SOLAR

МЕЖСЕТЕВОЙ ЭКРАН НОВОГО ПОКОЛЕНИЯ

Solar NGFW

МОСКВА, 2024

W:RT-SOLAR.RU

1. ПРОБЛЕМАТИКА

Защита сети – базовая функция информационной безопасности. Любой инцидент, связанный с проникновением за периметр корпоративной сети, может нарушить непрерывность бизнеса, привести к утечкам информации или стать началом крупномасштабной кибератаки. По данным исследования «Солара», проведенного в марте 2023 года, за 2022 год более 66% компаний столкнулись с сетевыми атаками. При этом средний ущерб составил:

- При заражении сети и ее сегментов, включая заражение вредоносным ПО – 9,4 млн руб., а затраты на устранение инцидента – в среднем 7,7 млн руб. 77% компаний признали такой инцидент опасным.
- При компрометации инфраструктуры, включая контроллеры доменов, – 9,9 млн руб., а затраты на устранение инцидента – в среднем 7,5 млн руб. 73% компаний признали такой инцидент опасным.
- При контроле сетевого оборудования – 10,7 млн руб., а затраты на его устранение – в среднем 7,9 млн руб. 66% компаний признали такой инцидент опасным.

Для защиты от сетевых атак уже несколько десятилетий используются межсетевые экраны. Постепенно их возможности развивались, к стандартным функциям межсетевого экранирования добавлялись новые механизмы защиты: потоковый антивирус, веб-прокси, система обнаружения и предотвращения вторжений (Intrusion Prevention System, IPS), шифрование для построения виртуальных частных сетей (Virtual Private Network, VPN). В итоге к 2004 году консалтинговой компанией IDC был выделен новый класс решений для обеспечения сетевой безопасности – UTM (Unified Threat Management), а к 2008 году эксперты аналитической компании Gartner ввели термин «межсетевой экран нового поколения» (Next Generation Firewall, NGFW).

Изначально у них были существенные различия, в первую очередь заключающиеся в наличии у NGFW функции глубокого анализа пакетов (Deep Packet Inspection, DPI), позволяющей контролировать трафик приложений. Кроме этого, в отличие от UTM у NGFW обработка трафика осуществлялась одновременно на нескольких механизмах защиты, а применение аппаратных ускорителей на программируемых вентильных матрицах (FPGA) или ASIC-чипах значительно повышали производительность при одновременном включении всех функций. По этой причине укоренилось мнение, что UTM предназначены для малого и среднего бизнеса, а также защиты филиалов, а NGFW – для крупного бизнеса и ЦОДов.

Но с течением времени UTM и NGFW функционально сближались друг с другом, и уже несколько лет аналитики Gartner считают, что они стали настолько схожи, что их уже нет смысла различать, и предлагают использовать общий термин Network Firewall. Но и в России, и в мире этот термин среди заказчиков пока так и не прижился, а абсолютное большинство вендоров межсетевых экранов позиционируют свои разработки как NGFW. Поэтому далее в этом документе мы будем использовать термин NGFW.

Одна из ключевых выгод применения NGFW – объединение нескольких средств защиты в одном продукте. Это позволяет легче и быстрее решать задачи по защите сети и управлению доступом в интернет. Кроме того, использование внешних источников для обогащения NGFW данными о киберугрозах позволяет быстрее и эффективнее справляться с ними. По этой причине сегодня NGFW используются в 90% российских организаций, представляющих крупный бизнес и федеральные органы исполнительной власти.

Долгое время в России абсолютное большинство используемых решений были иностранного производства. Но в 2022 году привычная ситуация кардинально изменилась. С началом специальной военной операции количество кибератак на крупный бизнес, государственные организации и критическую информационную инфраструктуру России лавинообразно возросло. Одновременно с этим большинство зарубежных вендоров начали уходить с российского рынка. Некоторые из них – просто отключая свои решения без возврата денег за оплаченные подписки. Другие – сворачивая техническую поддержку, продажи и обновления баз сигнатур.

При этом оказалось, что полноценной замены зарубежным NGFW среди российских решений нет. Это в большей степени связано с тем, что иностранные разработчики NGFW изначально завоевали самые выгодные позиции на рынке России. Многие российские вендоры выжили только потому, что в первую очередь занимались сертифицированными VPN шлюзами, которых избегали зарубежные конкуренты. Либо стали создавать решения для сегмента малого бизнеса, который крупным мировым вендорам был просто неинтересен.

И в момент, когда зарубежные вендоры ушли, ни один российский межсетевой экран не смог полностью заменить ушедшие зарубежные NGFW. Для создания решений этого класса требуется проработанная высокопроизводительная архитектура, широкие и глубокие знания сетевых технологий, большая команда профессионалов, постоянное обновление сигнатур для встроенных механизмов защиты. А это сложно, дорого и требует времени.

Более того, уже упомянутая специфика российского рынка привела к тому, что в архитектурном плане мало кто из отечественных разработчиков закладывал по-настоящему высокие требования к производительности. Теперь им приходится бороться с наследием прошлого. Нельзя просто так изменить архитектуру уже давно продающегося решения, так как есть обязательства перед текущими заказчиками, широкий модельный ряд, в

том числе устаревший, который нужно поддерживать, а также унаследованный код, часто созданный 10–20 лет назад. Начинают мешать казавшиеся ранее оптимальными архитектурные решения. В некоторых случаях быстрее и проще сделать NGFW с нуля.

В этих условиях российские организации оказались в ситуации, когда киберугрозы нарастают, иностранные средства для их сдерживания с каждым днем теряют возможность им противодействовать, а большинство российских решений не могут выступать эффективной заменой. Кроме того, согласно Указу Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», к 1 января 2025 года 100% средств в органах власти, на стратегических и системообразующих предприятиях, предприятиях с госучастием, а также объектах КИИ должны быть отечественными.

Группа компаний «Солар» уже более 10 лет разрабатывает собственное сетевое решение для управления доступом сотрудников в интернет и защиты от веб-угроз – Solar webProxy. Оно ориентировано на потребности крупного бизнеса и доказало свою зрелость в крупнейшем федеральном проекте по обеспечению контентной фильтрации для российских школ. Сейчас в его рамках каждый день обрабатываются запросы более 1 000 000 пользователей на 45 000 площадках по всей России. В 2020 году, еще до начала СВО и «лихорадки» по разработке российского NGFW, было принято решение создать на технологической базе Solar webProxy собственный межсетевой экран нового поколения – Solar NGFW. До 2025 года для этой цели запланированы инвестиции в размере 1,5 млрд руб. В настоящее время команда продукта насчитывает 70 человек, среди которых 45 разработчиков, тестировщиков и архитекторов, еще 25 – аналитики, инженеры внедрения и поддержки. Планируется расширение команды до 100 человек.

За полгода после презентации продукта рынку команда успела запустить 25 пилотных проектов в 6 отраслях: телекоммуникации, финансовый сектор, нефтегазовая отрасль, транспортная сфера, ИБ-компании, госучреждения и компании с госучастием. Помимо пилотов были проведены работы по регистрации продукта в Реестре отечественного ПО. Кроме этого, было выпущено первое обновление – версия 1.1, основными нововведениями которой стали возможность работы Solar NGFW в Active-Passive кластере, а также добавление первых нескольких десятков сигнатур от центра исследования киберугроз Solar 4RAYS, исходные данные об атаках которому поставляет Solar JSOC – крупнейший и старейший SOC в России.

Спустя год после презентации первой версии продукт получил программно-аппаратное исполнение с возросшей в два раза максимальной производительностью, а также следующую версию ПО – 1.2, в которой были внесены важные изменения для удобной работы с уже насчитывающими сотни и постоянно увеличивающимися в количестве уникальными сигнатурами от Solar 4RAYS.

2. КРАТКОЕ ОПИСАНИЕ

2.1 НАЗНАЧЕНИЕ

Solar NGFW – программный межсетевой экран нового поколения для комплексной защиты корпоративной сети от сетевых угроз и вредоносного ПО, а также контроля доступа к веб-ресурсам. Архитектура Solar NGFW изначально создавалась с учетом требований крупных компаний, которым необходимо обеспечение высокой производительности в сложных условиях, когда смешанный трафик обрабатывается сразу несколькими механизмами защиты при применении большого количества правил и политик.

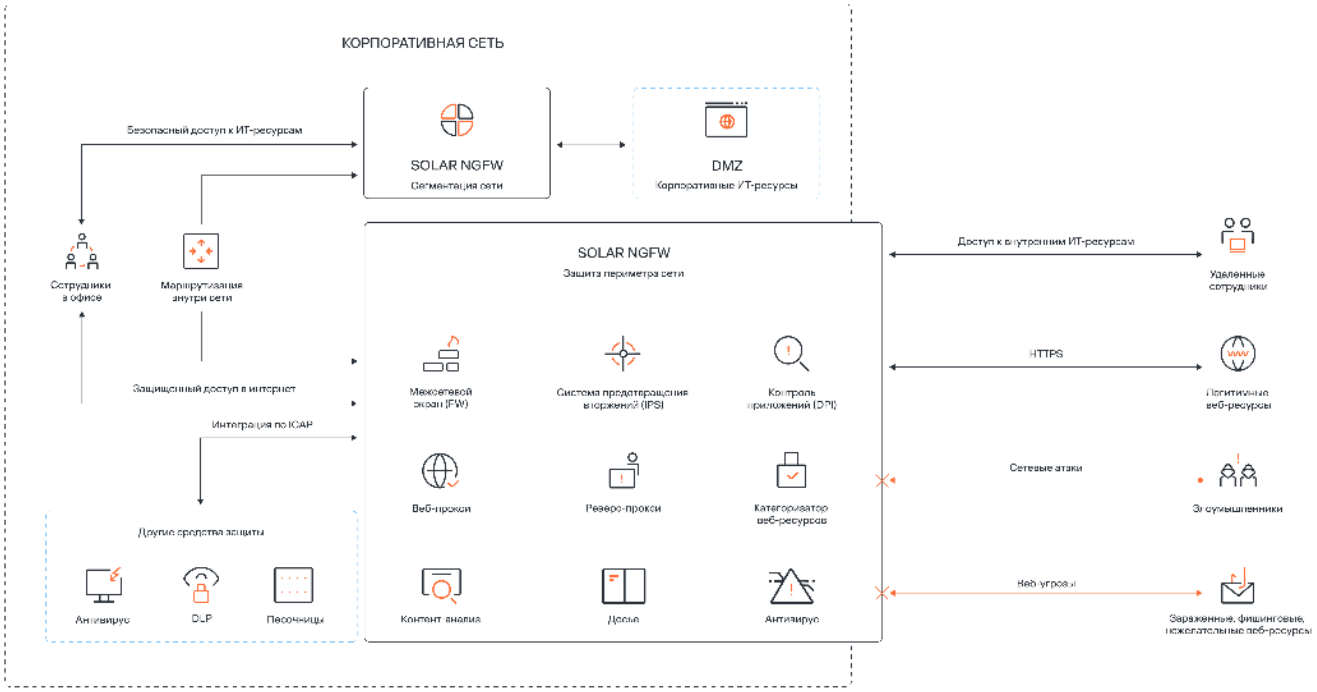

Рисунок 1. Solar NGFW в сетевой инфраструктуре

В Solar NGFW применяются следующие механизмы:

- Межсетевой экран (FW) – для обеспечения фильтрации трафика на основе IP-адресов и портов.
- Трансляция IP-адресов (NAT) – для сокрытия внутренних IP-адресов от возможных злоумышленников.
- Система предотвращения вторжений (IPS) – для сигнатурного обнаружения и блокирования сетевых атак, которые не могут быть отражены межсетевым экраном.
- Контроль сетевых приложений (App Control / DPI) – для контроля трафика приложений, приоритезации и выявления аномалий в их работе.
- Антивирус (AV) – для защиты от вредоносного ПО и веб фишинга.
- Аутентификация и авторизация – для контроля доступа сотрудников и приложений к конкретным веб-ресурсам.
- Веб-прокси – для проверки HTTPS-трафика и его передачи другим средствам защиты по протоколу ICAP.
- Реверс-прокси – для контроля доступа удаленных сотрудников к внутренним корпоративным веб-ресурсам.
- Категоризатор веб-ресурсов – для управления доступом к конкретным категориям веб-ресурсов: интернет-магазины, образовательные ресурсы, нежелательные сайты и т. д.

- Досье на персону – для применения персонализированных политик безопасности и индивидуального контроля трафика.
- Контентный анализ – для предотвращения утечек конфиденциальной информации.

Отличительные особенности Solar NGFW – высокая производительность, уникальные сигнатуры IPS от Solar 4RAYS, современный и удобный веб-интерфейс со встроенной справкой и интерактивными отчетами, быстрое обучение администрированию продукта, досье на сотрудника работающее в тесной интеграции с DLP-системой Solar Dozor для предотвращения утечек конфиденциальной информации в автоматическом режиме, а также сопровождение экспертами вендора на всем жизненном цикле продукта.

Solar NGFW обеспечивает максимально безболезненную интеграцию в существующую инфраструктуру и переход на российский полнофункциональный продукт со стабильным развитием и квалифицированной технической поддержкой в режиме 24/7.

2.2 РЕШАЕМЫЕ ЗАДАЧИ

Защита от атак на периметре сети и ее сегментация:

- Скорость межсетевого экрана Enterprise-уровня – до 40 Гбит/с
- Контроль приложений с помощью глубокого анализа пакетов (DPI)
- Сигнатуры IPS от Solar 4RAYS и Solar JSOC – коммерческого SOC № 1 в России
- Встроенный антивирус для защиты от вредоносного ПО и сайтов
- Интеграция с другими средствами защиты по протоколам ICAP и syslog

Управление доступом в интернет и к внутренним веб-ресурсам:

- Гибкие иерархические политики доступа пользователей к веб-ресурсам
- Категоризатор для блокирования доступа к нежелательному контенту
- Досье на сотрудника и интерактивные отчеты для анализа использования интернета
- Реверс-прокси для контроля доступа к внутренним веб-ресурсам: OWA, 1С и т. д.
- Нативная интеграция с DLP-системой Solar Dozor для предотвращения утечек

2.3 ОБЩИЙ ПРИНЦИП РАБОТЫ

Solar NGFW устанавливается «в разрыв» трафика и контролирует все данные, передаваемые между двумя сетями. При этом механизмы защиты Solar NGFW работают параллельно, но каждый по своим базам сигнатур и правил. Это обеспечивает комплексную проверку трафика на соответствие политике безопасности. Объединение нескольких механизмов защиты в одном решении гарантирует надежную защиту корпоративной сети от сетевых и веб-угроз, одновременно упрощая администрирование.

1. Расшифровка трафика. Сегодня более 95% сетевого трафика передается по протоколу HTTPS. Solar NGFW расшифровывает входящий и исходящий корпоративный трафик, после чего готовые к обработке данные передаются на другие компоненты защиты продукта.

2. Анализ данных. Механизмы защиты Solar NGFW работают параллельно, поэтому проверка трафика производится одновременно межсетевым экраном, системой обнаружения и предотвращения вторжений, системой глубокого анализа пакетов и встроенным антивирусом.
3. Дополнительные проверки. Данные из трафика могут также обрабатываться для разграничения доступа пользователей к веб-ресурсам или предотвращения утечек. Для дополнительной проверки трафика сторонними средствами защиты в Solar NGFW реализован протокол ICAP.
4. Блокировка или допуск трафика. Если результаты всех проверок соответствуют политикам безопасности, Solar NGFW разрешает обмен данными между внутренней и внешней сетями. В противном случае передача данных блокируется, а администратор получает оповещение об инциденте.

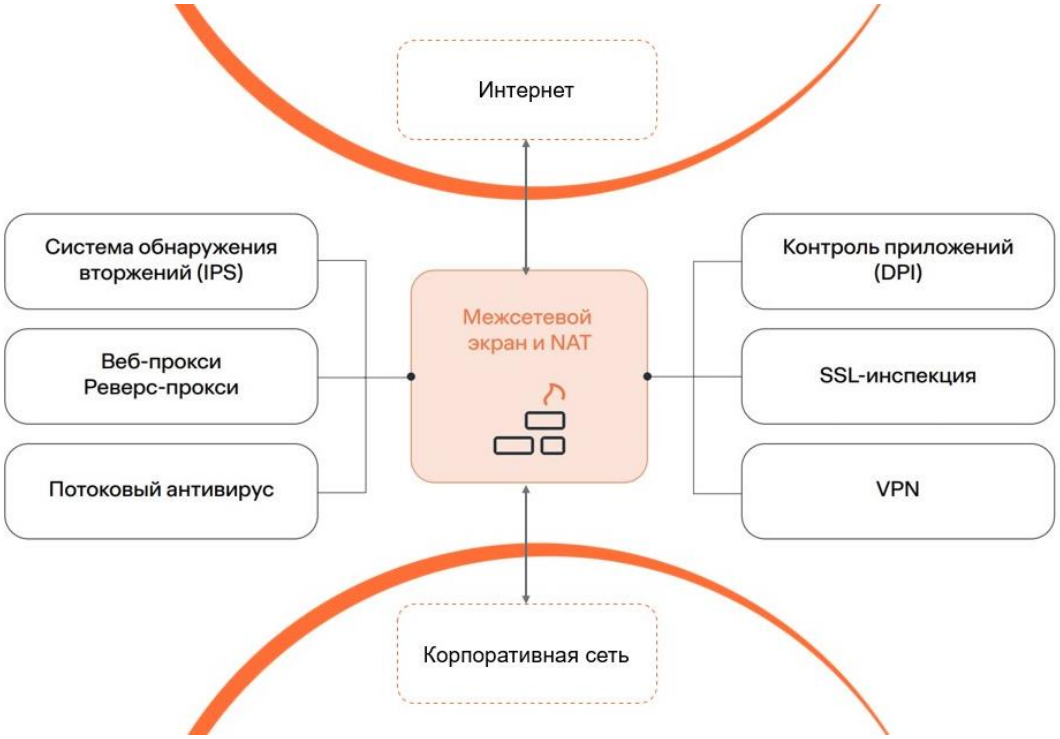

Рисунок 2. Принцип работы Solar NGFW

2.4 ОСНОВНЫЕ ВОЗМОЖНОСТИ

- <u>МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ И NAT</u>

  Основа NGFW. Работает в режиме stateful packet inspection (SPI), проверяет базовые характеристики трафика: IP-адреса назначения и отправления, порты, протоколы транспортного уровня и время передачи пакета (L3/L4 модели OSI).

  В межсетевом экране реализован механизм смены IP-адресов (NAT), позволяющий скрыть от злоумышленника внутреннюю топологию корпоративной сети и пресечь разведку.

- <u>СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ</u>

  В Solar NGFW встроена система обнаружения и предотвращения вторжений (IPS) на базе Suricata. Она позволяет быстро идентифицировать и остановить сложные сетевые атаки, которые могут быть пропущены межсетевым экраном. Возможно создание исключений по сетевым параметрам / ID сигнатур.

Входящий трафик проверяется на совпадение с сигнатурами атак. Это обеспечивает обнаружение и блокировку запросов и данных, не соответствующих политике безопасности. Также фиксируются потенциально опасные аномалии трафика. Стандартные сигнатуры IPS дополняются уникальными сигнатурами от Solar 4 RAYS и Solar JSOC – первого и крупнейшего коммерческого SOC в России.
В базовый набор входит 30 000+ сигнатур, которые обновляются ежедневно в автоматическом режиме. Есть возможность добавлять сигнатуры и их категории вручную.

- КОНТРОЛЬ ПРИЛОЖЕНИЙ

  Современные приложения не всегда используют стандартные порты. При подготовке атаки злоумышленники учитывают эти особенности, что позволяет им обходить межсетевой экран. Собственная технология проверки данных приложений внутри пакета трафика на основе nDPI решает эту проблему. При выявлении некорректного поведения приложения или попытки скрыть свой трафик модуль оповещает администратора о возможном инциденте.
  Дополнительно DPI позволяет управлять трафиком для оптимизации нагрузки на сеть. Примером могут быть блокировки нежелательных приложений – мессенджеров, торрентов и т. д., а также изменение приоритета трафика.
  Определяется трафик 300+ прикладных протоколов, в том числе и российских приложений. Возможна донастройка DPI под специфику заказчика.

- КОНТРОЛЬ HTTPS-ТРАФИКА

  Solar NGFW выступает в качестве посредника между клиентом и сервером, что позволяет расшифровывать HTTPS-трафик. Это необходимо для проверки трафика другими механизмами защиты и применения собственных политик безопасности, в том числе и проверки по ключевым словам. Реализована возможность запроса цепочки сертификатов для расшифровки HTTPS-трафика, если запрашиваемый веб-ресурс не предоставляет всю цепочку доверия.
  При отсутствии на рабочих станциях сотрудников сертификатов расшифровки HTTPS трафика Solar NGFW может перенаправлять пользователя на страницу с инструкцией по его загрузке и установке. В качестве страницы с инструкцией используется как предустановленная в Solar NGFW, так и любая внешняя страница. Доступ к интернету в этом случае прекращается до момента установки сертификата.
  При интеграции с DLP-системой Solar Dozor расшифровка HTTPS помогает выявлять утечки конфиденциальной информации, даже если она передается по защищенному каналу связи.

- ПРОВЕРКА НА НАЛИЧИЕ ВРЕДОНОСНОГО ПО

  При фильтрации трафика передаваемые файлы можно проверять на наличие вредоносного ПО. Для этого в систему интегрирован модуль антивирусной защиты, который осуществляет поиск и обезвреживание угроз в интернет-трафике, поступающем по протоколам HTTP / HTTPS / FTP over HTTP, ограничивает доступ к взломанным и потенциально опасным ресурсам, а сам механизм проверки оптимизирован за счет применения технологии Preview.
  Также модуль способен анализировать данные, передаваемые в интернет. Антивирус проверяет запросы пользователей, в том числе попытки подключения к веб-серверу и загрузки на него различных файлов. Проходят проверку и данные, направляемые веб серверами в ответ на запросы пользователей. При попытке загрузки вредоносной страницы или при обнаружении вируса система оповестит пользователя.
  Для ограничения доступа к нежелательным веб-сайтам используется автоматически обновляемая

база данных, содержащая черные списки сайтов, которые разбиты по категориям.
При этом сохраняется возможность интеграции с другими антивирусными решениями, как проприетарными, так и свободно распространяемыми.

