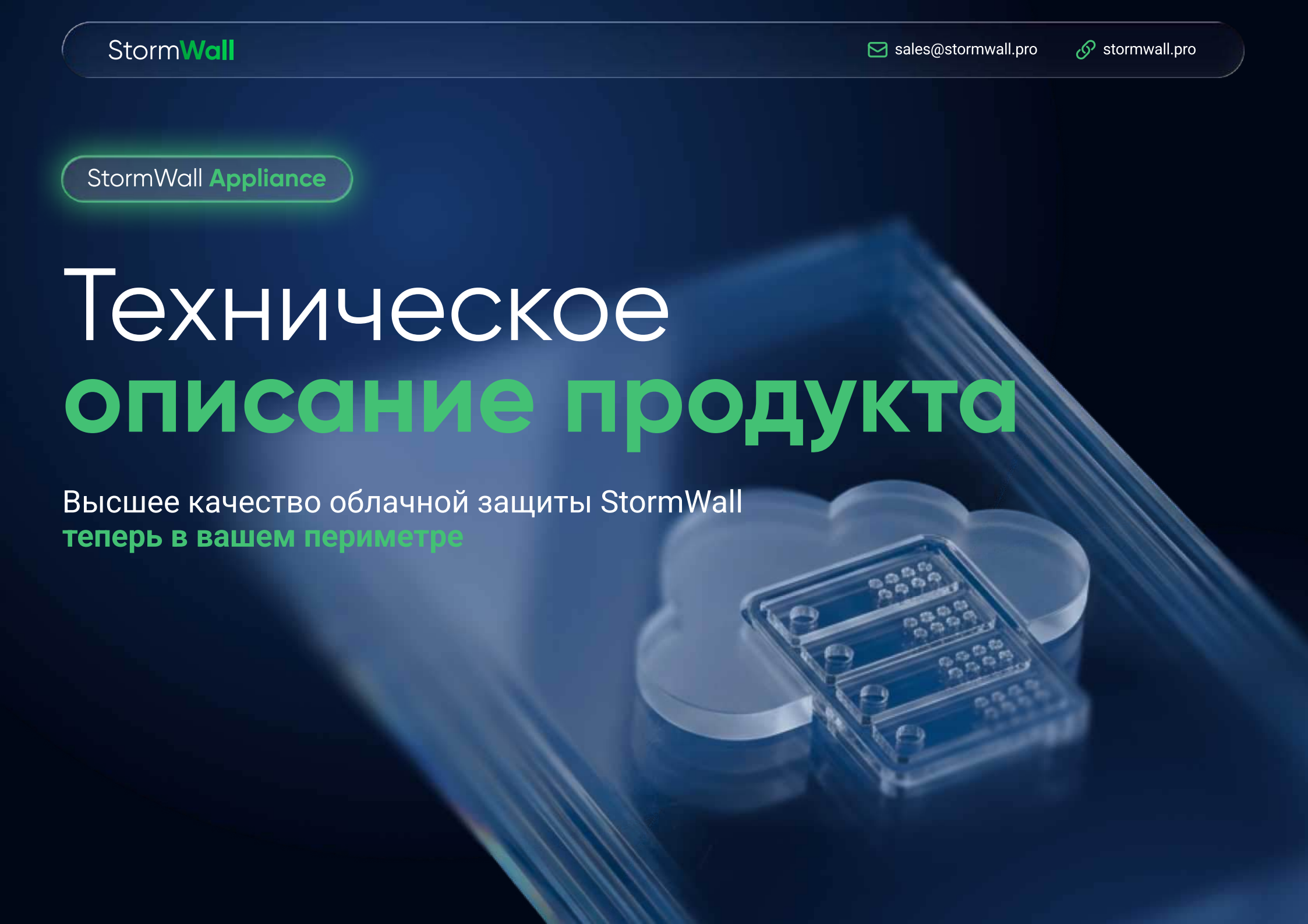
StormWall **Appliance**

Техническое **описание продукта**

Высшее качество облачной защиты StormWall
теперь в вашем периметре



StormWall Appliance

Защита от DDoS-атак на уровнях L3–L5 OSI в инфраструктуре заказчика

1. Общие сведения

Операторы связи, облачные провайдеры и предприятия сталкиваются с общей проблемой: DDoS-атаки — главный риск для доступности сервисов, а их мощность, сложность и частота продолжают расти. Тактики злоумышленников эволюционируют: ботнеты из IoT-устройств, готовые DDoS-инструменты и арендованные стрессер-сервисы сделали атаки дешёвыми и массовыми, а традиционные средства — сигнатурные IPS и простое ограничение скорости — перестали справляться. Нужна защита, которая отделяет атакующий трафик от легитимного, не прерывая работу бизнес-сервисов, — эффективная, экономичная и простая в управлении.

