Сетевая Безопасность

Инфосистемы Джет

Jet NGFW Lab: методика и ключевые итоги независимого тестирования решений NGFW в 2024 году

Евгений Пузаков

**Ведущий инженер
по информационной безопасности,
«Инфосистемы Джет»**

Инфосистемы Джет

Сетевая Безопасность

Структура презентации

1. Функциональное тестирование
2. Нагрузочное тестирование
3. Результаты 2024
4. Что будет дальше?

Инфосистемы Джет

Функциональное тестирование – это

Сетевая Безопасность

- **Инструмент для ИБ-специалистов, независимый от производителей**
- **Тестирование популярных NGFW с включенными модулями безопасности**
- **Условия приближены к реальным**

ГРУППА ФУНКЦИОНАЛА	КЕЙС	ШАГИ ВЫПОЛНЕНИЯ
Базовые функции	Работа в режиме L3 (Routing Mode)	1. Выбрать режим функционирования L3 2. Настроить IP-адресацию MGMT-интерфейса и статический маршрут (при необходимости) 3. Настроить IP-адресацию Internal/External-интерфейсов, маршрут по умолчанию 4. Настроить правило доступа для разрешения трафика INT->EXT (ETH2->WAN) 5. Настроить правило Source NAT (Many-to-One) для выхода в интернет для INT (ETH2) 6. Настроить на тестовой рабочей станции в качестве шлюза по умолчанию INT (ETH2)-интерфейс тестируемого МСЭ 7. Проверить доступ к ресурсам интернет (запустить команду ping 8.8.8.8, открыть ya.ru через браузер) 8. Убедиться в наличии событий доступа с тестовой рабочей станции
	Работа в режиме L2 (Transparent Mode)	1. Выбрать режим функционирования L2 2. Настроить IP-адресацию MGMT-интерфейса и маршрут по умолчанию (при необходимости) Дальнейшие шаги могут отличаться в зависимости от тестируемого МСЭ, среды тестирования (vSphere, EVE-NG) и особенностей работы МСЭ в L2 3. Определить Internal/External-интерфейсы 4. Настроить правило доступа для разрешения трафика INT->EXT 5. Настроить на тестовой рабочей станции подключена в сегмент INT) в качестве шлюза по умолчанию интерфейс L3-устройства, являющийся шлюзом по умолчанию в сегменте EXT 6. Проверить доступ к внешним ресурсам/ресурсам интернет 7. Убедиться в наличии событий доступа с тестовой рабочей станции
	Режим получения динамических маршрутов при работе в кластере	1. Собрать и настроить кластер 2. Включить динамическую маршрутизацию
	VRF	1. Создать и настроить VRF 2. Назначить интерфейсы указанным VRF
	Поведение МСЭ при ассиметричной маршрутизации	1. Передать трафик с использованием ассиметричных маршрутов 2. Выполнить изменение настроек МСЭ по обработке трафика при ассиметричной маршрутизации (при наличии такой возможности)
	Настройка Proxy ARP	1. Включить Proxy ARP для определенного интерфейса 2. Отправить трафик на сеть, для которой включен Proxy ARP
	Возможность указывать исходящий интерфейс при настройке маршрутизации	1. Создать маршрут с явно указанным исходящим интерфейсом 2. Отправить трафик, который должен использовать этот маршрут
	Приоритизация маршрутов	1. Создать несколько маршрутов с разными метриками 2. Передать трафик, который должен использовать эти маршруты
	Поддержка Fullview (маршрутизация)	1. Изучить документацию и функционал системы
		1. Настроить ECMP для определенных маршрутов