- УПРАВЛЕНИЕ ДОСТУПОМ СОТРУДНИКОВ В ИНТЕРНЕТ
  В Solar NGFW реализованы гибкие иерархические политики для разграничения доступа сотрудников и веб-приложений в интернет. К каждому пользователю, группе пользователей, IP-адресу или IP-диапазону источника можно применить политику фильтрации в виде набора правил. Она регулирует управление, защиту и распределение получаемой из интернета информации.
  При этом фильтрацию можно вести по нескольким десяткам параметров, в том числе членству в группе, URL- или IP-адресу ресурса, ключевым словам, расписанию, портам, протоколам, типу передаваемого файла и категории веб-сайта. Возможно предоставление частичного доступа к элементам сайта: видео на YouTube, комментарии и т. д.
  При поддержке ресурсом протокола HTTPS возможно принудительное перенаправление на HTTPS-версию сайта.

- АУТЕНТИФИКАЦИЯ
  Для разграничения прав доступа к веб-ресурсам на основе групп пользователей в Solar NGFW поддерживаются различные механизмы аутентификации – по IP-адресам, Kerberos (Negotiate), NTLM, NTLM + Negotiate, Basic.
  Для приложений, которые не поддерживают аутентификацию, возможно ее исключение для беспрепятственного доступа в интернет. Такими приложениями могут быть службы обновления ПО или банковские приложения.

- РАБОТА В РЕЖИМЕ ОБРАТНОГО ПРОКСИ-СЕРВЕРА
  Solar NGFW может работать в режиме обратного прокси-сервера, что позволяет проверять исходящий трафик компании и блокировать файлы с конфиденциальной информацией при попытке их выгрузки в интернет. Эта функция будет полезной для организаций, публикующих внутренние ресурсы «наружу», например, при организации удаленного доступа к корпоративной почте.
  Режим обратного прокси-сервера позволяет обеспечить дополнительную защиту компаний от утечек конфиденциальных документов и файлов через веб-ресурсы. При попытке выгрузки файлов с конфиденциальной информацией Solar NGFW проверяет их по ключевым словам и атрибутам, а также блокирует доступ к файлам, если обнаружено нарушение политик безопасности. При этом политика контентной фильтрации для прямого и обратного режима является общей и не требует дополнительных настроек.
  Весь трафик, проходящий в обратном режиме, получает соответствующую маркировку, которая отображается как в журналах запросов в разделе статистики, так и на рабочем столе системы.

- КАТЕГОРИЗАЦИЯ РЕСУРСОВ
  Solar NGFW осуществляет категоризацию интернет-ресурсов, используя для их определения сразу несколько сервисов: как собственный категоризатор Solar webCat, так и внешние, например SkyDNS и ЦАИР.
  Наличие собственного категоризатора позволяет не зависеть от внешних источников данных. Благодаря этому, заказчики могут пользоваться оперативно пополняемыми и обновляемыми базами категоризации интернет-сайтов.

Такая комбинация собственного и сторонних категоризаторов в совокупности с возможностью создания локального перечня категорий позволяет определять категории интернет-ресурсов максимально точно.

- УЧЕТ АКТИВНОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ И ОТЧЕТЫ

  Solar NGFW позволяет отслеживать деятельность пользователей в интернете, а также приложений, имеющих доступ в сеть. На основании получаемой информации можно формировать сводные данные о работе сотрудников и поведении трафика в виде статистических отчетов.
  Из общей статистической информации можно перейти к более детальной, а из нее – к «сырым» данным (записям журнала посещений веб-ресурсов).
  Для удобства пользователей в системе присутствуют рекомендуемые отчеты – готовые шаблоны по наиболее часто запрашиваемым срезам данных на основе статистики использования Solar NGFW. Например, вместо создания отчета по использованию социальных сетей в рабочее время можно воспользоваться уже готовым шаблоном с необходимыми настройками. Это позволит сэкономить время администраторов и ускорить выполнение задачи. Помимо готовых отчетов пользователь может создавать собственные шаблоны под каждую задачу с помощью набора фильтров-конструкторов. Отчеты можно как самостоятельно выгружать в формате PDF, а так и автоматически формировать и отправлять по электронной почте по расписанию.

- ВЕДЕНИЕ ДОСЬЕ СОТРУДНИКА

  Solar NGFW собирает в персонализированное досье информацию о каждом сотруднике, включая трафик приложений с его рабочей станции. Это позволяет применять к такому трафику правила политики безопасности, вести его учет и использовать в построении отчетов.
  В досье можно просмотреть статистику запросов по персонам, входящим в одну группу: ресурсы и их категории, объем использованного интернет-трафика. На графиках отображаются сведения о разрешенных и заблокированных запросах, объеме входящего и исходящего интернет-трафика. В таблицах приводятся выборки по наиболее посещаемым ресурсам и их категориям, а также по наиболее часто загружаемым типам данных.
  Возможна синхронизация досье сотрудников из Solar NGFW и DLP-системы Solar Dozor. Благодаря этому можно использовать единое досье с сохранением данных всех имеющихся в Solar Dozor и Solar NGFW персон и изменять их в любом из интерфейсов. Синхронизация выполняется автоматически.
  В досье можно создавать единые политики, настраивая доступ к данным в одной системе исходя из действий или нарушений в другой. Например, ограничение доступа к интернету для сотрудника, получившего доступ к чувствительным документам компании, – с целью предотвратить их возможную утечку. Или информирование администратора о каждом факте выхода в интернет сотрудника, в отношении которого ведется расследование, а также архивация всех подозрительных запросов пользователя и автоматическая блокировка доступа в интернет.

- МОНИТОРИНГ

  Позволяет в реальном времени контролировать работоспособность узлов и нагрузку, уведомлять администратора в случае недоступности какого-либо из ресурсов, а также перезапускать сервисы или автоматически отключать их от процесса обработки запросов.

- РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА АДМИНИСТРАТОРОВ

  Ролевая модель позволяет избирательно и гибко управлять доступом пользователей к системе.

Можно настраивать права доступа пользователей как к разделам системы (например, доступ к разделу «Политика»), так и к данным отдельных персон или групп.
В разделе «Пользователи» можно создавать, изменять, блокировать и удалять учетные записи пользователей системы, которым назначаются роли. Права доступа для пользователя определяются одной или несколькими ролями, которые можно назначить в карточке пользователя или в карточке роли.
Благодаря доступу к данным персон или групп можно через веб-интерфейс системы делегировать ответственному сотруднику полномочия по мониторингу активности пользователей подразделений. Можно настроить для роли список разрешенных для просмотра персон, а также настроить VIP-персоны, чей трафик не будет виден для созданной роли.

- ИНТЕГРАЦИЯ СО СМЕЖНЫМИ СИСТЕМАМИ
  Solar NGFW поддерживает интеграцию со смежными системами по ICAP. Продукт может работать в двух режимах – как клиент и как сервер.
  В качестве клиента Solar NGFW передает запрос на обработку данных в другую систему (песочницу, антивирус или DLP) и блокирует передачу данных в случае соответствующего ответа от этой системы.
  В качестве сервера Solar NGFW может проверять по собственной политике безопасности данные и запросы из других систем, сообщая им свое решение (заблокировать или нет).
  Интеграция с DLP-системой Solar Dozor позволяет проверять веб-трафик по ее политикам и блокировать утечки информации, которые нельзя отследить по ключевым словам. Например, если злоумышленник хочет переслать файл с конструкторской документацией в векторном формате на внешнее файловое хранилище.

