servicepipe
высокоточная защита
от кибератак

Обзор продуктов **Servicepipe**

SP DosGate и SP Cybert.

NETWELL

Предоставляем эшелонированную защиту на базе партнёрских технологий вендора **SP DosGate и SP Cybert.**.

servicepipe
высокоточная защита
от кибератак

Преимущества решений по информационной безопасности:

01. Сильная команда профессиональных экспертов

- 80+ ИБ-экспертов, включая специалистов highload и bigdata.
- Эксперты входят в рабочую группу противодействия атакам при Минцифре.

02. Эшелонированный подход к защите

1. On - premises компоненты:

- Очиститель SP DosGate на площадке клиента для высокоточной защиты DDoS-атак на сетевом и транспортном уровнях L3/L4 (ПАК).
- Анализатор SP FlowCollector на площадке клиента, который непрерывно отслеживает входящие и исходящие пакеты, гибко реагируя на обнаруженные в них аномалии (ПАК).

3. Гибридные инсталляции, объединяющие On-premises и сервисные модели поставки

2. Облачный/сервисный компоненты:

- Сервис по защите от DDoS-атак на сетевом и транспортном уровнях (L3/L4) с помощью технологии SP DosGate.
- Сервис по защите от DDoS-атак и ботового трафика на веб-приложения и API для прикладного уровня (L7) с помощью технологии SP Cybert с многофакторным анализом трафика и позапросной фильтрацией.
- Сервис по защите от целевых атак и эксплуатации уязвимостей веб-приложений и API за счет межсетевого экрана Web Application Firewall.

Преимущества решений по информационной безопасности

03. Уникальные продукты, технологии и инфраструктура

- Геораспределенная отказоустойчивая платформа фильтрации, узлы очистки трафика в РФ и Германии.
- Постоянное совершенствование технологий.

04. Высокоточная защита

- Зачастую, грубые, типовые алгоритмы очистки и фильтрации ограничивают доступ легитимных пользователей к данным. Многоступенчатые, адаптивные алгоритмы наших решений предоставляют высочайшую точность очистки и гранулярность данных.
- Совокупность этих мер обеспечивает доступность информации и критически важных бизнес-сервисов для ваших пользователей

05. PCI DSS Compliance

- Возможность защиты без раскрытия SSL-сертификатов и передачи логов с веб-сервера.

06. Отечественное ПО

- SP Cybert, SP DosGate зарегистрирован в реестре Отечественного ПО. Реестровая запись №15575 от 18.11.2022

07. Оперативная техподдержка 24/7/365

- Лучшая в классе техническая поддержка.
- Десятки сертифицированных специалистов с богатым опытом работы в ведущих международных компаниях – лидерах рынка

Защита ИТ-инфраструктуры

ON-PREMISES

NETWELL

On-premises защита ИТ-инфраструктуры

Реализуем комплекс партнёрских решений по очистке трафика и защите ИТ-инфраструктуры от автоматизированных угроз с помощью вендорских технологий **SP DosGate и SP FlowCollector**.

Предлагаем линейку on-premises решений для защиты от DDoS-атак и киберугроз на базе технологии SP DosGate:

01. ПАК SP DosGate

Поставляется в виде решения под ключ и устанавливается на инфраструктуре клиента.

02. SP FlowCollector

Очиститель трафика SP DosGate может поставляться вместе с интеллектуальным анализатором сетевого трафика SP FlowCollector, который непрерывно отслеживает входящие и исходящие пакеты, гибко реагируя на обнаруженные в них аномалии.

On-premises SP DosGate – ваш высокопроизводительный инструмент для максимальной защиты от DDoS- атак и киберугроз.

03. SP dlDosGate

(distribution layer DosGate)

Продукт защиты от DDoS-атак для конечных устройств. SP dlDosGate работает на уровне ядра Linux, сбрасывая вредоносные сессии и пакеты. Очищенный трафик направляется в операционную систему и к другим приложениям конечного устройства, на котором он установлен.

On-Prem защита ИТ-инфраструктуры

01. SP DosGate

NETWELL

On-premises защита ИТ-инфраструктуры SP DosGate

1. Суть технологии SP DosGate
2. Особенности ПАК SP DosGate
3. Преимущества ПАК SP DosGate по сравнению с облачной защитой
4. Другие преимущества SP DosGate
5. Реализованные кейсы

Суть технологии SP DosGate

Технология комплексной защиты ИТ-инфраструктуры от сетевых атак на L3/L4. Обеспечит безопасность сетевого периметра и защиту от DDoS-атак с первой минуты, не требуя настройки многочисленных сервисов и сетевых инфраструктур.

