

Инженерный подход к безопасности NGFW

Марк Коренберг
СТО



ideco

Ideco сегодня



20 лет на рынке, тысячи защищённых компаний и регулярные продуктовые релизы — решения Ideco создаются командой, где более половины сотрудников (150 человек) сосредоточены на разработке.

Мы растём вместе с нашими клиентами, масштабируем решения и поддерживаем безопасность сотен тысяч пользователей по всей стране.

20+

лет на рынке

5500+

компаний под
защитой

2400+

участников
сообщества

55%

сотрудников
в R&D

25000

атак блокируются
ежедневно

4

мажорных релиза
продукта в год

Инженерный подход к безопасности NGFW



Проблема

- Реальные инциденты возникают из-за архитектурных и процессных решений.
- Устойчивость NGFW определяется дисциплиной разработки и эксплуатации.

Тезис

Инженерный подход — это формализованные процессы, архитектурные принципы и строгий контроль

Безопасность встроена в жизненный цикл разработки



Процесс разработки

- 25 формализованных процессов разработки безопасного ПО.
- Охват всего цикла РБПО: архитектура, моделирование угроз, анализ кода, тестирование, сборка, выпуск, сопровождение.
- Внутренние и внешние аудиты.
- Соответствие требованиям ГОСТ.
- Мы не завязаны на поставщиков ПО, а все делаем сами. Базовая ОС обновляется каждый релиз.

Вывод

**Безопасность — это не этап,
а непрерывный процесс**

Все это знают)

Регламенты РБПО по этапам жизненного цикла ПО



Управление процессами и требованиями

- Процессы РБПО
- Обучение сотрудников РБПО
- Управление требованиями ПО
- Управление конфигурацией ПО
- Управление недостатками ПО

Сборка и защита среды разработки

- Использование безопасной системы сборки
- Безопасность сборочной среды
- Управление доступом и контроль целостности кода
- Обеспечение безопасности секретов

Безопасная разработка

- Оформление исходного кода
- Экспертиза исходного кода
- Статический анализ
- Динамический анализ
- Композиционный анализ
- Контроль цепочек поставок

Архитектура и моделирование угроз

- Анализ архитектуры ПО
- Разработка модели угроз и поверхности атаки

Тестирование

- Функциональное тестирование
- Нагрузочное тестирование
- Тестирование на безопасность

Выпуск и поставка

- Безопасность при выпуске версии
- Безопасная поставка пользователям

Эксплуатация и сопровождение

- Техническая поддержка
- Реагирование на уязвимости
- Поиск уязвимостей при эксплуатации
- Безопасность при выводе из эксплуатации

Статический и динамический анализ



Статический анализ

- Проводится по модулям поверхности атаки.
- Подтверждённые Critical и Major блокируют релиз.
- Повторный анализ до полного устранения.
- Обязательное кросс-ревью разметки.

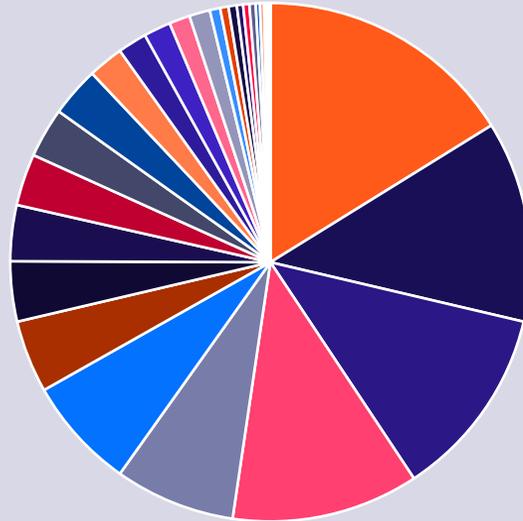
Динамический анализ и фаззинг

- Перечень модулей формируется по модели угроз.
- Повторный анализ после исправлений.
- Фиксация аварийных завершений и результатов.

Статический и динамический анализ

Проверено 1062 предупреждений в 40 проектах

Исправлено 88 уязвимостей



На каждый модуль потрачено не менее 50 часов фаззинга. На ядро ~350 часов.