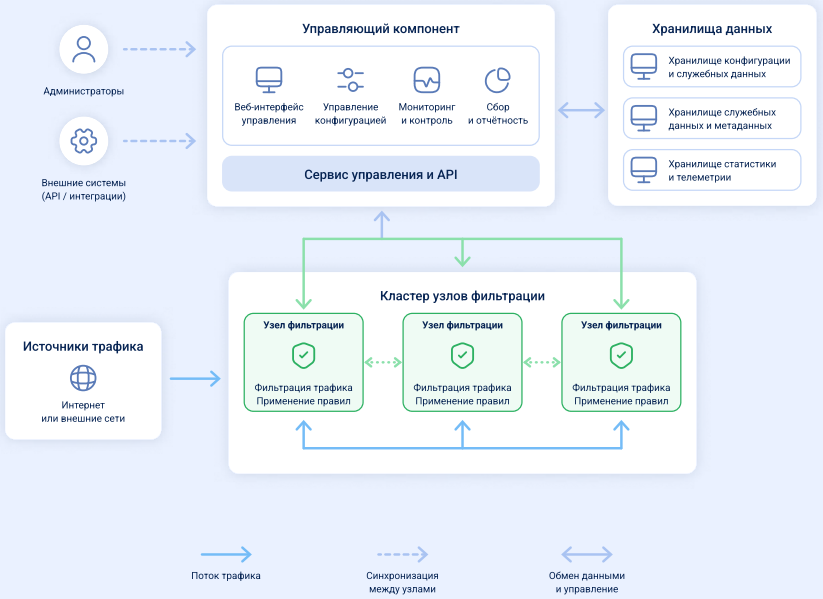
StormWall Appliance — программное решение для защиты сетевой инфраструктуры и сервисов от DDoS-атак на уровнях L3–L5 модели OSI. Продукт разворачивается в инфраструктуре заказчика и обеспечивает локальную обработку и фильтрацию трафика. Решение поставляется в виде программного обеспечения и не требует специализированной аппаратной платформы.

Архитектура решения StormWall Appliance состоит из двух основных компонентов:

- **Firewall Appliance** — управляющий компонент, включающий web-интерфейс, backend-сервисы и подсистему управления (Management). Обеспечивает централизованное управление системой, настройку политик фильтрации, сбор статистики и мониторинг состояния узлов фильтрации.
- **Узлы фильтрации (Filtering Nodes)** — серверы, выполняющие анализ и фильтрацию пользовательского трафика в режиме реального времени. Узлы работают параллельно в конфигурации Active-Active, обеспечивая горизонтальное масштабирование производительности и отказоустойчивость системы. Синхронизация служебного состояния между узлами осуществляется напрямую и не зависит от управляющего компонента.

Ключевые преимущества

- Защита от широкого спектра DDoS-атак. Многоуровневая система фильтрации обеспечивает защиту от атак на уровнях L3–L5 модели OSI, включая TCP-, UDP — и протоколо-ориентированные атаки, с применением попакетного анализа и анализа TLS ClientHello без расшифровки трафика.
- Развёртывание в инфраструктуре заказчика. Решение обрабатывает и фильтрует трафик локально, что позволяет соблюдать требования по размещению данных, информационной безопасности и отраслевого регулирования.
- Программная архитектура без привязки к оборудованию. Продукт поставляется в виде программного обеспечения и поддерживает развёртывание на физических серверах и в виртуальной инфраструктуре, соответствующих системным требованиям.
- Горизонтальное масштабирование. Архитектура Active-Active позволяет увеличивать производительность системы путём добавления узлов фильтрации без изменения логики работы сервиса. Высокопроизводительная обработка пакетов на базе DPDK обеспечивает эффективное использование вычислительных ресурсов.
- Высокая отказоустойчивость. Все узлы фильтрации одновременно участвуют в обработке трафика. При отказе одного из узлов трафик автоматически перераспределяется между оставшимися, а при недоступности управляющего компонента фильтрация продолжается с использованием ранее загруженной конфигурации.
- Централизованное управление. Единый интерфейс управления обеспечивает настройку политик защиты, мониторинг состояния системы и доступ к статистике, а также централизованное управление всеми узлами фильтрации.