50+ компаний уже используют SP DosGate для защиты от DDoS-атак и обеспечения безопасности своего сетевого периметра.

Поставляется как ПО/ПАК с веб-интерфейсом и уникальной базой вредоносных сигнатур.

Преимущества технологии SP DosGate:

- Технология в **реестре российского ПО.**
- Архитектор правил фильтрации с **глубокой настройкой** алгоритмов очистки на лету из веб-интерфейса.
- **50+ пресетов,** доступных «из коробки».
- Определение DDoS-атаки за **1 мс** в режиме постоянной фильтрации (Always-on).
- Собственная база вредоносных сигнатур от SP.
- Отражение атак мощностью до **200 Гбит/с** на одной аппаратной платформе.
- Кластеризация вплоть до **10+ Тбит/с.**
- Отражение рекордных атак мощностью **800 Гбит/с и 500 млн пакетов в секунду**.
- Детальная **статистика** по срабатыванию каждого активного правила.
- 100% **автономная** работа в инфраструктуре заказчика.
- Совместимость с любым стандартизированным серверным оборудованием.

Особенности ПАК SP DosGate

Гибкая автономная система защиты IT-инфраструктуры от DDoS-атак на L3–L7. Мгновенно заблокирует DDoS-атаки на почтовые серверы, видеоконференции, IP-телефонию, корпоративные порталы, удалённые рабочие места, другие сервисы и службы, работающие по протоколам TCP, UDP, SMTP, FTP, SSH, VoIP, VPN.

Сценарии использования ПАК SP DosGate

ПАК DosGate устанавливается в контуре.
Вредоносный трафик блокируется, легитимный — передаётся на целевые IP-адреса.

Возможно несколько сценариев использования:

- Защита от DDoS
- Пакетный и сессионный файрвол (ACL)
- Защита промежуточных узлов от сессионных атак (МСЭ, WAF, балансировщиков нагрузки)

Таким образом, **сетевая инфраструктура всегда остаётся защищённой.**

Заказчику не нужно взаимодействовать с несколькими разными операторами связи и их DDoS-защитой на уровне канала, пытаясь сохранить оптимальную сетевую связность и не деградировать из-за плохой точности детекции вредоносного трафика.

Преимущества SP DosGate по сравнению с облачной защитой

01. **Контроль над СЗИ**

Контроль над управлением и владение средствами защиты информации позволяют быть **независимыми от сторонних организаций** и принимать решения исходя из собственных потребностей и рисков, а не стандартных или общих подходов, которые не всегда соответствуют локальным требованиям.

02. **Моментальная реакция на DDoS**

В случае возникновения угроз вы можете **незамедлительно применить меры** защиты своей сети, не ожидая обновлений или действий со стороны подрядчика. При использовании установленного в контуре сети DosGate, время реагирования на DDoS-атаку или аномалию будет минимальным.

03. **Прогнозируемый аптайм и SLA**

Собственная выделенная система защиты позволяет исключить или свести к минимуму использование общих ресурсов на уровне защиты провайдера и **сохранить прогнозируемый SLA**.

04. **Развитие инфраструктуры**

Приобретение бессрочной on-premise лицензии с гарантированной поддержкой позволит определить и **упростить процесс бюджетирования** внутри организации. Кроме упрощения процесса закупки, долгосрочная лицензия позволит зафиксировать стоимость в условиях изменчивого рынка, обеспечив более выгодную сделку.

Преимущества SP DosGate по сравнению с облачной защитой

05. Интеграция с существующими платформами

Кроме повышения экономической эффективности, локальная интеграция SP DosGate обеспечивает более комплексную и **сбалансированную стратегию защиты**, дополняя другие продукты и сервисы информационной безопасности — например, как в случае с прямой интеграцией с WAF или SIEM.

06. Защита от многовекторных DDoS-атак

Использование ПО DosGate в собственной инфраструктуре, позволяет администратору задействовать все его функции, включая возможности сессионного фильтра (stateful). За счет использования всех возможных функций платформы очистки — **точность фильтрации сильно вырастает.**

