СОЛАР

Solar Next Generation Firewall

Методика тестирования

Версия 1.0

МОСКВА, сентябрь 2023

Содержание

Общие данные о продукте

Solar NGFW — программный межсетевой экран нового поколения для комплексной защиты локальной корпоративной сети от сетевых угроз и вредоносного ПО, а также контроля доступа к веб-ресурсам.

Solar NGFW обладает следующими функциональными возможностями:

- Межсетевой экран (FW) — фильтрация трафика на основе IP-адресов и портов.
- Трансляция IP-адресов (NAT) — сокрытие внутренних IP-адресов от возможных злоумышленников.
- Система предотвращения вторжений (IPS) — сигнатурное обнаружение и блокирование сетевых атак.
- Глубокий анализ трафика (DPI) — контроль трафика приложений.
- Веб-прокси — расшифровка и проверка HTTPS-трафика, передача его другим средствам защиты по протоколу ICAP.
- Обратный прокси — контроль доступа удаленных сотрудников к корпоративным веб-ресурсам.
- Категоризатор веб-ресурсов — каталогизирование информации о назначении веб-ресурсов и их опасности для пользователей.
- Аутентификация и авторизация — определение личности пользователя и его прав.

1. Цели и задачи

Объект тестирования

Программное обеспечение Solar NGFW.

Цель тестирования

Получение данных о производительности объекта тестирования в смоделированных условиях, приближенных к реальным инфраструктурам заказчиков «Солара», и публикация описания хода работ на продуктовой странице на официальном сайте компании.

Данная методика является первой версией, и с последующими релизами планируется ее обновление. Задачей первого этапа было определение максимальной производительности программного Solar NGFW при разных включенных модулях: FW, IPS, DPI. На следующих этапах планируется добавление тестов для других модулей, а также испытаний с различными генераторами трафика.

Задачи тестирования

1. Определение максимальной пропускной способности.

   Убедиться, что Solar NGFW достигает заявленных значений в разных режимах: 20 Гбит/с в режиме FW и 4 Гбит/с в режиме NGFW (FW+IPS+DPI).

2. Оценка длительности работы.

   Убедиться, что Solar NGFW может работать стабильно в течение длительного времени без потери производительности.

3. Выявление оптимальных значений — количество новых соединений (CPS) и количество одновременных соединений (CC).

   Провести ряд тестов, последовательно увеличивая или делая корректировку, для выявления оптимального значения.

4. Оценка поведения системы при изменении условий.

   Определение характеристик CPS и CC при изменении различных параметров Solar NGFW: включенных модулей безопасности (FW, DPI, IPS) и используемых ядер.

2. Оборудование для тестирования

Объект тестирования — Solar NGFW — установлен на аппаратной серверной платформе в ОС Astra Linux 1.7.3, аппаратные характеристики приведены в таблице 1.

Таблица 1. Аппаратные характеристики серверной платформы

Параметр	Модель	Характеристики
Процессор	Intel Xeon Silver 4210R, 2 шт.	2,4 ГГц, 40 vCPU
Запоминающее устройство	INTEL SSDSC2KG96, 1 шт.	1 ТБ
Оперативная память	DDR4 32GB Micron MTA18ASF4G72PDZ-3G2, 2 шт.	DDR4 64 ГБ
Сетевые карты	Intel Ethernet Connection X722, 2 шт.	10 GbE SFP+

Тестирование выполняется на лабораторном стенде с использованием генератора трафика Ixia Breaking Point, имитирующего реальный легитимный трафик, на базе аппаратной платформы Ixia PerfectStorm (далее — Ixia).

В ходе тестирования Ixia генерирует и направляет на объект тестирования трафик. По сети управления исключено прохождение трафика, предназначенного для нагрузки. Схема подключения представлена ниже.