2. Архитектура и компоненты StormWall Appliance

Firewall Appliance

Firewall Appliance — управляющий компонент системы, обеспечивающий централизованное управление узлами фильтрации, настройку политик защиты, мониторинг состояния системы и сбор статистики.

Основные функции:

- централизованное управление конфигурацией;
- распространение политик и правил фильтрации;
- мониторинг состояния узлов фильтрации;
- сбор, хранение и визуализация статистики;
- предоставление интерфейса администрирования и API для управления системой.

Для хранения данных используются:

- **PostgreSQL** и **MySQL** — хранение конфигурации и служебных данных;
- **ClickHouse** — хранение статистики и телеметрии.

Узлы фильтрации (Filtering Nodes)

Узлы фильтрации выполняют обработку и фильтрацию пользовательского трафика в режиме реального времени.

Основные функции:

- анализ и фильтрация сетевого трафика;
- применение политик защиты;
- обнаружение и блокирование вредоносного трафика;
- обмен служебной информацией между узлами кластера.

Обработка пакетов реализована с использованием DPDK, что обеспечивает высокую производительность обработки трафика и минимальные задержки. Каждый экземпляр узла фильтрации использует отдельный процессорный сокет, а вычислительная нагрузка распределяется между ядрами процессора.

Отказоустойчивость

Узлы фильтрации работают в конфигурации Active-Active, одновременно участвуя в обработке пользовательского трафика.

Синхронизация внутреннего состояния между узлами фильтрации выполняется напрямую и не зависит от управляющего компонента. При недоступности Firewall Appliance обработка и фильтрация трафика продолжаются с использованием ранее загруженной конфигурации. При этом становятся недоступны функции централизованного управления, изменения конфигурации и просмотра статистики.

Масштабирование

Решение поддерживает различные варианты развёртывания:

- размещение управляющего компонента и узлов фильтрации на одном физическом сервере;
- раздельное размещение компонентов на отдельных серверах;
- развёртывание в виртуальной инфраструктуре;
- географически распределённую архитектуру.

На одном физическом сервере может быть запущено несколько экземпляров узлов фильтрации. При увеличении их количества возрастают требования преимущественно к управляющему серверу — объёму оперативной памяти и дисковой подсистеме, используемой для хранения статистики в **ClickHouse.**

3. Варианты развёртывания

Архитектура StormWall Appliance поддерживает различные варианты развёртывания в зависимости от требований к производительности, отказоустойчивости и доступной вычислительной инфраструктуре. Управляющий компонент и узлы фильтрации могут размещаться на одном физическом сервере, на отдельных серверах или в виртуальной среде, включая географически распределённые инсталляции.

3.1. Принципы распределения **вычислительных ресурсов**

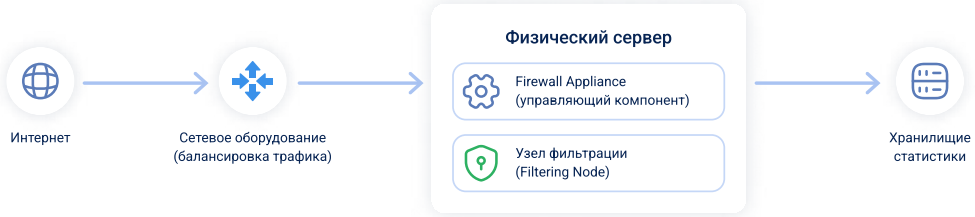
- **Один экземпляр узла фильтрации — один физический процессор.** Для обеспечения максимальной производительности каждому экземпляру узла фильтрации выделяется отдельный физический процессор. Обработка трафика распределяется между вычислительными ядрами данного процессора.
- **Масштабирование производительности.** На серверах с несколькими процессорами может быть развёрнуто несколько экземпляров узлов фильтрации — по одному на каждый процессор. Количество экземпляров определяется аппаратной конфигурацией сервера и параметрами лицензирования.
- **Гибкое размещение управляющего компонента.** Firewall Appliance не требует выделенного физического процессора и может быть развернут как на одном сервере с узлами фильтрации, так и на отдельном физическом сервере или в виртуальной машине.
- **Масштабирование системы.** При увеличении количества узлов фильтрации возрастают требования преимущественно к серверу Firewall Appliance — к объёму оперативной памяти и дисковой подсистеме, используемой для хранения статистики. Требования к вычислительным ресурсам процессора изменяются незначительно.