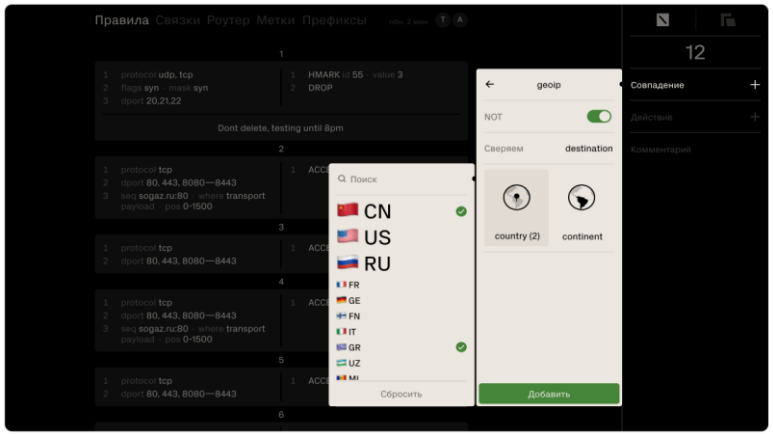
07. Эшелонированная защита

Эшелонированная защита позволяет **увеличить собственную производительность** центра очистки в сети заказчика с помощью облака Servicepipe.

Если вредоносный трафик переполняет каналы связи или центр очистки, система **автоматически** с помощью BGP начинает маршрутизацию входящего трафика через центры очистки Servicepipe расположенные по всему миру, а также синхронизирует политики фильтрации с локальной платформы на облачную.

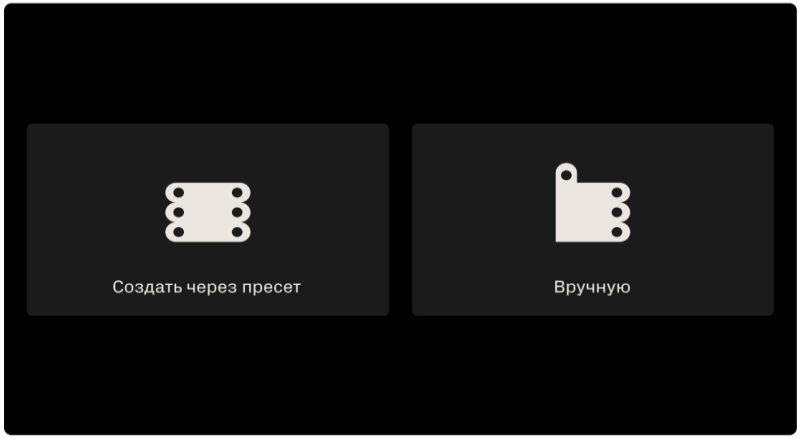
Преимущества SP DosGate

Защита от всех типов DDoS-атак



SP DosGate предоставляет гибкий и функциональный инструмент защиты сетевых ресурсов от многовекторных DDoS-атак **L3–L7, включая VPN, веб-серверы и другие элементы сети.**

Несколько режимов управления

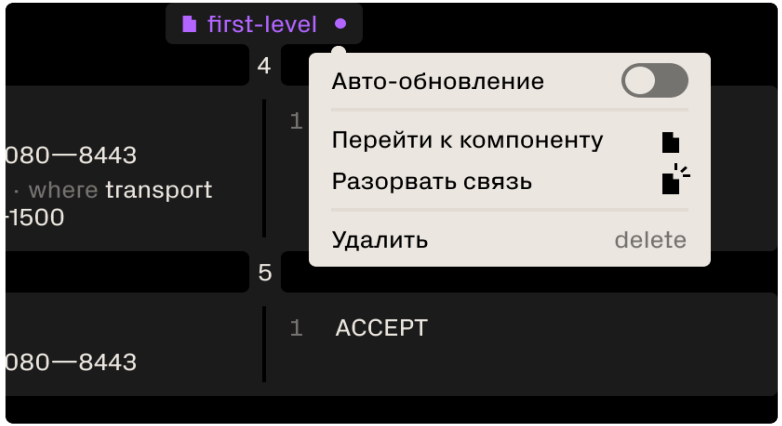


В экспертном режиме администратор системы может **самостоятельно реализовывать собственные контрмеры** прямо из веб-интерфейса без написания программного кода.

В продвинутом режиме для защиты сервисов и сетевых сегментов применяются пресеты.

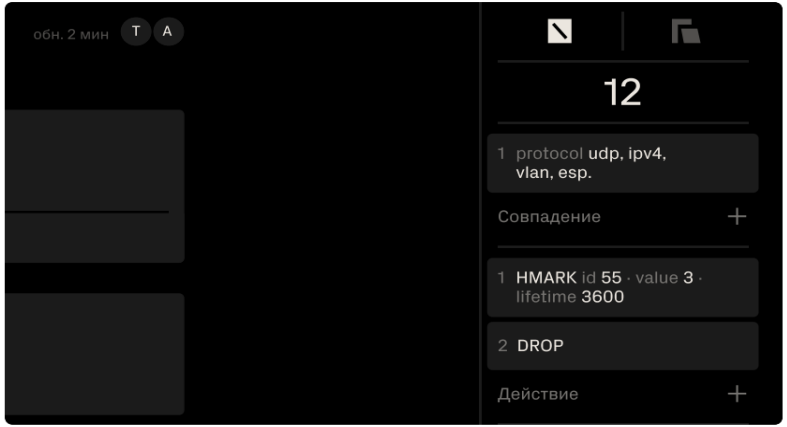
Преимущества SP DosGate

Система компонентов



С помощью системы компонентов можно моментально **вносить изменения в большое количество выбранных профилей защиты** (например, в 50 из 100). Это существенно ускоряет управление высоконагруженными платформами.

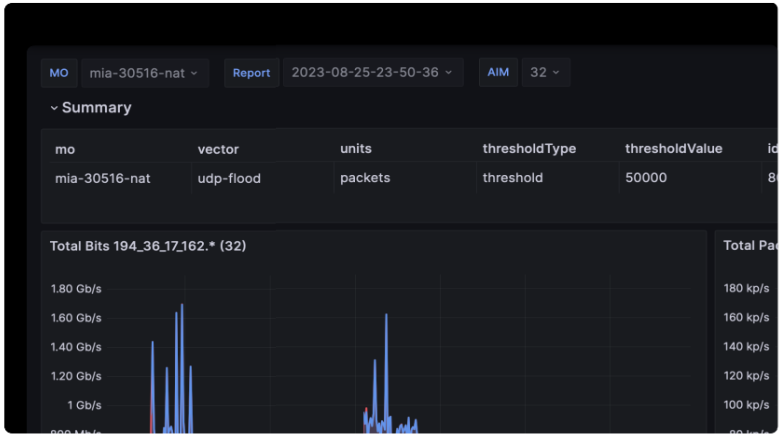
Stateless+Stateful



SP DosGate работает одновременно с сетевыми пакетами и сессиями. Это позволяет эффективно защищать не только конечные устройства и сервисы, но и промежуточные узлы, уязвимые к сессионным атакам (например, межсетевые экраны или WAF).

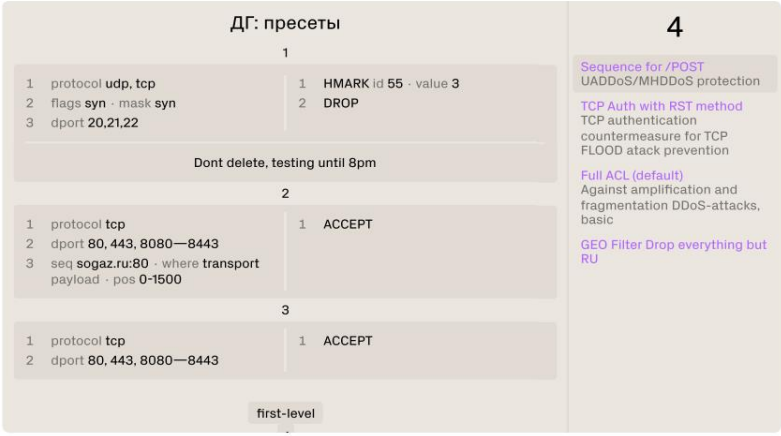
Преимущества SP DosGate

Единая платформа детекции и аналитики



SP FlowCollector в комплекте с SP DosGate позволяет детектировать сетевые аномалии, составлять отчёты и управлять маршрутизацией трафика внутри сети. Он также поддерживает механизмы Cloud Signaling (эшелонированной защиты).

База вредоносных сигнатур



Вместе с IP-списками и TLS-отпечатками распространяются **“пресеты”** (эволюционирующие правила) для plug & play защиты сетей и сервисов. Пресеты поддерживаются командой SP и обновляются каждый час.

Реализованные кейсы

Крупный медиахолдинг

- Кластер 12 платформ 1200 GBps
- Система детекции сетевых аномалий FlowCollector

Межфилиальная защита

- Установка очистителя на уровне ядра сети

Банк топ-10 в РФ

- Плановый поиск поставщика на замену ушедшему Arbor
- Установка DosGate в разрыв с bypass сетевой картой
- Успешно пройдены функциональные тестирования
- Заложен бюджет на 2 ПАК x 10GB
- Реализована мультивендорная эшелонированная защита «Servicepipe + Конкурент»

Оператор почтовых отправлений

- Оперативная поставка ПАК
- 2 ПАК x 20GB
- Оперативная настройка и включение специалистами вендора
- Закупка через 5 месяцев

On-Prem защита ИТ-инфраструктуры

02. SP Flow Collector

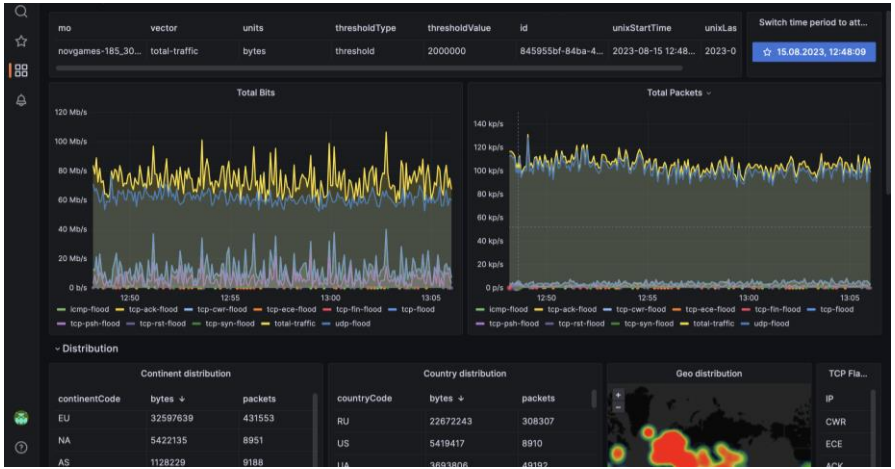
NETWELL

SP FlowCollector (анализатор трафика)

Технология интеллектуального анализа трафика. Проанализирует всё до конечного IP-адреса в подсети, за 100 мс обнаружит и переведёт DDoS-атаку на фильтрацию. Работает как в связке с DosGate, так и с любым другим очистителем. Формирует детальные отчёты по сетевым аномалиям, расширяя возможности аналитики.

02. SP FlowCollector

Технология непрерывно отслеживает входящие и исходящие из сети пакеты и гибко реагирует на обнаруженные в них аномальные всплески сетевой активности, включая DDoS-атаки.



Преимущества SP FlowCollector:

- Позволяет **отсортировать** вредоносный трафик, даже если количество легитимного стремительно растет.
- Анализирует более **25 различных векторов** атак из порогов, заведенных автоматизированно или вручную (TCP SYN, DNS Flood и другие).
- Обрабатывает до **250 000 Netflow** в секунду на одну платформу.
- Детектирует как ковровые, так и точечные DDoS-атаки.
- **Обогащает системы киберразведки** и инструменты мониторинга SOC информацией об источниках атак.
- **Совместим** с любым очистителем трафика.

On-Prem защита ИТ-инфраструктуры

03. SP dlDosGate

NETWELL

SP dlDosGate (distribution layer DosGate)

Продукт защиты от DDoS-атак для конечных устройств. На сегодняшний день SP dlDosGate — это самый простой, быстрый и доступный на рынке вариант on-prem защиты от DDoS-атак на L3-L7.

03. SP dlDosGate

Работает на уровне ядра Linux, сбрасывая вредоносные сессии и пакеты. Очищенный трафик направляется в операционную систему и к другим приложениям конечного устройства, на котором он установлен. Таким образом, нелегитимный трафик сбросится еще до того, как, например, попадет на WAF, NGFW, балансировщик, веб-сервер или любое другое приложение конечного устройства.

Преимущества SP dlDosGate:

- **Уникальность**. Конкурентные решения устанавливаются как промежуточный узел инфры. Их нельзя установить как "конечный узел". А dlDosGate — можно.
- **Простота**. dlDosGate легко устанавливается в ОС и настраивается без необходимости перекраивать текущую сетевую инфраструктуру.
- **Доступность**. Стоимость лицензии dlDosGate на порядок дешевле аналогичной лицензии DosGate on-premises.

Для кого подходит:

- **Для растущих компаний**, которых волнует сетевая безопасность, но пока нет возможности купить и самостоятельно настраивать полноценные ПО/ПАК.
- Для тех, **у кого в контуре уже есть WAF или веб-сервера** нуждающиеся в защите от DDoS-атак как конечные устройства.
- Для тех, **кто работает с ВМ в облаке**, т.к. SP dlDosGate можно разместить на каждой ВМ и получить своё управляемое средство защиты от DDoS.

Коммерческие вопросы:
Геннадий Соколов
gsokolov@netwell.ru
+7.985.279.99.38

Технические вопросы:
Максим Бузмаков
mbuzmakov@netwell.ru
+7.909.664.23.68

NETWELL