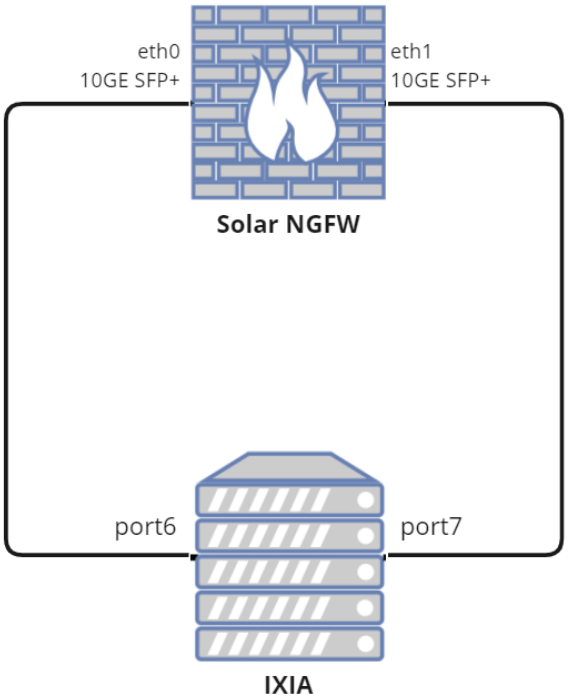

Рисунок 1. Физическая схема сети для нагрузочного тестирования

3. Подготовительные тестирования

Подготовительное тестирование необходимо для выявления характеристик, которые будут использованы в качестве максимальных для нагрузочных тестов в разделах 4–6. Данные тестирования выполняются с включенными модулями FW+IPS+DPI.

Таблица 2. Конфигурация параметров TCP-стека на генераторе трафика

Maximum Segment Size (MSS)	Максимальный размер сегмента	1460
Retry Quantum	Интервал в миллисекундах между повторными попытками отправки	500
Retry Count	Количество попыток отправки до того, как соединение будет признано неудачным и сброшено	5
Initial Receive Window	Размер окна приема в байтах для нового соединения	5792
TCP Keepalive Timer	Таймер до отправки пакета TCP Keepalive	0

3.1. Тестирование на определение максимального количества новых соединений в секунду (CPS) в режиме FW+DPI

Задача теста — подтвердить соответствие целевому значению количества соединений, которые Solar NGFW может принять на анализ ежесекундно (100 000 cps).

Примечание: Solar NGFW является гибкой системой, поддерживающей различные платформы. В данном тесте, помимо подтверждения соответствия целевым показателям в условиях, описанных на сайте, приводится общая методика определения максимального значения. Эта методика рекомендуется для выявления характеристик Solar NGFW на оборудовании заказчиков в конфигурациях, отличных от использованных для тестирования.

Таблица 3. Тестирование на определение максимального количества новых соединений в секунду

Настройки NGFW	Включены функции FW, DPI со следующими характеристиками: • Включены 1000 правил FW с анализом приложений • Журналирование включено для всех правил
Особенности трафика	Для тестирования используются соединения вида: • TCP SYN — SYNACK • TCP ACK • HTTP 1.0 GET (No Compression) • TCP FIN

	• TCP FINACK • TCP ACK Соединения устанавливаются в одном направлении
Методика тестирования	Начальная скорость создания/удаления соединений — 10 000 cps (далее — CPS_1). В качестве максимальной скорости (далее — CPS_2) выбрано значение 110 000 cps. Порядок проверок: 1) Запустить тестирование со скоростью создания/удаления соединений CPS_1. В ходе тестирования разрешены TCP Retransmit, однако TCP Reset недопустимы. Средствами мониторинга системы снимать показатели количества соединений и загруженности ресурсов. 2) Через 100 секунд остановить тест. Зафиксировать результат. 3) Произвести анализ статистики: a. Если потерь соединений нет, и разница между CPS_2 и CPS_1 меньше или равна 10 000, то прекратить тестирование и принять CPS_1 в качестве результата теста. b. Если потерь соединений нет и разница между CPS_2 и CPS_1 больше 10 000, увеличить CPS_1 до $\frac{CPS\_2 + CPS\_1}{2}$ и перейти к шагу 1. c. Если обнаружены ошибки при установлении соединений, уменьшить CPS_2 до $\frac{CPS\_2 + CPS\_1}{2}$ и перейти к шагу 1. Провести 3 проверки. Убедиться в стабильности результата
Ожидаемый результат	Solar NGFW поддерживает создание и удаление соединений на скорости до 100 000 cps
Полученный результат	• Целевое значение 100 000 cps подтверждено • Генератор не обнаруживает потерь установленных соединений