- | | | | |
|-------------------------|--------------------------|-------------------------|---------------------------------|
| ■ техцентр 4 | ■ frr(bgpd и ospfd) | ■ python3 | ■ etcd |
| ■ net-snmp(snmp) | ■ fail2ban | ■ ideco-acl-helpers | ■ suricata |
| ■ zabbix | ■ openssh | ■ modsecurity | ■ unbound |
| ■ squid | ■ dnsmasq | ■ nginx | ■ iptables |
| ■ netmap-ipfw(kipfw) | ■ cerberus | ■ ideco-app-control-nfq | ■ igmpproxy |
| ■ ideco-ad-backend | ■ ideco-routing-backend | ■ ideco-web-backend | ■ ideco-ald-backend |
| ■ ideco-cluster-backend | ■ ideco-firewall-backend | ■ ideco-system-backend | ■ ideco-user-backend |
| ■ ideco-app-backend | ■ ideco-auth-backend | ■ ideco-backup-backend | ■ ideco-central-console-backend |
| ■ ideco-dns-backend | ■ ideco-local-menu | ■ ideco-logs-backend | ■ ideco-network-backend |
| ■ ideco-proxy-backend | ■ ideco-shaper-backend | ■ kernel | |

Результаты анализа CVE



Сравнение веток

Структура найденных CVE

- Основной вклад: golang, dnsmasq, системные библиотеки.
- Часть CVE относится к Windows-only сценариям или неиспользуемым функциям.
- Некоторые CVE являются FP или уже устранены.

Вывод

- В новой версии 21.12 зафиксировано снижение CRITICAL CVE: 13 → 9.
- Отсутствуют HIGH/MEDIUM/LOW уровни.
- Часть CVE классифицирована как Mitigated (3 штуки) или NotAffected (24 штуки).
- Используется автоматизированный анализ на базе NVD (980 831 записей).

22_release Show all

Author	Commit	Message	Commit date
	56870795a90	ICS-57902 add unit tests 22_release	21 янв. 2026
	9dc4f374f87	ICS-60298 Возвращены наши правки	22 янв. 2026
	a557c4aca6f	ICS-60298 Распакован ванильный dnsmasq-2.90-6.fc42.src.rpm	22 янв. 2026
	5bc1fd56c8c	ICS-56609: forward port patches from 19_release to 21_release	17 окт. 2025
	f32d8fa564f	ICS-56609: unpack dnsmasq-2.90-4.fc41.src	17 окт. 2025
	1cf9c095a0b	ICS-52865 patched fuzzing crashes	06 авг. 2025
	0b3e703587e	ICS-52231 fix dnsmasq 51505 svace patch 19_9_35 19_release	15 июл. 2025
	4493456d254	ICS-52170 [svace] fix MEMORY_LEAK in src/domain-match	14 июл. 2025
	391bbafe469	ICS-51504 [svace] fix Deref_of_Null.Ex.Cond in src/dnsmasq 3 tags	01 июл. 2025
	0f89adc9d45	ICS-51505 fix Deref_of_Null.Ex.Cond in src/option.c	01 июл. 2025
	247aea8da07	ICS-51506 [svace] fix Division_By_Zero in src/cache	01 июл. 2025
	9f824fd095c	ICS-51507 [svace] fix Division_By_Zero in src/dbus	01 июл. 2025
	f8a34582f6d	ICS-51508 [svace] fix Handle_Leak in src/netlink	01 июл. 2025
	0e7a855bbbe	ICS-51509 [svace] fix Memory_Leak.Ex in src/option	01 июл. 2025
	d231924beae	ICS-51510 fix UNINIT.LOCAL_VAR in src/forward	01 июл. 2025
	93d7d52fbe5	ICS-51510 Адаптация dnsmasq под систему сборки	01 июл. 2025