3.2. Типовые варианты **развёртывания**

Вариант	Описание
Совмещённое развёртывание	Firewall Appliance и один узел фильтрации размещаются на одном физическом сервере
Многопроцессорный сервер фильтрации	На одном физическом сервере размещается несколько экземпляров узлов фильтрации — по одному на каждый физический процессор. Firewall Appliance может быть развернут на этом же сервере или отдельно
Раздельное развёртывание	Firewall Appliance размещается на отдельном физическом сервере или в виртуальной машине (VMware, KVM, Hyper-V), а узлы фильтрации — на выделенных физических серверах
Географически распределённое развёртывание	Управляющий компонент размещается в центральной точке, а узлы фильтрации — в различных географических локациях

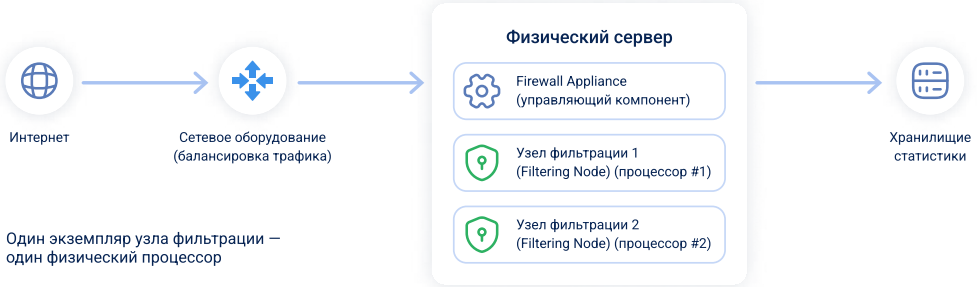
01 Совмещённое развёртывание

Firewall Appliance и один узел фильтрации размещаются на одном физическом сервере.



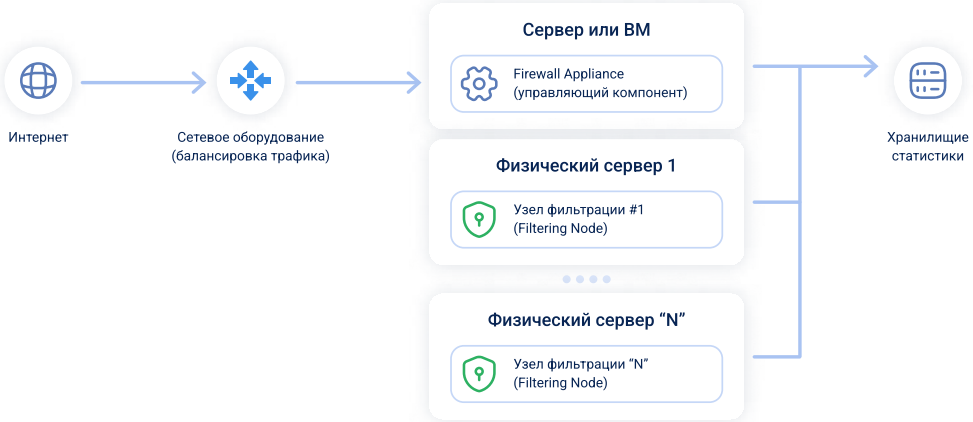
02 Многопроцессорный сервер фильтрации

На одном физическом сервере размещается несколько экземпляров узлов фильтрации — по одному на каждый физический процессор. Firewall Appliance может быть развернут на этом же сервере или отдельно.



03 Раздельное развёртывание

Firewall Appliance размещается на отдельном физическом сервере или в виртуальной машине, а узлы фильтрации — на выделенных физических серверах.



04 Географически распределённое развёртывание

Управляющий компонент размещается в центральной точке, а узлы фильтрации — в различных географических локациях.

Общие принципы функционирования

Независимо от выбранного варианта развёртывания система работает по единым принципам:

- узлы фильтрации функционируют в конфигурации Active-Active;
- синхронизация служебных данных осуществляется напрямую между узлами фильтрации;
- распределение пользовательского трафика между узлами выполняется средствами внешней сетевой инфраструктуры;
- при отказе одного из узлов фильтрации трафик автоматически перераспределяется между оставшимися узлами;
- при недоступности Firewall Appliance узлы фильтрации продолжают обработку трафика с использованием ранее загруженной конфигурации.

4. Ландшафт угроз и поддерживаемые типы DDoS-атак

4.1. Современные DDoS-угрозы

Современные DDoS-атаки характеризуются высокой интенсивностью, использованием нескольких векторов воздействия и быстрым изменением сценариев в ходе атаки. В качестве источников атак широко используются ботнеты, распределённые сети заражённых устройств (IoT), арендованные DDoS-платформы (Stresser/Booter) и специализированные инструменты генерации сетевого трафика.