3.2. Тестирование на количество одновременных соединений (CC) в режиме FW+DPI

Задача теста — подтвердить соответствие целевому количеству одновременно открытых соединений TCP, поддерживаемому Solar NGFW (1 000 000 соединений).

Таблица 4. Тестирование на количество одновременных соединений (CC) FW+DPI+IPS

Настройки NGFW	Включены функции FW, DPI со следующими характеристиками:

	• Включены 1000 правил FW с анализом приложений • Журналирование включено для всех правил
Особенности трафика	Для тестирования используются соединения вида: • TCP SYN — SYNACK • TCP ACK • HTTP 1.0 GET (No Compression) Соединения устанавливаются в одном направлении и не закрываются во время тестирования
Методика тестирования	Порядок проверок: 1) Запустить тестирование с ограничением максимального количества открытых соединений на уровне целевого и со скоростью создания соединений на уровне 0,4 от значения CPS, определенного в разделе «3.1 Тестирование на определение максимального количества новых соединений в секунду (CPS)». В ходе тестирования разрешены TCP Retransmit, однако TCP Reset недопустимы. Во время тестирования средствами мониторинга системы снимаются показатели количества соединений и загруженности ресурсов. 2) Через 10 минут после достижения целевого количества установленных соединений остановить тест. Зафиксировать результат. Провести 3 проверки. Убедиться в стабильности результата
Ожидаемый результат	Solar NGFW поддерживает до 1 000 000 одновременно открытых соединений
Полученный результат	• Целевое значение 1 000 000 соединений подтверждено • Генератор не обнаруживает потерь установленных соединений

4. Нагрузочное тестирование в режиме FW

Задача теста — подтвердить соответствие пропускной способности Solar NGFW в режиме межсетевого экранирования (20 Гбит/с).

Таблица 5. Нагрузочное тестирование в режиме межсетевого экранирования

Настройки NGFW	Отключены функции DPI и IPS. Оставлено одно правило FW (разрешает все). Журналирование включено
Особенности трафика	Для тестирования используются соединения HTTP, в каждом из которых передается 64 КБ данных в каждом направлении
Методика тестирования	Порядок проверок: 1) Запустить тестирование с ограничением полосы пропускания на уровне целевого значения и со скоростью создания соединений на уровне 0,4 от значения CPS, определенного в разделе «3.1 Тестирование на определение максимального количества новых соединений в секунду (CPS)». В ходе тестирования разрешены TCP Retransmit, однако TCP Reset недопустимы. Во время тестирования средствами мониторинга системы снимаются показатели количества соединений и загруженности ресурсов. 2) Через 10 минут после достижения целевой пропускной способности остановить тест. Зафиксировать результат. Провести 3 проверки. Убедиться в стабильности результата
Ожидаемый результат	Solar NGFW обеспечивает функции межсетевого экранирования при скорости трафика 20 Гбит/с
Полученный результат	• Целевое значение пропускной способности 20 Гбит/с подтверждено • Генератор фиксирует потери трафика на уровне не более 0,1% общего числа пакетов

5. Нагрузочное тестирование в режиме FW+DPI

Задача теста — подтвердить соответствие целевому значению пропускной способности Solar NGFW в комбинированном режиме FW+DPI (15 Гбит/с).

