# 10 советов для крупных организаций

Как избежать подводных камней при внедрении NGFW

rt-solar.ru
rt.ru

Ростелеком
Солар

# 10 Советов для крупных организаций

## Как избежать подводных камней при внедрении NGFW

**NGFW — оптимальное решение для защиты крупного бизнеса от киберугроз. Внедрение современного российского межсетевого экрана нового поколения позволяет значительно уменьшить риски инцидентов, повысить защищенность и обеспечить соответствие законодательству. Это напрямую влияет на устойчивость бизнеса в условиях социальной и экономической неопределенности.**

Внедрение NGFW — сложный процесс для ИТ-, ИБ- и смежных с ними подразделений. Требования к экспертизе высоки, а ошибка может привести к неизмеримым финансовым и репутационным потерям.

В этом материале расскажем о том, как минимизировать риски при внедрении межсетевого экрана нового поколения — при переходе со старого решения или во время внедрения с нуля.

### Важно знать

Next Generation Firewalls (NGFW) — межсетевые экраны с технологией глубокого анализа пакетов, способные выйти за рамки стандартной проверки/блокировки IP-адресов, портов и протоколов, исследуя трафик уровня приложений, предотвращая вторжения, а также используя внешние данные о киберугрозах.

Источник: глоссарий Gartner, апрель 2023

## Проведите аудит

- [ ] Оценка текущих мер безопасности
- [ ] Анализ угроз и рисков
- [ ] Систематизация используемых протоколов
- [ ] Систематизация политик безопасности

Часть из этого уже должна быть реализована в крупной организации, а что-то может быть уникальным именно для вас. В любом случае на первом этапе нужно определить основные инфраструктурные, операционные и финансовые «бутылочные горлышки» и особенности вашей организации, которые могут повлиять на процесс.

Будет правильным подойти к этому вопросу вооружившись инструментами управления — и относиться к внедрению NGFW как к запуску нового процесса внутри экосистемы информационной безопасности. В частности, не забывайте обо всех заинтересованных сторонах (воспользуйтесь матрицей RACI [1]), определите, как вы будете оценивать результаты внедрения, задайте параметры финансового обоснования исходя из лимитов по CAPEX и желаемой окупаемости вашего NGFW. Это поможет не только вовлечь в процесс всех стейкхолдеров, но и грамотно выстроить отношения с вендором.

[1] Responsible, Accountable, Consulting, Informed — инструмент для управления отношениями в команде; это таблица, с помощью которой распределяют ответственность, полномочия и роли.

## Определитесь с требованиями и целями

1. Определите цели и задачи, которые планируете решить с помощью межсетевого экрана. Например, обеспечить защиту периметра, заменить существующие средства сетевой защиты (прокси-серверы, устаревшие межсетевые экраны), контролировать трафик внутри сети.

2. После этого вам необходимо рассмотреть необходимый набор функций, включающий, к примеру, систему обнаружения вторжений, фильтрацию веб-трафика, защиту от вредоносного ПО и глубокий анализ пакетов.

3. Также оцените специфические требования к производительности и соответствию стандартам безопасности, если, к примеру, ваша организация является частью КИИ, работает с персональными данными или государственной тайной.

## Соберите информацию о рынке

**Что оцениваем?**

- [ ] Репутацию поставщика
- [ ] Отзывы пользователей
- [ ] Техническую поддержку
- [ ] Подход поставщика к обновлениям
- [ ] Особенности лицензирования

В свою очередь, анализ технической документации поможет оценить, насколько выбранное решение подходит для ваших запросов и сетевой инфраструктуры. Собранную информацию переведите в числовой вид для удобства определения наилучшего соотношения «цена/качество». На этом этапе может возникнуть ситуация, когда ваши технические возможности будут сильно отличаться от требований к инфраструктуре — в таких случаях советуем сделать выбор в пользу провайдеров облачных решений, которые предоставляют свои вычислительные мощности, например, таких как Solar MSS.