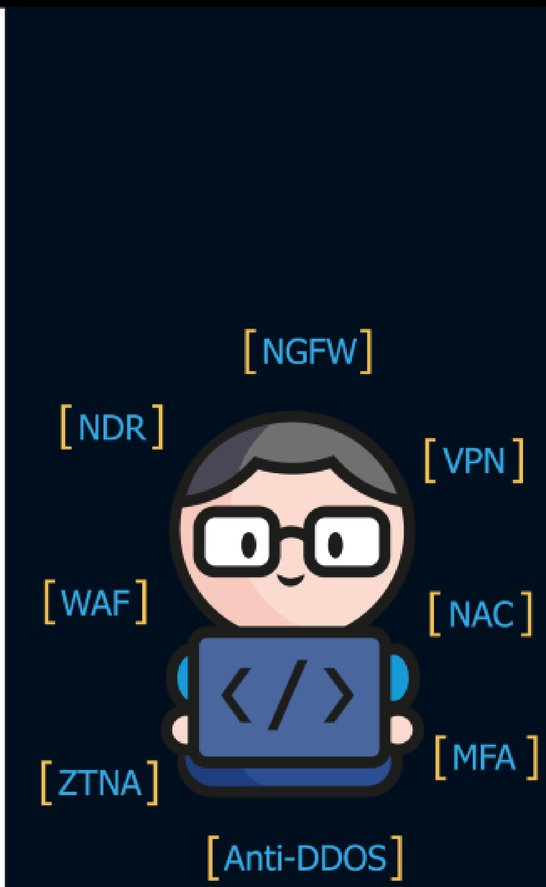
Инфосистемы Джет

Функциональное тестирование

Сетевая Безопасность

Сетевые функции **Режимы работы**	Континент 4.1.9 ↗	Check Point R81.2 ↗	Ideco NGFW v16 ↗
Работа в режиме L3 (Routing Mode)	✓	✓	✓
Работа в режиме L2 (Transparent Mode)	Да, с ограничениями	✓	✗
Маршрутизация			
Режим получения динамических маршрутов при работе в кластере	Анонсы только на активной ноде. На резервной служба bird не активна	Обе ноды	Маршруты получает активная нода. При переключении кластера пассивная нода получает маршруты
Поведение МСЭ при ассиметричной маршрутизации	Трафик блокируется. Тест с дефолтной конфигурацией антиспуфинга	В зависимости от настроек	Трафик блокируется
Возможность указывать исходящий интерфейс при настройке маршрутизации	ограничениями	✓	Да, с ограничениями
Приоритизация маршрутов	✓	✓	✓
Поддержка Fullview (маршрутизация)	✓	✓	✓
ECMP	✓	✓	Да, с ограничениями

- **Один унифицированный демостенд**
- **Более 250 параметров по одной методике**
- **Опубликовано 8 решений**
- **Прозрачная методика**
- **Возможность удобного поиска и скачивание результатов**

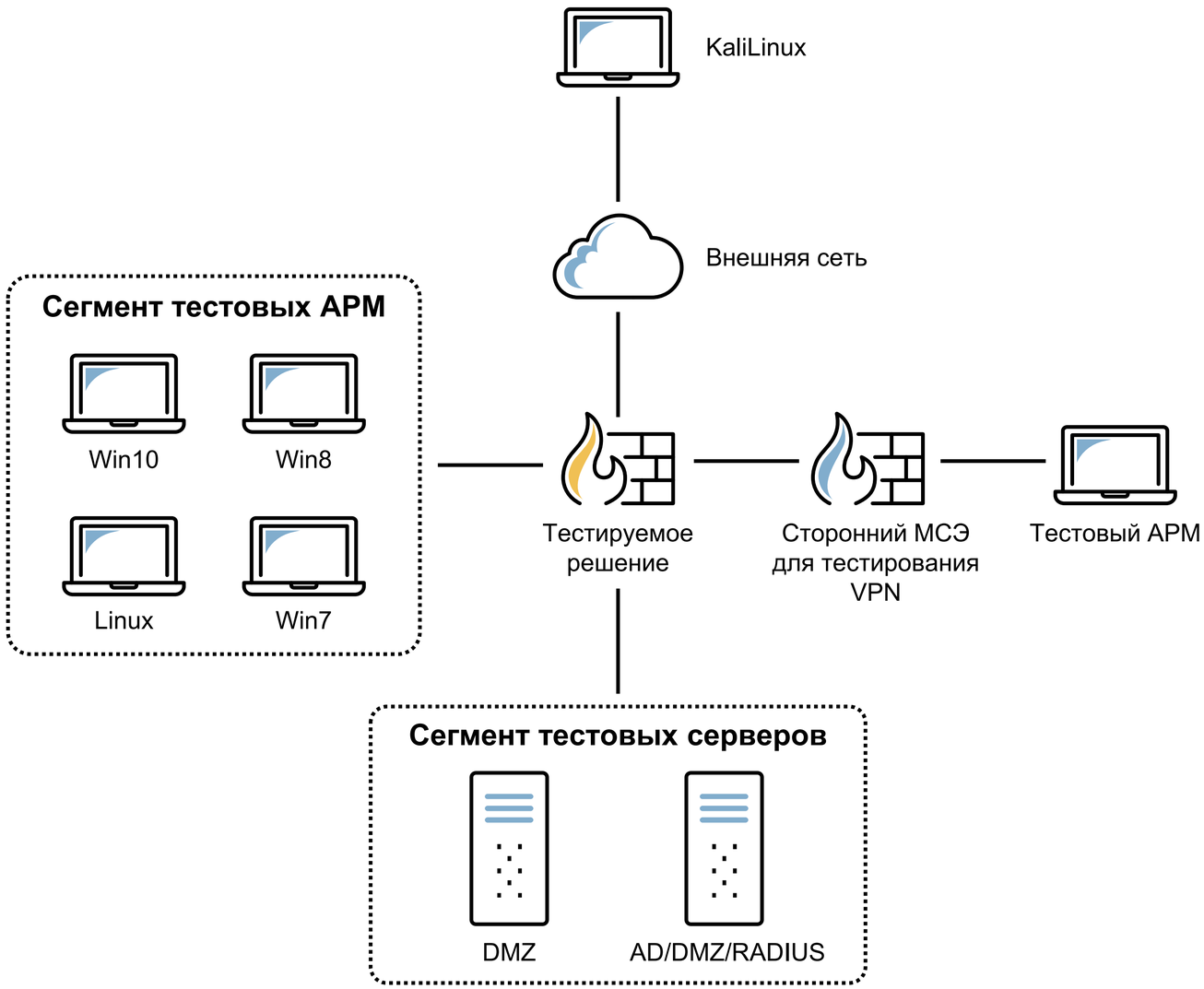


Инфосистемы Джет

Сетевая Безопасность

Функциональное тестирование

Схема демостенда



Инфосистемы Джет

Сетевая Безопасность

Нагрузочное тестирование

ЗАДАЧА

Определить предельную производительность NGFW, при превышении которой его работа становится нестабильной либо не выполняются заявленные функции безопасности

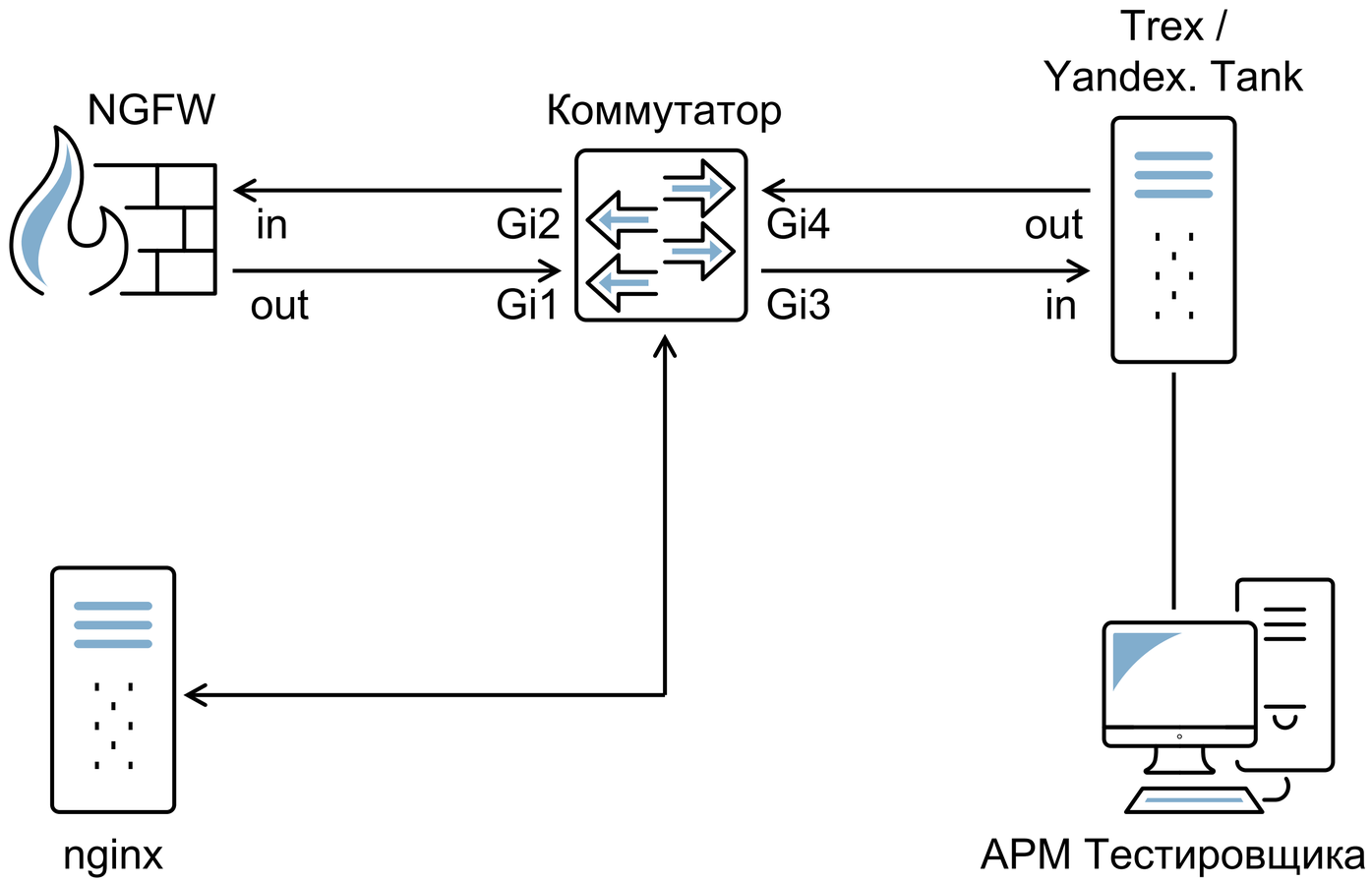
Сравнить пропускную способность, заявленную производителем, с результатом на нашем демостенде

Инфосистемы Джет

Сетевая Безопасность

Нагрузочное тестирование

Описание стенда



Нагрузочное тестирование

Сетевая Безопасность

Тест-кейсы

- Максимальное число новых соединений в секунду
- Определение максимальной пропускной способности (EMIX)
- Максимальное число конкурентных соединений в секунду
- Максимальное число транзакций в секунду при инспекции TLS
- Максимальное число пакетов в секунду
- Работоспособность функций безопасности под нагрузкой

Инфосистемы Джет

Функциональное тестирование – это

Сетевая Безопасность

ЗАДАЧА

Определить максимальную пропускную способность для трафика EMIX

ПРОЦЕСС ТЕСТА

1. Запустить генератор трафика:
   - Профиль трафика emix.py
2. В статистике генератора зафиксировать:
   - текущее значение пропускной способности (в Гбит/с)
   - число потерь
3. Используя бинарный поиск, найти значение пропускной способности, при котором потери сессий близки к 1%
4. Рекомендуемое время прохождения каждой итерации теста — **5 минут**

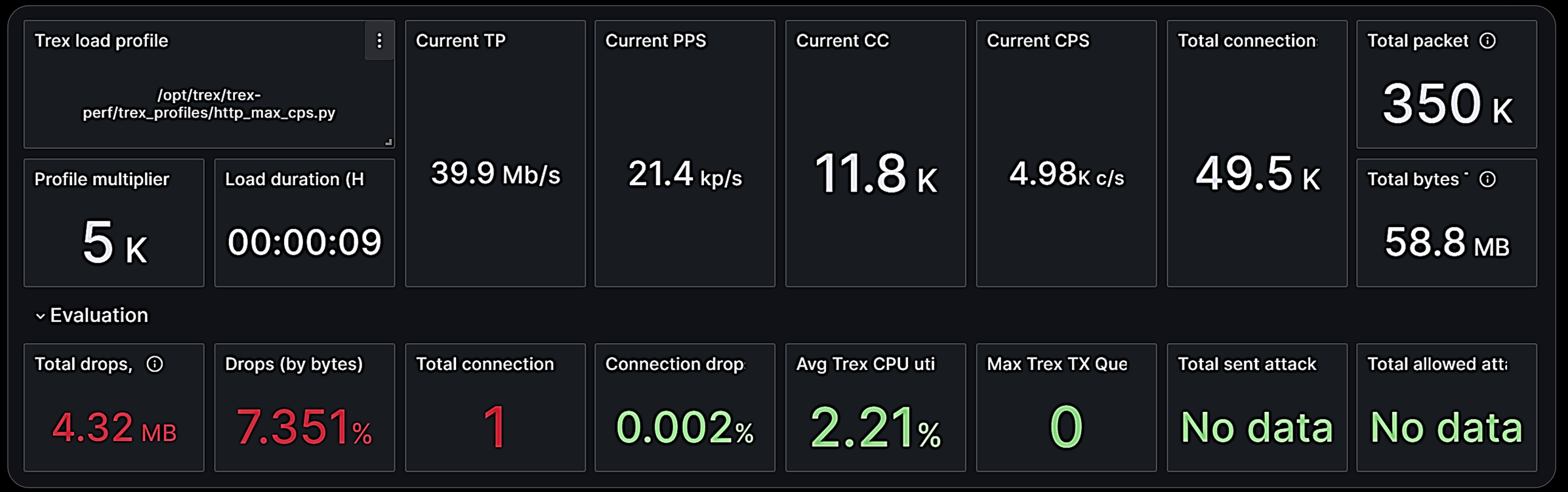
ПРОФИЛЬ EMIX

ТРАФИК	% BY BYTES	% BY PACKETS	% BY CONN
NFS (TCP)	0,1	0,5	1
HTTP (TCP)	33,44	25,2	19,94
HTTPS (TLS1.2)	35,08	23,83	15,95
HTTP (POST)	0,77	0,88	1,99
VIDEO_CALL	20,09	19,03	1
RTP (UDP)	0,84	11,52	1
SMB (TCP)	1,45	1,59	5,38
DNS (UDP)	0,26	2,55	7,98
SMTP (TCP)	0,55	1,33	4,49
POP (TCP)	0,16	0,59	1
IMAP (TCP)	0,05	0,51	1
Generic TCP	2,02	2,54	9,97
Generic UDP	1,97	4,51	5,38
SIP (UDP)	2,84	4,42	19,94
RDP (UDP)	0,18	0,15	1,99
SYSLOG (UDP)	0,09	0,47	1
SSH (TCP)	0,08	0,38	1

Сетевая Безопасность

Нагрузочное тестирование

Пример | Максимальное число новых соединений в секунду MAX HTTP CPS

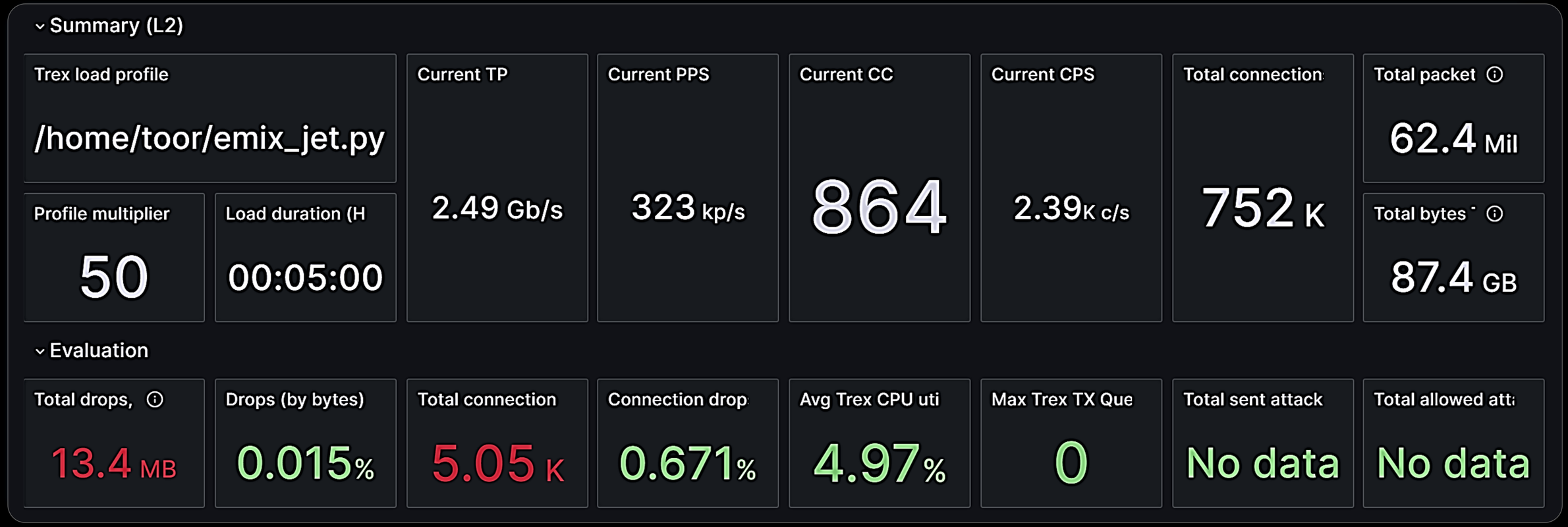


Инфосистемы Джет

Сетевая Безопасность

Нагрузочное тестирование

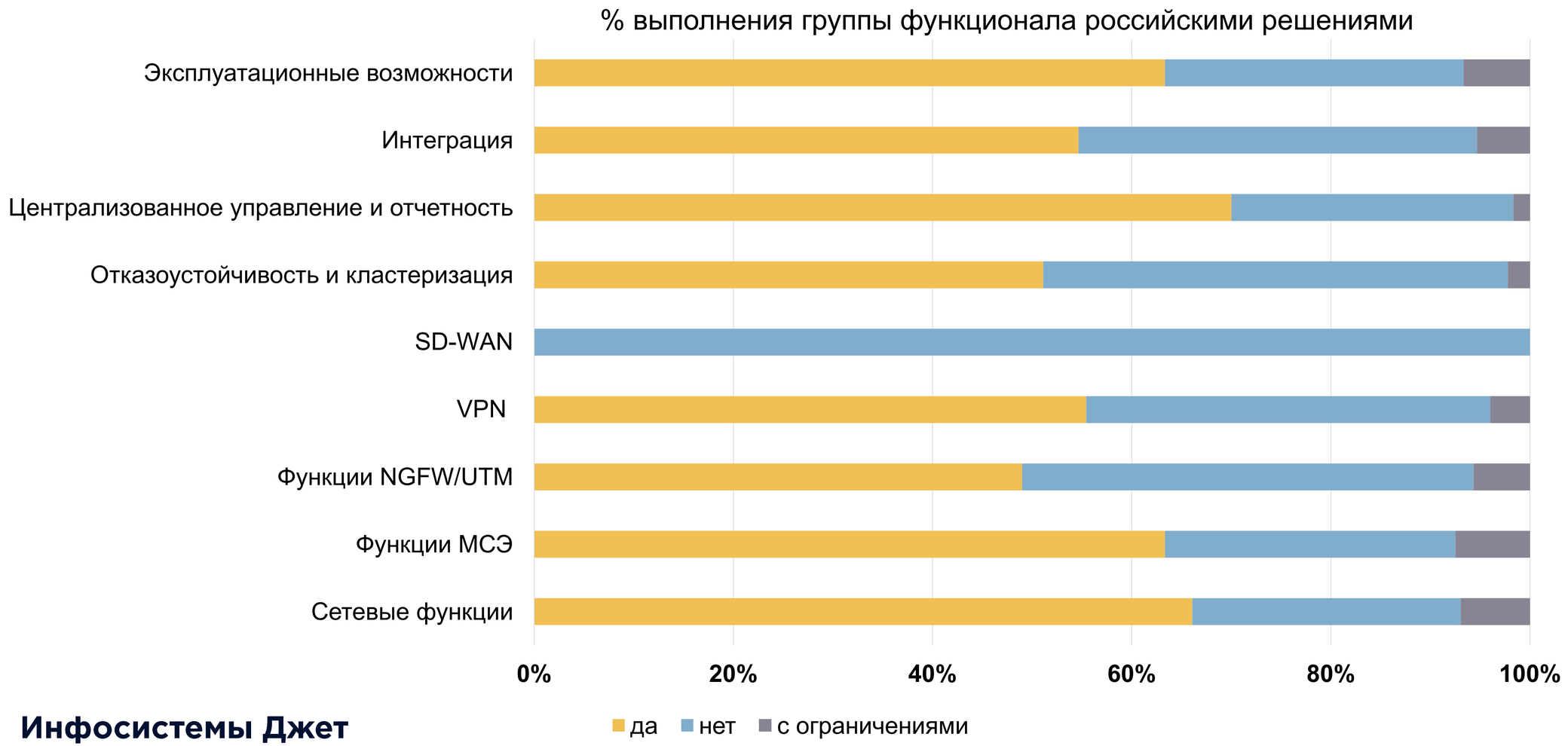
Пример | Определение максимальной пропускной способности (EMIX)