На практике злоумышленники одновременно применяют несколько методов воздействия, сочетая объёмные атаки, атаки на сетевые и транспортные протоколы, а также атаки, направленные на исчерпание ресурсов защищаемых сервисов.

StormWall Appliance обеспечивает обнаружение и фильтрацию DDoS-атак на уровнях L3–L5 модели OSI и поддерживает защиту от наиболее распространённых современных векторов атак.

4.2. Противодействие различным типам DDoS-атак

Фильтрация выполняется в режиме реального времени на основе попакетного анализа. Каждый пакет последовательно проверяется набором специализированных механизмов защиты и правил фильтрации, после чего легитимный трафик передаётся в защищаемую инфраструктуру. Политики безопасности формируются из набора готовых механизмов защиты и могут быть адаптированы под особенности защищаемых сервисов.

Класс атак	Примеры
Атаки на TCP-протокол	SYN Flood, SYN/ACK Flood, ACK Flood, FIN/RST Flood, TCP Spoofing, некорректные TCP-флаги и пр.
Исчерпание таблиц TCP-соединений	Flood установленными соединениями, медленные соединения и пр.
Пакетные атаки L3/L4	UDP Flood, ICMP Flood, IP Protocol Flood, PPS Flood
Reflection / Amplification	DNS Reflection, NTP Reflection, SSDP, CLDAP, Memcached и другие UDP Reflection-атаки
Атаки с IP-фрагментацией	Fragment Flood, ICMP Fragment Flood, UDP Fragment Flood
DNS-атаки	DNS Flood, некорректные DNS-запросы, запросы ресурсоемких типов записей
TLS — и QUIC-атаки	TLS ClientHello Flood, QUIC Flood, бот-трафик в зашифрованных соединениях
Атаки на игровые сервисы	Steam Query Flood, Source Engine Query, FiveM, RakNet, SA-MP, TeamSpeak 3
Атаки из отдельных сетей и регионов	Ботнеты из определённых ASN, атаки по географическому признаку, Carpet Bombing
Аномальные параметры IP-пакетов	Превышение MTU, аномальные размеры пакетов

Примечание: Набор механизмов фильтрации и поддерживаемых протоколов постоянно развивается и дополняется по мере появления новых механизмов противодействия DDoS-атакам

5. Механизмы защиты и контрмеры

StormWall Appliance использует многоуровневую систему защиты, объединяющую специализированные механизмы анализа, фильтрации и управления трафиком. Политики безопасности формируются из набора готовых механизмов защиты и могут быть адаптированы под особенности сетевой инфраструктуры, прикладных сервисов и профиля легитимного трафика.

Фильтрация выполняется в режиме реального времени на основе попакетного анализа. Механизмы защиты могут использоваться совместно, обеспечивая эффективное противодействие как отдельным векторам атак, так и сложным мультивекторным DDoS-атакам.

Механизм	Возможности
Защита TCP-протокола	Валидация TCP-трафика на соответствие требованиям RFC, включая проверку корректности установления соединений, последовательности пакетов, TCP-флагов, обработки фрагментации и управления жизненным циклом соединений. Поддерживаются механизмы защиты, основанные на требованиях RFC 793 (Transmission Control Protocol), RFC 1122 (Requirements for Internet Hosts), RFC 1323 (TCP Extensions for High Performance), RFC 2018 (Selective Acknowledgment), RFC 5961 (Improving TCP Robustness Against Blind In-Window Attacks) и RFC 6528 (Defending Against Sequence Number Attacks)
Ограничение нагрузки (Rate Limiting)	Ограничение пропускной способности (BPS), количества пакетов (PPS), количества новых и активных TCP-соединений, многоуровневое каскадное ограничение скорости, защита от исчерпания ресурсов
Защита DNS	Нативные DNS-фильтры с поддержкой RFC 1034 (Domain Names — Concepts and Facilities) и RFC 1035 (Domain Names — Implementation and Specification). Валидация DNS-пакетов, фильтрация по типам записей, доменным именам, классам запросов и ограничение интенсивности DNS-трафика
Защита TLS и QUIC	Анализ параметров TLS ClientHello без расшифровки пользовательского трафика в соответствии с RFC 5246 (TLS 1.2), RFC 8446 (TLS 1.3), RFC 6066 (Server Name Indication, SNI), RFC 7301 (Application-Layer Protocol Negotiation, ALPN), RFC 8999 (Version-Independent Properties of QUIC) и RFC 9000 (QUIC Transport Protocol). Поддерживается анализ JA3/JA4-отпечатков, версий TLS, SNI, ALPN и авторизация клиентов QUIC
Challenge-авторизация	Проверка легитимности клиентов с использованием challenge-механизмов для защиты игровых и специализированных протоколов
Географическая и ASN-фильтрация	Фильтрация трафика по странам, автономным системам (ASN) и другим сетевым признакам
Статические и динамические списки доступа	Белые и чёрные списки IP-адресов, поддержка IP Sets, динамические списки доступа с автоматическим временем жизни (TTL). Формирование правил по множеству параметров, включая IP-адреса источника и назначения, подсети, номера портов, транспортные протоколы и их комбинации
Глубокий анализ пакетов (DPI)	Фильтрация по значениям заголовков сетевых и транспортных протоколов, отдельным полям пакетов, диапазонам значений, HEX-маскам, байтовым смещениям (Byte Offset), сигнатурам полезной нагрузки (Payload), размерам пакетов и пользовательским условиям обработки трафика
Контроль параметров пакетов	Контроль размеров пакетов, поддержка PMTUD (RFC 1191), обработка IP-фрагментации (RFC 791, RFC 815), фильтрация по протоколам, портам, типам пакетов и другим параметрам сетевого трафика
Интеграция с сетевой инфраструктурой	Прозрачное включение в сеть на уровне L2, интеграция с VRF, работа в составе существующей сетевой инфраструктуры
Мониторинг и аналитика	Сбор статистики по трафику и событиям безопасности, хранение и визуализация данных в едином web-интерфейсе
Управление и автоматизация	Централизованное управление через web-интерфейс, REST API для автоматизации конфигурирования, управления политиками безопасности, получения статистики и интеграции с внешними системами

Примечание: Набор механизмов фильтрации и поддерживаемых протоколов постоянно развивается и дополняется по мере появления новых механизмов противодействия DDoS-атакам

6. Поддерживаемые аппаратные платформы

Для обеспечения заявленной производительности, стабильной работы и предоставления полной технической поддержки рекомендуется использовать аппаратные платформы, прошедшие внутреннее тестирование StormWall. Развёртывание на платформах, не входящих в перечень протестированных, допускается; в этом случае совместимость оборудования оценивается индивидуально.

6.1. Общие требования

Параметр	Требование
Архитектура	x86-64-v2 или AMD Zen2
Минимальная конфигурация одного узла фильтрации	4 физических вычислительных ядра; 16 Гб оперативной памяти; не менее 64 ГБ дискового пространства; сетевой адаптер с пропускной способностью не менее 1 Gbps
Обработка трафика	Требуется поддержка hugepages и совместимый с DPDK сетевой адаптер
Управление энергопотреблением	Поддерживается адаптивное управление энергопотреблением на уровне обработчика трафика. Требуется, чтобы управление частотой процессора было передано операционной системе

6.2. Процессоры

Производитель	Требования и совместимость	Протестировано StormWall
AMD	Процессоры AMD EPYC на архитектуре Zen 2 и выше	EPYC 7702 (64 ядра), EPYC 7742 (64 ядра), EPYC 7543 (32 ядра), EPYC 7763 (64 ядра), EPYC 7773X (64 ядра)
Intel	Процессоры Intel Xeon, поддерживающие архитектуру x86-64-v2 и выше, включая линейку Intel Xeon Scalable	Xeon E5–2696 v4 @ 2.20 GHz, Xeon E5–2699 v4 @ 2.20 GHz, Xeon E5–2699A v4 @ 2.40 GHz

Последующие поколения процессоров указанных линеек считаются совместимыми при сохранении требований к архитектуре и набору инструкций. Совместимость конкретной модели, не входящей в перечень протестированных, подтверждается по запросу.

6.3. Поддерживаемые сетевые адаптеры

Поддерживаются сетевые адаптеры с поддержкой DPDK, прошедшие внутреннее тестирование StormWall.

Физические адаптеры

Производитель	Драйвер	Совместимые модели	Протестировано StormWall
Intel	i40e	Intel 7xx	Intel Ethernet Controller XL710 for 40GbE QSFP+
NVIDIA (Mellanox)	mlx5	ConnectX-5, ConnectX-6	MT27800–ConnectX–5, MT28800–ConnectX–5 Ex, MT2892–ConnectX–6 Dx

Виртуальные адаптеры (при развёртывании в виртуальной инфраструктуре)

Адаптер	Платформа виртуализации
VirtIO	QEMU
VMXNET3	VMware

Рекомендуется использовать последнюю доступную версию драйвера и компонентов виртуализации для соответствующей платформы.