2.5 ИНТЕРФЕЙС

Solar NGFW управляется из единой веб-консоли по защищенному протоколу HTTPS. Интерфейс веб-консоли разработан с учетом пользовательского опыта администраторов заказчиков и современных тенденций в дизайне. В каждой версии продукта вносятся изменения для повышения эргономичности, а также расширяется встроенная справка

Пользователю доступны следующие возможности:

- Просмотр статуса подключения к интернету и списка подключенных пользователей в онлайн-режиме;
- Управление политикой безопасности, в том числе управление списками ресурсов;
- Управление пользователями;
- Настройка и просмотр отчетов;
- Общая настройка системы и управление правами доступа администраторов на основе ролевой модели.

Рисунок 3. Интерфейс Solar NGFW. Главный рабочий стол

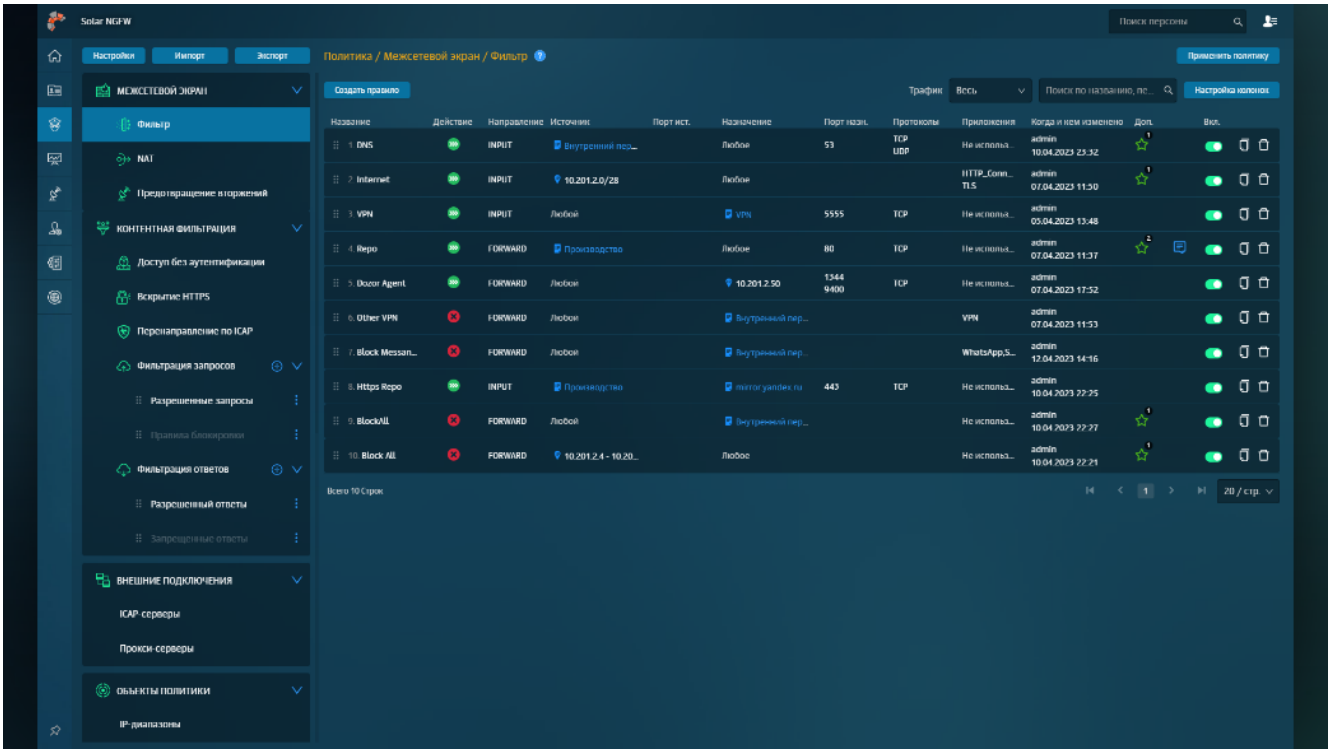

Рисунок 4. Интерфейс Solar NGFW. Политики FW

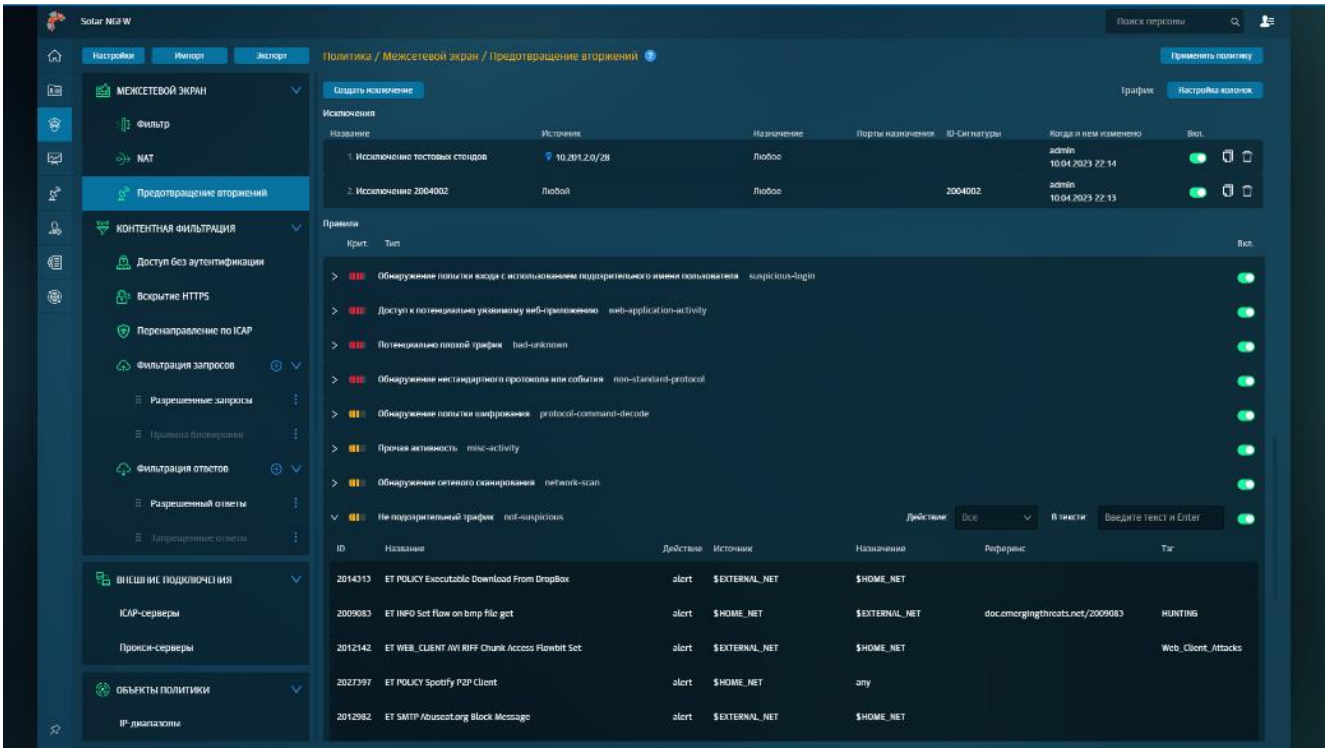

Рисунок 5. Интерфейс Solar NGFW. Политики IPS

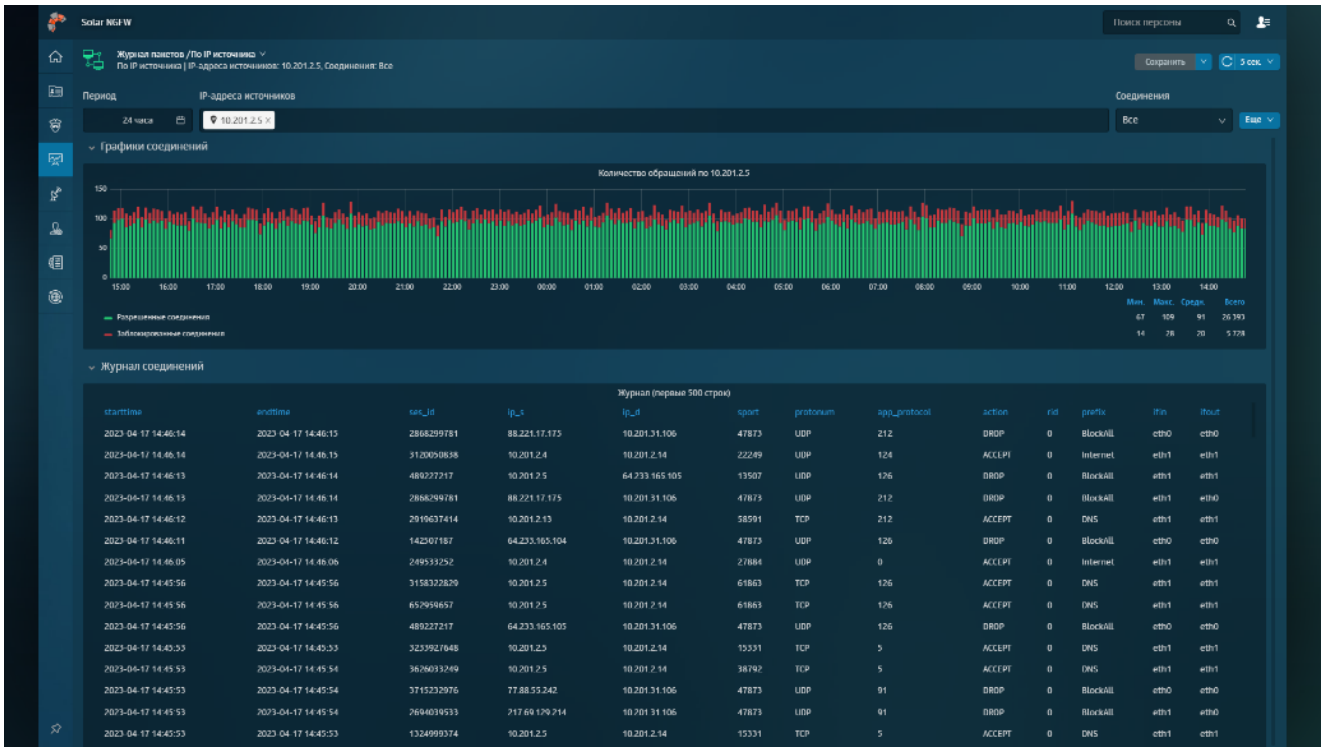

Рисунок 6. Интерфейс Solar NGFW. Журнал статистики по IP источника

3. ПРЕИМУЩЕСТВА

Высокая производительность и подтвержденная надежность решения, дополненные удобством использования, профессиональной поддержкой и уникальными сигнатурами IPS от Solar 4RAYS, позволяют Solar NGFW полноценно решать задачи крупного бизнеса и корпораций.

- ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

  В отличие от большинства российских конкурентов, архитектура Solar NGFW изначально создавалась с учетом нагрузок крупного бизнеса. Это большое преимущество, так как изменение архитектуры решения – один из самых болезненных и дорогостоящих процессов в разработке и обслуживании продукта и сильно замедляет его дальнейшее развитие.

  Производительность программной версии Solar NGFW может достигать 20 Гбит/с в режиме межсетевого экрана и 4 Гбит/с в режиме NGFW (со всеми включенными функциями FW, IPS, DPI и журналирование). Такая скорость виртуального исполнения позволяет решить задачи большинства крупных компаний.

  Для программно-аппаратного исполнения доступны скорости до 40 Гбит/с в режиме межсетевого экрана. А в 2025 году планируется переход на обновленную архитектуру второго поколения, которая увеличит возможности пропускной способности до 100 Гбит/с.

  Замеры и тестирования, при которых были достигнуты эти показатели, производились по собственной методике, которая, в отличие от данных многих конкурентов Solar NGFW, полностью прозрачна и доступна для ознакомления на сайте.

- УНИКАЛЬНЫЕ СИГНАТУРЫ IPS ОТ SOLAR 4RAYS

  Кроме стандартного набора распространенных сигнатур IPS в Solar NGFW используются уникальные сигнатуры от центра исследования киберугроз Solar 4RAYS, обладающего крупнейшей TI-базой киберугроз в РФ, пополняемой в том числе из данных об инцидентах, зафиксированных Solar JSOC – коммерческим SOC № 1 в России. Эксперты центра анализируют более 180+ млрд событий в сутки от 250 крупных коммерческих и государственных клиентов.

  Выявленные кибератаки на любого из клиентов Solar JSOC и Solar MSS вносятся в базу киберразведки (Thread Intelligence, TI). На ее основе создаются собственные сигнатуры, дающие возможность обнаруживать и предотвращать сетевые атаки, которые еще неизвестны другим производителям NGFW и IPS. У экспертов Solar 4RAYS есть 24 часа, за которые они должны гарантированно подготовить средства противодействия.

- УДОБНЫЙ И ПОНЯТНЫЙ ВЕБ-ИНТЕРФЕЙС

  Взаимодействие с Solar NGFW происходит через единую консоль управления, доступную из любого браузера без установки дополнительного ПО. Она устроена как ситуационный центр и позволяет в едином окне оперативно оценить обстановку и выделить приоритетные направления работы без необходимости обращаться к нескольким консолям. Интерфейс системы сделан с уважением к администраторам, их задачам и времени, поэтому рутинные операции максимально автоматизированы, а для использования продукта не требуется проходить сложное обучение, так как в каждом разделе встроена интерактивная справка с примерами настроек, что позволяет быстро разобраться и приступить непосредственно к задачам по защите корпоративной инфраструктуры.

  И, наконец, это просто удобно и красиво.

- ВИРТУАЛЬНОЕ ИЛИ ПРОГРАММНО-АППАРАТНОЕ ИСПОЛНЕНИЕ

  Solar NGFW может поставляется в виде виртуальной машины (RUN-файл). Виртуальное исполнение

дает независимость от конкретных аппаратных платформ и простую масштабируемость, а также позволяет снизить стоимость решения и использовать существующие вычислительные ресурсы. Поддерживаются среды виртуализации VMware, Microsoft Hyper-V, OpenStack
Для заказчиков, которые не могут использовать виртуальное исполнение, в мае 2024 года были представлены программно-аппаратные комплексы (ПАК) среднего (до 20 Гбит/с) и высокопроизводительного (до 40 Гбит/с) сегмента. Подробная информация о характеристиках модельного ряда доступна на сайте.

- СТАБИЛЬНОСТЬ И ОТКАЗОУСТОЙЧИВОСТЬ
  Технологической основой для создания Solar NGFW стал высокопроизводительный шлюз веб-безопасности Solar webProxy, развивающийся более 10 лет. Применение отработанных технологий гарантирует надежность Solar NGFW при решении задач в высоконагруженных проектах и придает ему дополнительную технологическую зрелость.

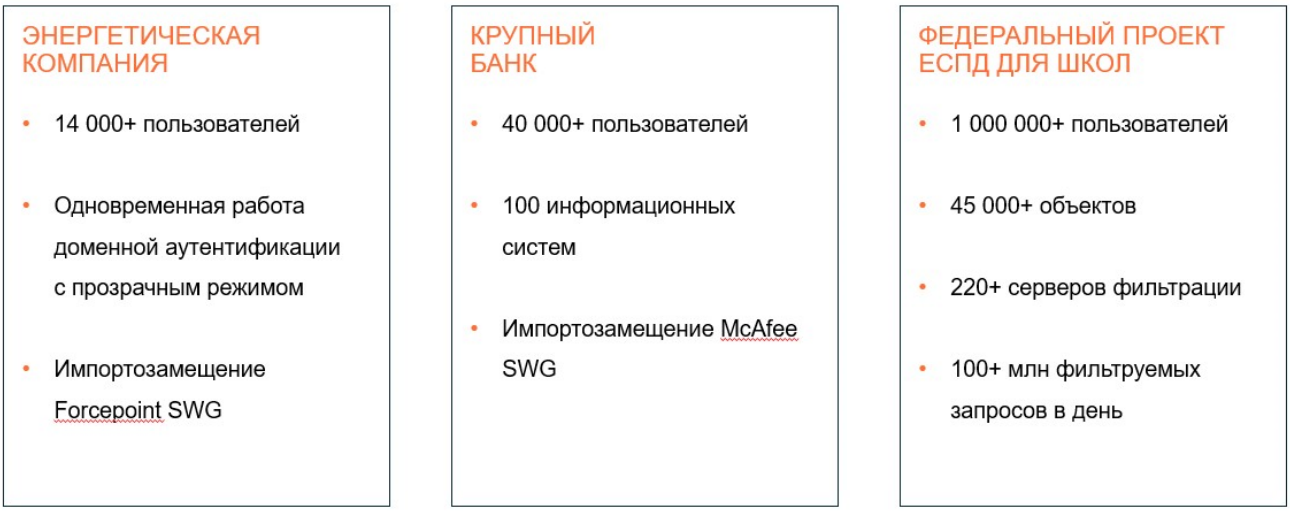

Рисунок 7. Примеры реализованных проектов Solar webProxy

- ВСТРОЕННАЯ СИСТЕМА ОТЧЕТОВ
  В Solar NGFW есть встроенная система аналитики и отчетности. С ее помощью можно за несколько кликов получить визуализированный срез данных, который затем можно импортировать в PDF или распечатать.
  Сами отчеты интерактивны и позволяют менять параметры выборки данных прямо на дашбордах, а также «спускаться» от агрегированных показателей к «сырым» данным. В поставку включены типовые шаблоны отчетов, которые можно донастраивать либо на их основе создавать собственные шаблоны.

- ДОСЬЕ НА СОТРУДНИКА
  В Solar NGFW реализована уникальная функция, отсутствующая у конкурентов, – «Досье на сотрудника». С ее помощью в реальном времени накапливается вся необходимая информация об использовании веб-ресурсов конкретным сотрудником. Обновление данных происходит в реальном времени.
  Это дает офицеру безопасности возможность работать с конкретными сотрудниками, а не с технической информацией (идентификаторы, адреса и т. д.), которые обычно разрозненны и не всегда очевидны. Такой «человекоцентричный» подход применяется и в других продуктах компании.
  Также можно интегрировать досье Solar NGFW с досье DLP-системы Solar Dozor.

- ВОЗМОЖНОСТИ ИНТЕГРАЦИИ

  Solar NGFW поддерживает взаимодействие по протоколу ICAP с дополнительными средствами защиты, которые уже могут быть внедрены у заказчика. Например, антивирус, песочница, DLP-система. Поддержка syslog позволяет передавать данные в SIEM-системы.

  Возможна нативная интеграция Solar NGFW с DLP-системой Solar Dozor. Она обеспечивает синхронизацию досье сотрудника в двух продуктах, автоматическое блокирование утечек через веб-канал согласно единой политике безопасности DLP, а также предотвращение утечек из внутренних корпоративных веб-ресурсов с помощью функций реверс-прокси.

- ГОТОВ К ИМПОРТОЗАМЕЩЕНИЮ

  Solar NGFW разработан в России и зарегистрирован в Едином реестре отечественного ПО. В качестве базовой ОС используется Astra Linux SE. Ведутся работы по сертификации продукта в системе ФСТЭК России.

  За 2022-23 год нами накоплен большой опыт по замещению иностранных SWG в нескольких корпорациях на примере Solar webProxy, который стал технологической основой Solar NGFW. Квалифицированные специалисты внедрения и техподдержки могут сопровождать заказчика в режиме 24/7 на всей территории страны.

4. СПЕЦИФИКАЦИЯ

Класс решения	NGFW (Next Generation Firewall)
Исполнение	Программное и аппаратное
Базовая операционная система	Astra Linux SE (не входит в комплект поставки)
Способ установки виртуального исполнения продукта	RUN-файл
Поддержка виртуализации	VMware Microsoft Hyper-V OpenStack
ПРОИЗВОДИТЕЛЬНОСТЬ	
Производительность FW, Мбит/с (UDP 1518 байт)	До 40 000
Производительность IPS, Мбит/с (с включенными сигнатурами, 24 тыс., TCP)	До 20 000
Максимальное число одновременных сессий (MCC)	До 1 000 000
Максимальное число сессий в секунду (CPS)	До 100 000
КОМПОНЕНТЫ ЗАЩИТЫ	
Межсетевой экран	Есть
Система предотвращения вторжений (IPS)	Есть
Система контроля приложений (фильтрация трафика по приложениям, DPI)	Есть

Количество поддерживаемых прикладных протоколов (контроль приложений, DPI)	342
Антивирус	Есть
Веб-прокси, обратный прокси	Есть
Система фильтрации почтового трафика	Нет
Remote Access VPN	Планируется в релизе 2025 года
Site-to-site VPN	Планируется в релизе 2025 года
Шифрование ГОСТ	Нет
Фильтрация трафика по URL адресам и категориям веб-ресурсов	Есть
SSL-инспекция	Вскрытие SSL
Категоризатор веб-ресурсов	Есть, модуль Solar webCat
Аутентификация пользователей	Есть (для функции контентной фильтрации)
Методы аутентификации	По IP-адресам, Kerberos (Negotiate), NTLM, NTLM + Negotiate, Basic, прозрачная аутентификация

СЕТЕВЫЕ ВОЗМОЖНОСТИ

Статическая маршрутизация	Есть
Динамическая маршрутизация	Есть
Поддержка технологии NAT (Source NAT, Destination NAT и PAT)	Есть
Multi-WAN	Планируется в релизе 2025 года
Поддержка Policy-based routing	Планируется в релизе конца 2024 года

Поддержка QoS	Планируется в релизе 2025 года
Поддержка VLAN	Есть
Поддержка Geo-IP	Планируется в релизе конца 2024 года
Агрегация каналов (LACP и другие)	Есть
Поддержка Multicast	Нет
Поддержка IPv6	Нет
Поддержка NetFlow	Нет
Поддержка Syslog	Есть
Поддержка ICAP	Есть
Поддержка протоколов АСУ ТП	Нет
Безопасная публикация ресурсов и сервисов	С помощью обратного прокси

ИНТЕГРАЦИЯ И ВЗАИМОДЕЙСТВИЕ С СИСТЕМАМИ ОКРУЖЕНИЯ

С Microsoft Active Directory	Есть
С другими средствами защиты	по ICAP
С SIEM системами	по Syslog
В экосистеме вендора	Solar webProxy Solar Dozor