Инфосистемы Джет

Сетевая Безопасность

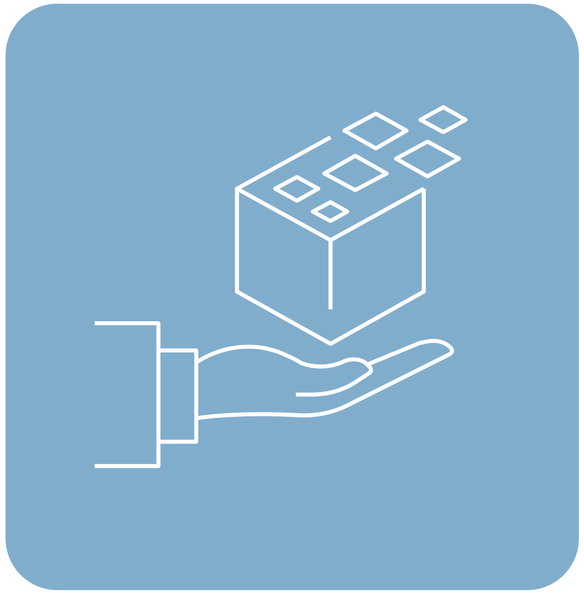
Результаты 2024



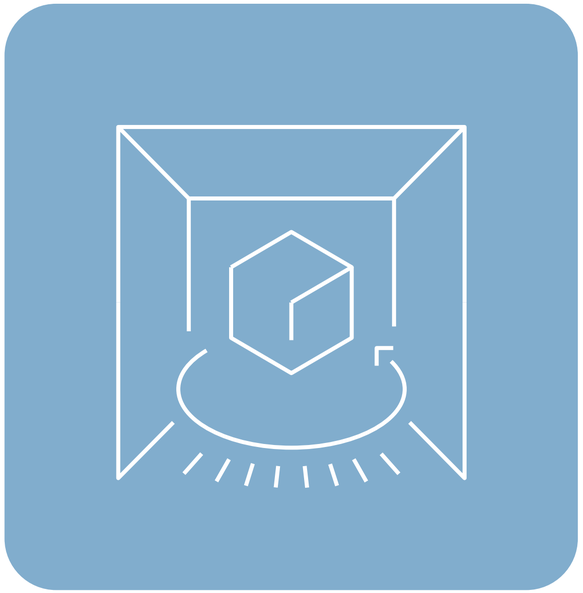
Инфосистемы Джет

Сетевая Безопасность

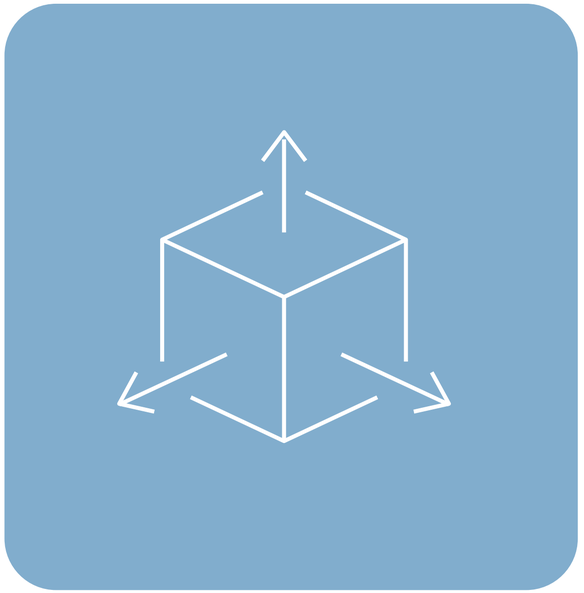
Что будет дальше?



Тестируются другие производители



При выходе новой версии — новый тест



Расширение методики тестирования

Инфосистемы Джет

Сетевая Безопасность

Результаты тестирования и методика тестирования

https://ngfw.jet.su

Инфосистемы Джет

Сетевая
Безопасность

Спасибо за внимание!

Инфосистемы Джет