## Создайте план

**Что планируем?**

- [ ] Установку и настройку NGFW
- [ ] Согласование необходимых для работы доступов
- [ ] Регламентацию процессов взаимодействия ИТ- и ИБ-отделов
- [ ] Интеграцию с текущими системами безопасности
- [ ] План переноса политик

Мы рекомендуем при проработке плана переноса политик уделять внимание их оптимизации, ведь это позволяет в разы повысить удобство работы с системой. В плане обязательно должны быть контрольные точки, которые помогут вам корректно оценивать ход пилотирования и внедрения.

## Обучите

- Подготовьте персонал к работе, проведя его обучение самостоятельно или при поддержке вендора. Лекции и вебинары должны включать в себя как общие принципы работы NGFW, так и конкретные задачи по управлению, настройке и обслуживанию системы. Рекомендуем уделить внимание практической работе с системой
- Запросите записи лекций и вебинаров для адаптации сотрудников, которые не пройдут обучение у заказчика

**Важно знать**

Большинство клиентов не берут на себя риск самостоятельного обучения, так как администраторам важно понимание функций «под капотом». Обучение заказчика, организованное вендором, должно обязательно входить в базовый пакет услуг.

## Настройте, пропилотируйте, внедрите

- Первый этап состоит из настройки всех функций NGFW, интеграции его с существующими системами и подготовки к запуску в рабочей среде
- Второй этап должен включать создание и применение политик безопасности, управление доступом и настройку функций обнаружения и предотвращения угроз
- Отдельное внимание уделите сетевой составляющей: откройте все необходимые доступы и подготовьте схему инфраструктуры

## Протестируйте и проверьте

- Функциональное тестирование
- Нагрузочное тестирование

Эти тесты дадут возможность убедиться, что новая система успешно защищает вашу сеть от угроз (для понимания, выдерживает ли система необходимую скорость обработки трафика).

Такой подход поможет выявить и исправить любые уязвимости или скорректировать мощности перед полным развертыванием системы. Такие меры часто помогают сэкономить бюджет. Обязательно учитывайте ваши требования к кластеризации, балансировке и будущему масштабированию системы, чтобы предвосхитить будущие требования и провести эффективное тестирование.

## Мониторьте и управляйте

После развертывания NGFW важно обеспечить непрерывное отслеживание его работы и эффективности. Это включает в себя выявление угроз, анализ трафика и проведение регулярных проверок безопасности. Большинство крупных компаний отдают предпочтения решениям, которые интегрируются (например, по протоколу SNMP или syslog) с системами для централизованного мониторинга, например, с такими как Zabbix.

## Обновляйтесь и пользуйтесь поддержкой

Важно поддерживать NGFW в актуальном состоянии с последними обновлениями, сигнатурами и патчами. Регулярное обновление и обслуживание системы помогают обеспечить ее долгосрочную эффективность и защиту от новых угроз.

# Анализируйте и улучшайте

Оценивайте эффективность системы на основе собранных данных и обратной связи от пользователей. Используйте эту информацию для постоянного улучшения решения и оптимизации того, что можно усовершенствовать, — и для предоставления качественной обратной связи производителю системы, включая:

- Регулярный анализ угроз
- Оценку эффективности политик безопасности
- Исправление любых выявленных проблем

Мы также рекомендуем создавать отчетность по выявленным угрозам в переложении на финансовые показатели. Подобная аналитика поможет вам точнее оценить окупаемость текущего решения и в дальнейшем уверенно закладывать бюджет на новые.

---

# Solar NGFW

Solar NGFW – программный межсетевой экран нового поколения для крупных компаний с централизованным выходом в интернет.

**4 Гбит/с в режиме NGFW**

**Сигнатуры IPS от Solar JSOC**

**Современный интерфейс**

Для консультации и получения дополнительной информации оставьте заявку на нашем сайте.

Оставить заявку

Ростелеком
Солар

rt-solar.ru
rt.ru

**Email:**

solar@rt-solar.ru
support@rt-solar.ru

Телефоны:

+7 (499) 755-07-70 — продажи и общие вопросы
+7 (499) 755-02-20 — техническая поддержка

Адреса

125009, Москва, Никитский пер., 7, стр. 1
127015, Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд