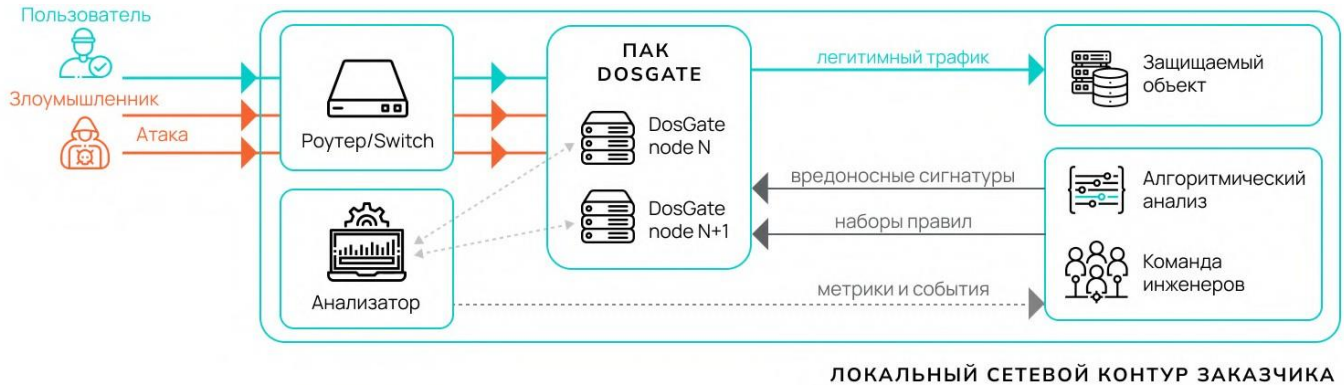


Имея прямую связанность со всеми московскими дата-центрами, Servicepipe способен поместить любой сетевой объект под защиту решения DosGate. С подключением клиенту помогает собственная команда эксплуатации Servicepipe. Все это позволяет в кратчайшие сроки организовать прямой стык с комплексом фильтрации – даже в момент атаки и недоступности сервисов заказчика.

Software/Hardware node

Решение DosGate передается в виде ПАК ПО и интегрируется в его инфраструктуру. Инсталляция и первичная настройка профилей осуществляется инженерами Servicepipe. Дальнейшее обслуживание осуществляется инженерами заказчика.

По запросу клиента доступна расширенная поддержка. В этом случае заказчик пользуется услугами Servicepipe SOC (“Service Operations Center”) – центра по реагированию и защите от DDoS-атак. Квалифицированные ИБ-инженеры контролируют оборудование, сетевой контур заказчика, управляют комплексом очистки в случае атак, обновляют вредоносные сигнатуры, реализуют меры по защите сервисов и приложений в сети заказчика.



Производительность - 400 Gbps/200 Mpps на 1U-сервер (HPE DL360 GEN10, Intel Xeon 8255C x2, 192GB RAM, MCX516A-CCAT x2)

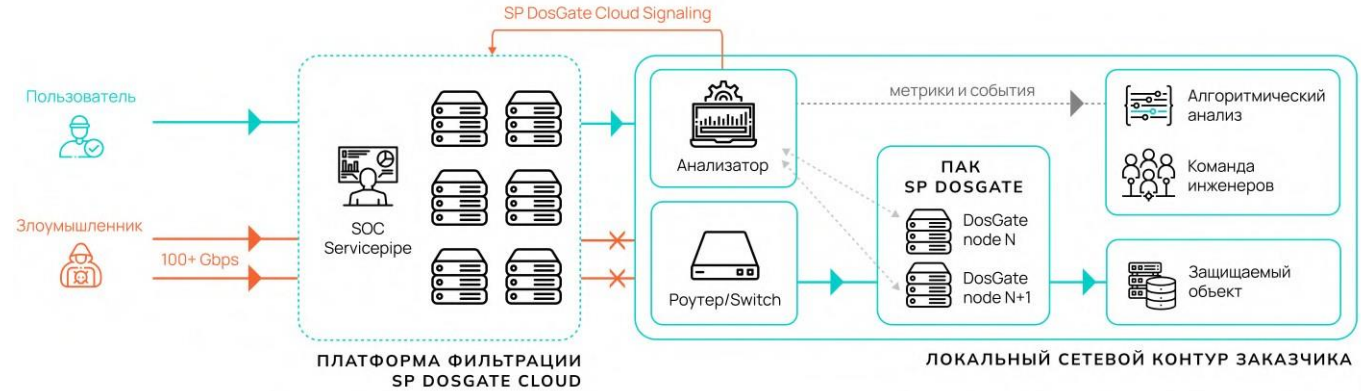
Hybrid protection

По запросу клиента команда Servicepipe способна реализовать гибридную инсталляцию решения - локальную инсталляцию DosGate в инфраструктуре клиента с подключением фильтрации на уровне защищенного канала Servicepipe.

Узлы фильтрации синхронизируются между собой и работают как единая многослойная система. Любое изменение профиля защиты в рамках ПО заказчика может автоматически распространяться на защищенный канал Servicepipe, который страхует заказчика на случай, если локальный комплекс очистки не справится с атакой. Защищенный канал автоматически активирует очистку на своей стороне в случае облачной сигнализации от ПО DosGate в локальной сети заказчика.

Схема работы гибридной модели защиты при атаке небольшой мощности

Схема работы гибридной модели защиты DosGate при объемной атаке



Дополнительные возможности с Servicepipe:

1. Сопровождение решения в сети заказчика в рамках расширенной поддержки по запросу:

- после внедрения специалисты Servicepipe могут осуществлять техническое сопровождение, включающее полную настройку и администрирование решения внутри локального сетевого контура заказчика;

- защита от DDoS-атак в формате мониторинга и реагирования силами команды инженеров Servicepipe (SOC);

2. Технологическое сотрудничество в формате интеграции продукта Servicepipe или его модулей в сторонние программные решения или программно-аппаратные комплексы;

Также заказчику/партнеру доступны:

1. Дополнительные сценарии использования DosGate, возможные благодаря расширенному конструктору правил:

- в качестве полноценного высокопроизводительного сетевого брандмауэра, глобального фаервола, инструмента защиты магистральной сети или конкретных сервисов;

- в качестве дополнительного более мощного узла фильтрации, а также offload-решения комплексов WAF, анти-бот систем или иных вышестоящих систем очистки;

- в качестве классификатора входящего сетевого трафика;

2. Удобное управление и настройка DosGate через CLI

3. Поддержка любого user-space приложения на том же оборудовании;

4. Прямая интеграция с Arbor Peakflow, FastNetMon для обнаружения атак плагином collectd;

5. Интеграция с любыми комплексами WAF, антибот-системами (включая решение Servicepipe Cybert для защиты веб-ресурсов и API), а также другими системами очистки для увеличения их производительности.

Преимущества DosGate

- Собственная разработка с гибкими возможностями интеграции локально, в формате подключения к облачному сервису SaaS или гибридной инсталляции;
- Комплексная защита всех сервисов, использующих любые протоколы (TCP, UDP, SMTP, FTP, SSH, VoIP и другие) от автоматизированных угроз на транспортном уровне;
- Минимальный процент ложноположительных срабатываний и высокоточная фильтрация без блокировки реальных пользователей за счет расширенного конструктора правил;
- Возможность быстрой организации прямого стыка с любым объектом в Москве и в регионах;
- Множество сценариев использования – от DDoS-защиты и интеграции со сторонними решениями до глобального Firewall для большой корпоративной сети;
- Always-on и on demand режимы, способные параллельно поддерживать до 150 млн активных правил фильтрации на 150 тыс. профилях защиты;
- Поддержка облачной сигнализации (Cloud Signaling) для интеграции с локальными средствами защиты, включая поддержку решений сторонних производителей;
- Отказоустойчивость и высокая производительность облачной инфраструктуры SP за счет георасределенной модели резервирования сети, каналов связи и узлов фильтрации;
- Высокая производительность решения DosGate, обусловленная модульной архитектурой и собственным ядром обработки трафика;
- Индивидуальная адаптация правил реагирования под профиль сетевого трафика, сервисы и задачи каждого заказчика;
- Техническая поддержка 24/7/365 в рамках собственного центра реагирования (SOC);
- Собственная обновляемая база вредоносных сигнатур и распространение правил фильтрации на всех клиентов из схожих или смежных сегментов бизнеса.