positive technologies

ИСТОРИЯ УСПЕХА

PT NGFW защищает сетевую инфраструктуру Карачаровского механического завода

Производительность:
до 10 Гбит/с

Отрасль:
машиностроение

Решение:
PT NGFW 2050, 2010, 1050

Срок внедрения:
4 месяца

ПАО
КАРАЧАРОВСКИЙ
МЕХАНИЧЕСКИЙ ЗАВОД
ОСНОВАН В 1950 ГОДУ

«Карачаровский механический завод» один из ведущих российских производителей лифтового и подъёмно-транспортного оборудования. КМЗ является предприятием, которое входит в структуру Правительства Москвы. Это накладывает на компанию высокие обязательства по надежности и безопасности инфраструктуры, а также определяет стратегический вектор на приоритетное использование отечественных технологических решений.

Прежнее зарубежное решение по защите сети перестало справляться с реальными задачами крупного предприятия. Базовой маршрутизации и фильтрации трафика было недостаточно. В этот момент компания выбрала новый путь — PT NGFW от Positive Technologies. Это позволило реализовать производительную систему сетевой защиты с поддержкой глубокой инспекции трафика и механизмов предотвращения вторжений.

Евгений Белов
заместитель генерального директора по безопасности

«До внедрения PT NGFW нам хотелось бы улучшить сразу несколько направлений: повысить отказоустойчивость инфраструктуры, усилить защиту периметра и получить инструменты для контроля аномалий. Все они решены в полной мере, и с хорошим заделом на дальнейшее развитие».

Задача

Изменение ландшафта киберугроз и стремительный рост объёмов данных поставили перед КМЗ задачу внедрения современного межсетевого экрана нового поколения (NGFW). Новое решение должно было обеспечить надёжную защиту распределённой инфраструктуры.

Евгений Белов
заместитель генерального директора по безопасности

«Мы искали решение, которое могло бы нам обеспечить отказоустойчивость и надежную защиту периметра, а в перспективе еще возможность детального анализа данных и контроль аномалий».

Перед командой стояли конкретные вызовы:

1. Обеспечить защиту периметра — детальный контроль передаваемых данных и высокое качества обнаружения атак.
2. Гарантировать отказоустойчивость — крупное промышленное предприятие не может позволить даже минутного простоя инфраструктуры, поэтому требовалось обеспечить возможность автоматического переключения в случае аварии на резервный узел или канал за время менее секунды, без потери данных или разрыва пользовательских сессий.
3. Перейти на отечественный продукт в соответствии со стратегией импортозамещения.
4. Построение защищенных туннелей для передачи данных между объектами инфраструктуры.
5. Заложить фундамент для развития с расчётом внедрения Remote Access VPN для удаленных пользователей.

Выбор решения

Команда КМЗ подошла к выбору системно. Рассматривались несколько российских решений, а также параллельно анализировались мировые лидеры как ориентиры зрелости.

Евгений Белов
заместитель генерального директора по безопасности

«На российском рынке нет ни одного полностью готового, отработанного решения с многолетней экспертизой. Все решения — развивающиеся. Но если рассматривать именно российские продукты, мы пришли к выводу, что на сегодняшний день самое сильное ускорение — у Positive Technologies».

В финальный шорт-лист вошли два российских решения, включая PT NGFW. Выбор в пользу Positive Technologies был сделан по совокупности факторов:

- Собственная высокоскоростная архитектура.
  Уникальная архитектура продукта позволяет PT NGFW показывать выдающиеся данные производительности даже на младших моделях.
- Стабильный Site-to-Site VPN с балансировкой по ядрам.
  Для КМЗ это был ключевой момент в выборе: у конкурирующего продукта данная функция показывала низкие цифры производительности, так как весь трафик обрабатывался только одним ядром процессора.
- Доверие к команде разработки и прозрачная дорожная карта.
  На протяжении последнего года разработка PT NGFW демонстрировала высокую скорость выпуска новых функций и выдерживала данные рынку обязательства.
- Результаты пилота.
  Несмотря на то, что тестировались ещё относительно ранние версии, в ходе пилота был отмечен технологический потенциал PT NGFW.