УПРАВЛЕНИЕ

Интерфейс управления	Веб-интерфейс SSH
Централизованное управление	Планируется в релизе конца 2024 года
Безопасный доступ в веб-интерфейс управления по HTTPS	Есть

Ролевая модель доступа администраторов	Есть
Мультифакторная аутентификация	Нет
Журналирование срабатывания правил	Есть
Журналирование пользовательской активности	Есть
Журналирование действий администраторов	Есть
Экспорт журналов	Есть
Выгрузка отчетов	Есть, в PDF
Отправка отчетов	По расписанию
Оповещения	Есть, в интерфейсе и по e-mail
Формирование досье пользователя	Есть
Управление резервными копиями	Нет
МОНИТОРИНГ	
В режиме реального времени	Есть
Собственных показателей работоспособности	Есть
Нагрузки на NGFW	Есть
Состояния ОС	Есть
Сетевой активности пользователей	Есть
Мониторинг по SNMP	Планируется в релизе конца 2024 года
ОТКАЗОУСТОЙЧИВОСТЬ	
Кластер отказоустойчивости (Active-Passive)	Есть

Балансировка	Есть, поддерживается внешний балансировщик

СЕРТИФИКАЦИЯ И ЛОКАЛИЗАЦИЯ

Техническая поддержка на русском языке от вендора	Есть
Техническая поддержка 24/7	Есть
Актуальная документация на русском языке	Есть
Демо-стенд	Доступ в рамках пилотного проекта
Внесен в Реестр отечественного ПО	В процессе регистрации
Сертификация ФСТЭК России	Планируется по УД4, ИТ.МЭ.А4.ПЗ, ИТ.СОВ.С4.ПЗ в Q4 2024
Сертификация ФСБ России	Нет
Сертификаты ЕАЭС	Нет

5. ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС

В модельный ряд Solar NGFW входят три устройства в форм-факторе 1U 19” для решения задач заказчиков с самой разной корпоративной инфраструктурой.

- SOLAR NGFW L 2000

  Подходит для небольших организаций или филиалов.
- SOLAR NGFW XL 4000

  Подходит для обеспечения безопасности организаций enterprise-уровня.
- SOLAR NGFW XXL 10000

  Подходит для обеспечения защиты передачи данных между ЦОД.

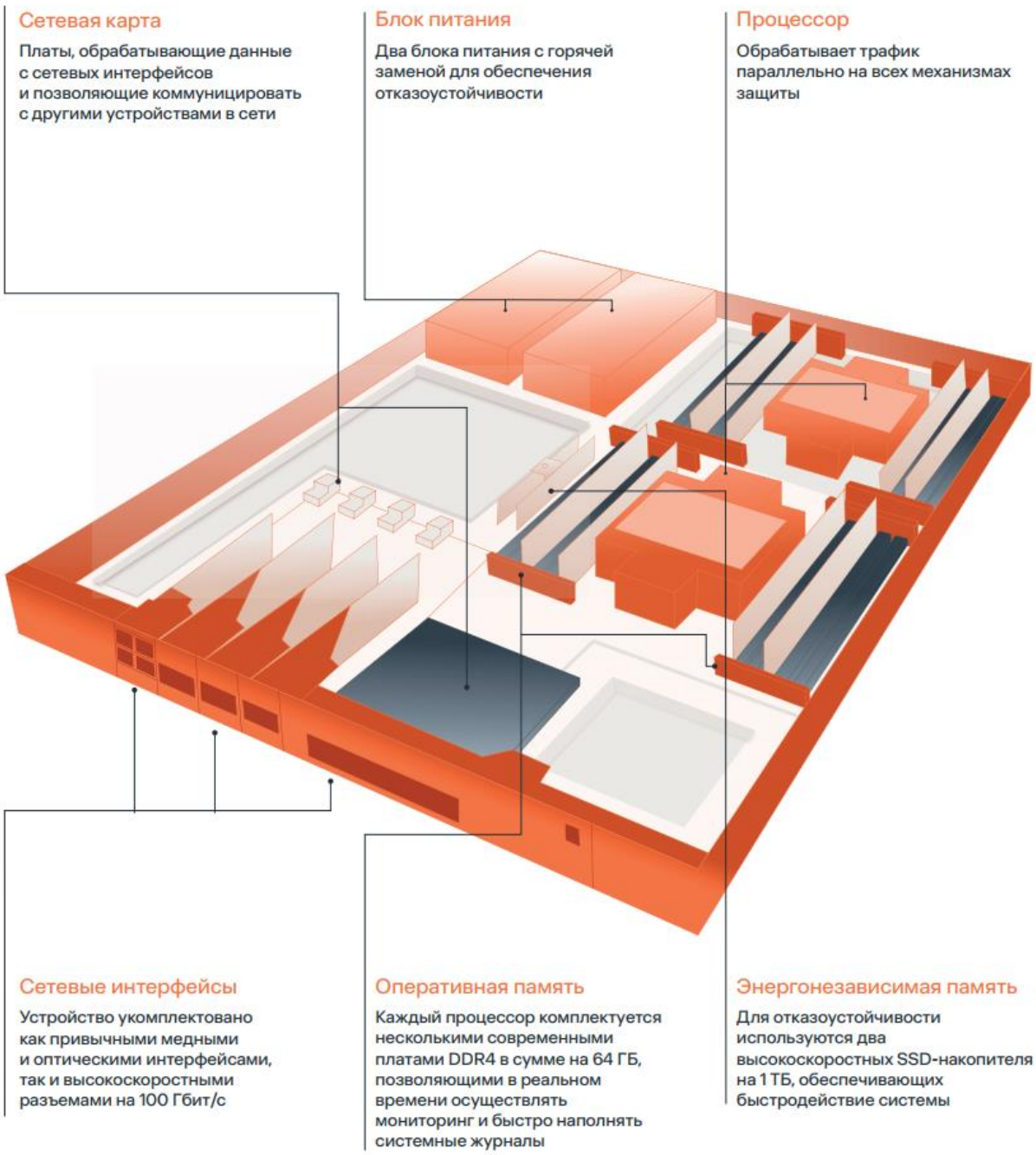

Рисунок 8. Устройство ПАК Solar NGFW

О ГРУППЕ КОМПАНИЙ «СОЛАР»

Группа компаний «Солар» — ведущий поставщик решений кибербезопасности в России, архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солара» – более 850 крупнейших компаний России. Продукты и сервисы «Солара» объединены в домены экспертизы: Безопасная разработка программного обеспечения, Управление доступом, Защита корпоративных данных, Детектирование угроз и хакерских атак. Домены экспертизы закрывают все потребности заказчиков и включают собственные разработки, решения партнеров, услуги по созданию стратегии и архитектуры ИБ, консалтинг, обучение персонала.

Компания предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие.

ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир». Работа центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности.

Группа компаний «Солар» инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита. Совместно с Минцифры реализует всероссийскую программу кибергигиены, направленную на повышение цифровой грамотности населения.

Штат компании — более 1 800 специалистов. Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.

КОНТАКТНАЯ ИНФОРМАЦИЯ

ТЕЛЕФОНЫ:

+7 (499) 755-07-70 – продажи и общие вопросы

+7 (499) 755-02-20 – техническая поддержка

E-MAIL:

solar@rt-solar.ru – продажи и вопросы по сервису

support@rt-solar.ru – техническая поддержка

АДРЕСА:

- Москва, Никитский пер., 7, стр. 1
- Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд
- Нижний Новгород, Казанское ш., 25, корп. 2
- Самара, Молодогвардейская ул., 204
- Ростов-на-Дону, Доломановский пер., 70Д
- Хабаровск, ул. Серышева, 56