6.4. Серверные платформы и настройки BIOS:

Решение StormWall Appliance не привязано к серверам конкретных производителей. Совместимость серверной платформы определяется возможностью применения необходимых настроек BIOS и требуемой конфигурации аппаратных компонентов. При необходимости совместимость конкретной серверной платформы оценивается индивидуально.

Узел фильтрации поддерживает адаптивное управление энергопотреблением: частота процессорных ядер изменяется в зависимости от текущей нагрузки на обработку трафика. Для работы этого механизма управление частотой должно быть передано операционной системе, а механизмы глубоких состояний энергосбережения — отключены.

Для обеспечения стабильной и предсказуемой производительности DPDK на серверах фильтрации необходимо использовать профиль BIOS, ориентированный на максимальную производительность. NUMA должна быть включена, сетевые адаптеры должны располагаться в PCIe-слотах с достаточной пропускной способностью и быть локальными для NUMA-узла, на котором выполняются DPDK-потоки.

Настройки энергосбережения CPU и PCIe рекомендуется отключить. DPDK-потоки рекомендуется размещать на физических ядрах CPU. Конкретные значения NUMA/NPS и другие платформозависимые параметры определяются с учётом архитектуры сервера, CPU, сетевых адаптеров.

Физические адаптеры

BIOS-параметр	AMD	Intel	Требование / значение	Приоритет
Профиль производительности системы (Performance Profile)	✓	✓	Производительность / Максимальная производительность	Обязательно
NUMA	✓	✓	**Включено**	Обязательно
Настройка NUMA / NPS	✓	✗	Значение **NPS1/NPS2/NPS4** выбирается с учётом топологии CPU, памяти и сетевых адаптеров	Обязательно настроить
Оптимизация памяти NUMA	✓	✓	**Включено;** память должна быть равномерно распределена между NUMA-узлами и каналами памяти	Обязательно
Расположение сетевого адаптера относительно NUMA	✓	✓	Сетевой адаптер должен быть подключён к PCIe-слоту, локальному для NUMA-узла, на котором работают DPDK-потоки	Критично
Состояния энергосбережения CPU (C-States)	✓	✓	**Отключено** для минимизации задержек и повышения предсказуемости производительности	Рекомендуется
Глубокие состояния энергосбережения CPU (C3/C6 и аналоги)	✓	✓	**Отключено**	Рекомендуется

Физические адаптеры

BIOS-параметр	AMD	Intel	Требование / значение	Приоритет
Управление энергопотреблением CPU	✓	✓	**Режим производительности**	Рекомендуется
SMT / Hyper-Threading	✓	✓	Рекомендуется включение	Рекомендуется
Частота памяти	✓	✓	Максимальная поддерживаемая процессором и установленными модулями памяти	Рекомендуется
Распределение модулей памяти	✓	✓	Симметричное заполнение каналов памяти в соответствии с рекомендациями производителя сервера	Обязательно
PCIe ASPM / энергосбережение PCIe	✓	✓	**Отключено** для сетевых адаптеров	Рекомендуется
Скорость PCIe	✓	✓	**Максимально поддерживаемая** сетевым адаптером, процессором и материнской платой	Обязательно проверить
Above 4G Decoding	✓	✓	**Включено**	Обязательно рекомендуется
Аппаратная предварительная выборка данных (Hardware Prefetcher)	✓	✓	**Включено** / значение по умолчанию производителя	Рекомендуется
AMD IOMMU / Intel VT-d	✓	✓	**Включено при использовании VFIO или SR-IOV;** для обычного доступа DPDK к физическому сетевому адаптеру не является обязательным	При необходимости
SR-IOV	✓	✓	**Включено только при использовании виртуальных функций (VF)**	При необходимости
Аппаратная виртуализация (AMD–V / Intel VT-x)	✓	✓	**Включено при использовании виртуализации;** для работы DPDK на физическом сервере не является обязательным	При необходимости
AMD Determinism Control	✓	✗	Для производительного профиля использовать режим, обеспечивающий максимальную и предсказуемую производительность	AMD
L3 Cache как отдельные NUMA-узлы	✓	✗	**Отключено** как базовая конфигурация; изменение допускается только после проверки производительности конкретной платформы	AMD
Intel SpeedStep / аналогичное динамическое управление частотой	✗	✓	Для старых поколений Intel — **отключено** при использовании профиля фиксированной производительности; на современных Xeon настройка определяется профилем производителя	Intel
Energy Efficient Turbo / энергосберегающий Turbo	✗	✓	**Отключено,** если приоритетом являются минимальная задержка и предсказуемость производительности	Intel

6.5. Использование аппаратных платформ, не входящих в перечень протестированных

StormWall допускает развёртывание решения на аппаратных платформах, не входящих в перечень протестированных конфигураций.

В этом случае:

- специалисты StormWall оказывают консультационную поддержку по вопросам установки и настройки решения;
- совместимость оборудования оценивается индивидуально;
- достижение заявленных характеристик производительности, масштабируемости и отказоустойчивости не гарантируется;
- при выявлении аппаратно-зависимых особенностей поддержка может рекомендовать использование одной из протестированных аппаратных платформ.

7. Системные требования

Приведённые ниже требования являются минимально необходимыми для установки и запуска компонентов StormWall Appliance. Рекомендуемая аппаратная конфигурация определяется архитектурой развёртывания, объёмом защищаемого трафика, количеством узлов фильтрации и сроком хранения статистических данных.

7.1. Сервер Firewall Appliance

Параметр	Минимальные требования
Операционная система	AlmaLinux 9.0 и выше
Архитектура	x86_64
Платформа развёртывания	Физический сервер или виртуальная машина (VMware, KVM, Microsoft Hyper-V)
Процессор	Не менее 8 физических вычислительных ядер
Оперативная память	Не менее 16 GB
Дисковая подсистема	SSD объёмом не менее 128 GB
Сетевое подключение	Доступ по HTTPS (порты 8444 и 9444) к licensing.stormwall.network и HTTPS (TCP/443) к repo.stormwall.network

Примечания:

- При использовании виртуальной инфраструктуры должны быть установлены гостевые дополнения, совместимые с используемой версией ядра Linux.
- Рекомендуется выделить не менее **30 GB** дискового пространства для компонентов системы и не менее **50 GB** для хранения статистики ClickHouse.

7.2. Сервер узла фильтрации (Filtering Node)

Параметр	Минимальные требования
Операционная система	Только Alma Linux 9.X
Архитектура	x86-64-v2 или AMD Zen2
Платформа развёртывания	Физический сервер
Процессор	Не менее 4 физических ядер
Оперативная память	Не менее 16 GB
Диск	Не менее 64 GB
Пропускная способность	Согласно параметрам лицензии
Сетевые адаптеры	Согласно параметрам лицензии. Не менее одного адаптера с пропускной способностью от 1 Gbps и поддержкой DPDK

Примечания:

- Необходимо использовать отдельный физический процессор для каждого экземпляра узла фильтрации.
- При использовании виртуальной инфраструктуры должны быть установлены дополнения, совместимые с используемой версией ядра Linux.
- Для обеспечения заявленной производительности рекомендуется использовать поддерживаемые серверные платформы, процессоры и сетевые адаптеры, приведённые в разделе **6.**

Общие рекомендации

- Минимальные системные требования обеспечивают установку и запуск компонентов системы.
- Производительность решения зависит от объёма защищаемого трафика, количества узлов фильтрации, числа одновременно обрабатываемых соединений и выбранной архитектуры развёртывания.
- При увеличении количества узлов фильтрации возрастают требования преимущественно к серверу **Firewall Appliance,** в первую очередь к объёму оперативной памяти и дисковой подсистеме для хранения статистики.
- При проектировании высоконагруженных инсталляций рекомендуется использовать поддерживаемые аппаратные платформы и выделенные физические серверы для узлов фильтрации.

8. Лицензирование

StormWall Appliance использует программную систему лицензирования. Основным параметром лицензии является активная портовая ёмкость. В зависимости от выбранной лицензии также определяются максимально доступные аппаратные ресурсы узлов фильтрации, включая количество процессорных ядер, объём оперативной памяти и максимальную пропускную способность.

По умолчанию применяется онлайн-модель лицензирования, при которой управляющему компоненту Firewall Appliance требуется доступ к серверу лицензирования licensing.stormwall.network по протоколу HTTPS (порты 8444 и 9444) для активации лицензии и периодической проверки её статуса. После восстановления сетевого подключения активация лицензии может быть выполнена без переустановки системы.

Для инфраструктур, не имеющих доступа к внешним сетям или предъявляющих повышенные требования к изоляции, предусмотрена офлайн-модель лицензирования. В этом случае лицензия предоставляется в виде индивидуального аппаратного ключа Guardant, обеспечивающего работу системы без подключения к серверу лицензирования StormWall.

StormWall Appliance

По всем вопросам, связанным с развёртыванием решения, **обращайтесь по контактам ниже:**

8 800 550-89-36

sales@stormwall.pro

https://stormwall.pro