Евгений Белов
заместитель генерального директора по безопасности

«Финально, при выборе решения, мы руководствовались мощью команды разработки, силой бренда, собственным ядром. В ходе пилотного тестирования, решение показало себя хорошо, хотя мы пилотировали достаточно раннюю версию. Тем не менее, пройти пилотное тестирование с хорошим результатом — этим не каждый зрелый продукт может похвастаться, а PT NGFW справился очень достойно».

Архитектура решения

Для КМЗ была спроектирована трёхуровневая отказоустойчивая архитектура с разделением функциональных ролей между моделями PT NGFW.

PT NGFW 2050 — ядро сети. Два устройства в кластере взяли на себя роль ядра инфраструктуры: терминирование подключений, циркуляция трафика, формирование основных политик безопасности.

PT NGFW 2010 — периметр и связь между площадками. Кластер из двух устройств обеспечивает выход пользователей в Интернет, Site-to-Site VPN-туннели площадками и фильтрацию данных.

PT NGFW 1050 — задел на будущее. Отдельный кластер для терминирования Remote Access VPN подключения для удалённых пользователей.

Евгений Белов
заместитель генерального директора по безопасности

«IPSec в PT NGFW работает стабильно, что является важным преимуществом в условиях распределённой инфраструктуры».

Процесс внедрения

Миграция со старой инфраструктуры — испытание для любой сети. КМЗ не стал исключением, поэтому процесс миграции стал длительным и постепенным, однако достаточно предсказуемым.

Евгений Белов
заместитель генерального директора по безопасности

«Сложно. Даже при идеально описанных правилах одна система межсетевого экранирования отличается от другой. Не могу сказать, что это лёгкая задача. Но технологических ограничений мы не встречаем. Мы видим, как это работает, и постепенно переносим настройки».

Проект прошёл все классические этапы: разработка и согласование архитектуры, пусконаладка, переключение трафика, тестирование в эксплуатации и корректировка настроек. Благодаря тщательной предварительной подготовке, переключение трафика прошло в согласованное технологическое время, практически незаметно для инфраструктуры. На сегодняшний день развёрнуты и активно используются:

- Правила межсетевого экранирования
- Пакетная фильтрация трафика
- IPS: предотвращение вторжений
- Application Control:определение приложений в трафике
- Централизованное журналирование событий безопасности
- Site-to-Site VPN с балансировкой между площадками

Отдельно отмечено качество и скорость работы технической поддержки Positive Technologies.

Евгений Белов
заместитель генерального директора по безопасности

«Мы определённо видим преимущество российского решения в том плане, что есть очень оперативная поддержка решения наших вопросов. Мы понимаем, что даже в случае выхода из строя «железок» или их некорректной работы, нам активно и быстро помогут. Мы убедились в этом на практике, когда возникали определённые проблемы. Они были оперативно решены, т.к. техническая поддержка PT NGFW работает очень грамотно, инженеры компетентны».

Результат: «не на бумаге, а в жизни»

Завод получил именно то, что искал: надежную защиту периметра и гарантированную отказоустойчивость.

Сегодня инфраструктура КМЗ строится на трехуровневой архитектуре PT NGFW, где каждое семейство устройств решает свою задачу. Это позволило объединить объекты в защищенную систему с высокой пропускной способностью и балансировкой нагрузки.

По сравнению с ранее используемым оборудованием, решение класса NGFW обеспечило более высокий уровень контроля трафика и снизило риски компрометации информационных систем предприятия.

Но, пожалуй, главным результатом стало не только техническое решение, а опыт работы с вендором, который держит слово:

Евгений Белов
заместитель
генерального директора
по безопасности

«Вот это наглядное преимущество — не на бумаге, а в жизни. Как выбрать отечественный продукт с высоким SLA и понятной сервисной базой».

О Positive Technologies

Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят ущерб бизнесу и целым отраслям экономики.

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.

Технические характеристики

Карта развития продукта

Чат продукта

Тест-драйв