Таблица 6. Нагрузочное тестирование в режиме FW+DPI

Настройки NGFW	Включены функции FW, DPI со следующими характеристиками: • Включены 1000 правил FW с анализом приложений • Журналирование включено для всех правил
Особенности трафика	Для тестирования используются соединения HTTP, в каждом из которых передается 64 КБ данных в каждом направлении
Методика тестирования	Порядок проверок: 1) Запустить тестирование с ограничением полосы пропускания на уровне целевого значения и со скоростью создания соединений на уровне 0,4 от значения CPS, определенного в разделе «3.1 Тестирование на определение максимального количества новых соединений в секунду (CPS)». В ходе тестирования разрешены TCP Retransmit, однако TCP Reset недопустимы. Во время тестирования средствами мониторинга системы снимаются показатели количества соединений и загруженности ресурсов. 2) Через 10 минут после достижения целевой полосы пропускания остановить тест. Зафиксировать результат. Провести 3 проверки. Убедиться в стабильности результата
Ожидаемый результат	Solar NGFW обеспечивает функции DPI при скорости трафика 15 Гбит/с
Полученный результат	• Целевое значение пропускной способности 15 Гбит/с подтверждено • Генератор фиксирует потери трафика на уровне не более 0,1% общего числа пакетов

6. Нагрузочное тестирование в режиме FW+DPI+IPS

Задача теста — подтвердить соответствие целевому значению пропускной способности Solar NGFW в комбинированном режиме FW+DPI+IPS (4 Гбит/с).

Таблица 7. Нагрузочное тестирование в режиме FW+DPI+IPS

Настройки NGFW	Включены функции FW, DPI и IPS со следующими характеристиками: • Включены 10 правил FW с анализом приложений • Включен анализ по всем сигнатурам IPS • Журналирование включено для всех правил
Особенности трафика	Для тестирования используются соединения HTTP, в каждом из которых передается 64 КБ данных в каждом направлении
Методика тестирования	Порядок проверок: 1) Запустить тестирование с ограничением полосы пропускания на уровне целевого значения и со скоростью создания соединений на уровне 0,4 от значения CPS, определенного в разделе «3.1 Тестирование на определение максимального количества новых соединений в секунду (CPS)». В ходе тестирования разрешены TCP Retransmit, однако TCP Reset недопустимы. Во время тестирования средствами мониторинга системы снимаются показатели количества соединений и загруженности ресурсов. 2) Через 10 минут после достижения целевой полосы пропускания остановить тест. Зафиксировать результат. Провести 3 проверки. Убедиться в стабильности результата
Ожидаемый результат	Solar NGFW обеспечивает одновременную работу функций FW, DPI и IPS при скорости трафика 4 Гбит/с
Полученный результат	• Целевое значение пропускной способности 4 Гбит/с подтверждено • Генератор фиксирует потери трафика на уровне не более 0,1% общего числа пакетов

7. Итоги

- Производительность.

  В в ходе нагрузочного тестирования устройство показало, что способно обеспечить пропускную способность до 20 Гбит/с в режиме FW и до 4 Гбит/с в режиме NGFW (FW+IPS+DPI).

- Стабильность работы.

  Solar NGFW обеспечил стабильную работу во время всех проведенных тестов. Не было обнаружено сбоев или непредвиденных прерываний в том числе и при максимальной нагрузке.

- Мониторинг и управление.

  Интерфейсы управления оставались доступными на протяжении всего процесса, позволяя проводить мониторинг и корректировать параметры в режиме реального времени.

- Характеристики для осуществления сайзинга.

  Количество новых соединений (CPS), количество одновременных соединений (CC) при изменении различных параметров Solar NGFW: включенных модулей безопасности (FW, DPI, IPS) и используемых ядер зафиксированы.

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 систему повышения эффективности труда Solar addVisor.

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 1800 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