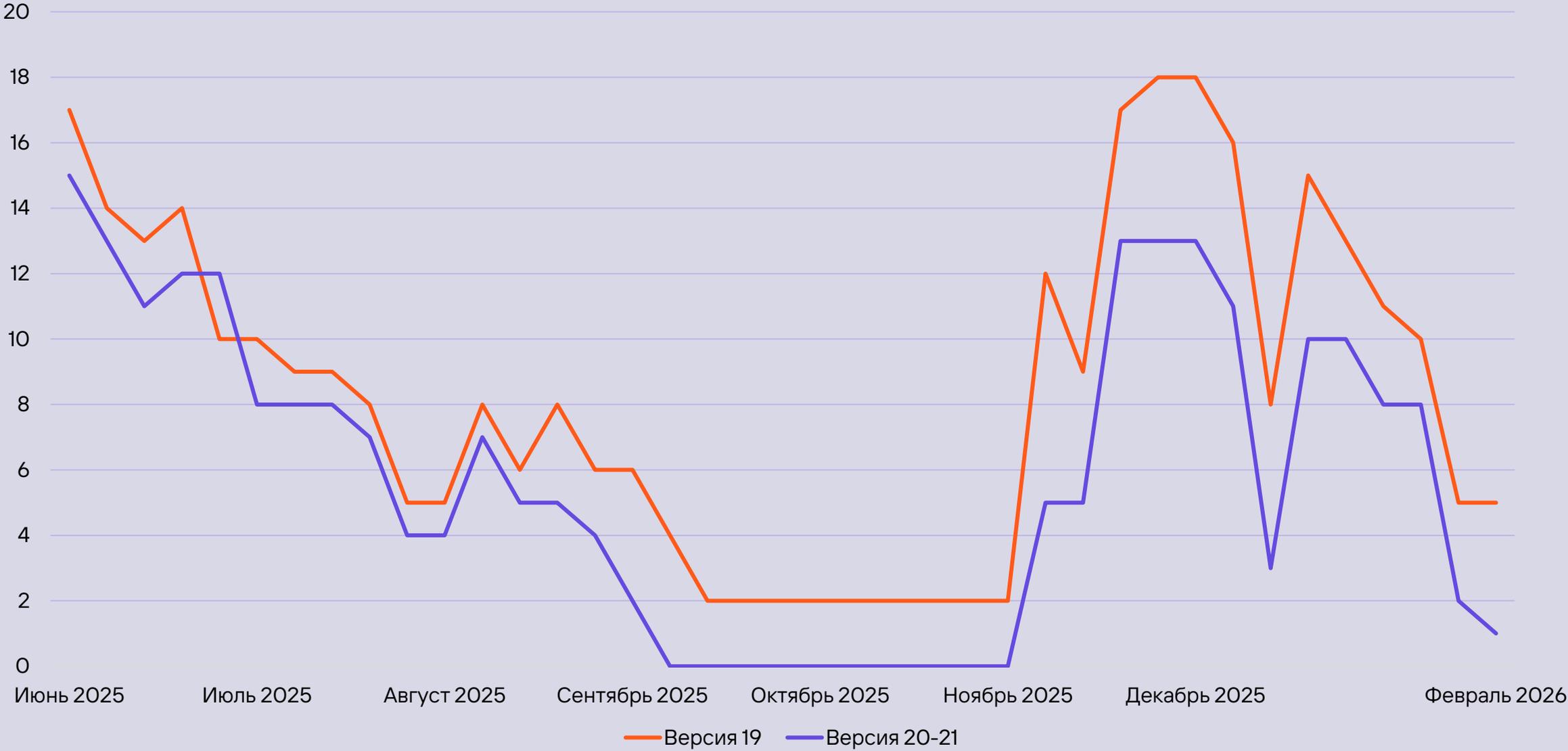
Версия 19.17

CRITICAL: 13
HIGH/MEDIUM/LOW: 0

Версия 21.12

CRITICAL: 9 (снижение)
HIGH/MEDIUM/LOW: 0

Medium/Low уязвимости



Проекты Запросы Дашборды Теги Настройки проектов Администрирование Архив

Идеco NGFW

Введите название

Создать дефект Перезапустить автотесты

Фильтр Колонки Всего: 119

ID	Название	Запуски	Результат	Причины п
1157...	Подключение freeipa юзера по VPN	1	Провален	Проду
1157...	Подключение freeipa юзера по VPN	1	Провален	Проду
1157...	Подключение freeipa юзера по VPN	1	Провален	Проду
1157...	Подключение freeipa юзера по VPN	1	Провален	Проду
1099...	Подключение ald юзера по VPN	1	Успешен	
1099...	Подключение ald юзера по VPN	1	Успешен	
1099...	Подключение ald юзера по VPN	1	Успешен	
1099...	Подключение ald юзера по VPN	1	Успешен	
1099...	Ограничение скорости - авторизация пользователя из внеш...	1	Успешен	
1099...	Ограничение скорости - авторизация пользователя из внеш...	1	Успешен	
1099...	Ограничение скорости - авторизация пользователя из внеш...	1	Успешен	
1099...	Ограничение скорости - авторизация пользователя из внеш...	1	Успешен	
1098...	Netflow v10 - Учёт интерфейса клиентского vpn трафика (ike...	1	Успешен	
1098...	Netflow v10 - Учёт интерфейса клиентского vpn трафика (sstp)	1	Успешен	
1098...	Netflow v10 - Учёт интерфейса клиентского vpn трафика (l2tp)	1	Успешен	
1098...	Netflow v10 - Учёт интерфейса клиентского vpn трафика (ppt...	1	Успешен	
1098...	Netflow v9 - Учёт интерфейса клиентского vpn трафика (ikev2)	1	Успешен	
1098...	Проверка negotiate авторизации AD пользователя на UTM	1	Успешен	
1098...	Netflow v9 - Учёт интерфейса клиентского vpn трафика (sstp)	1	Успешен	

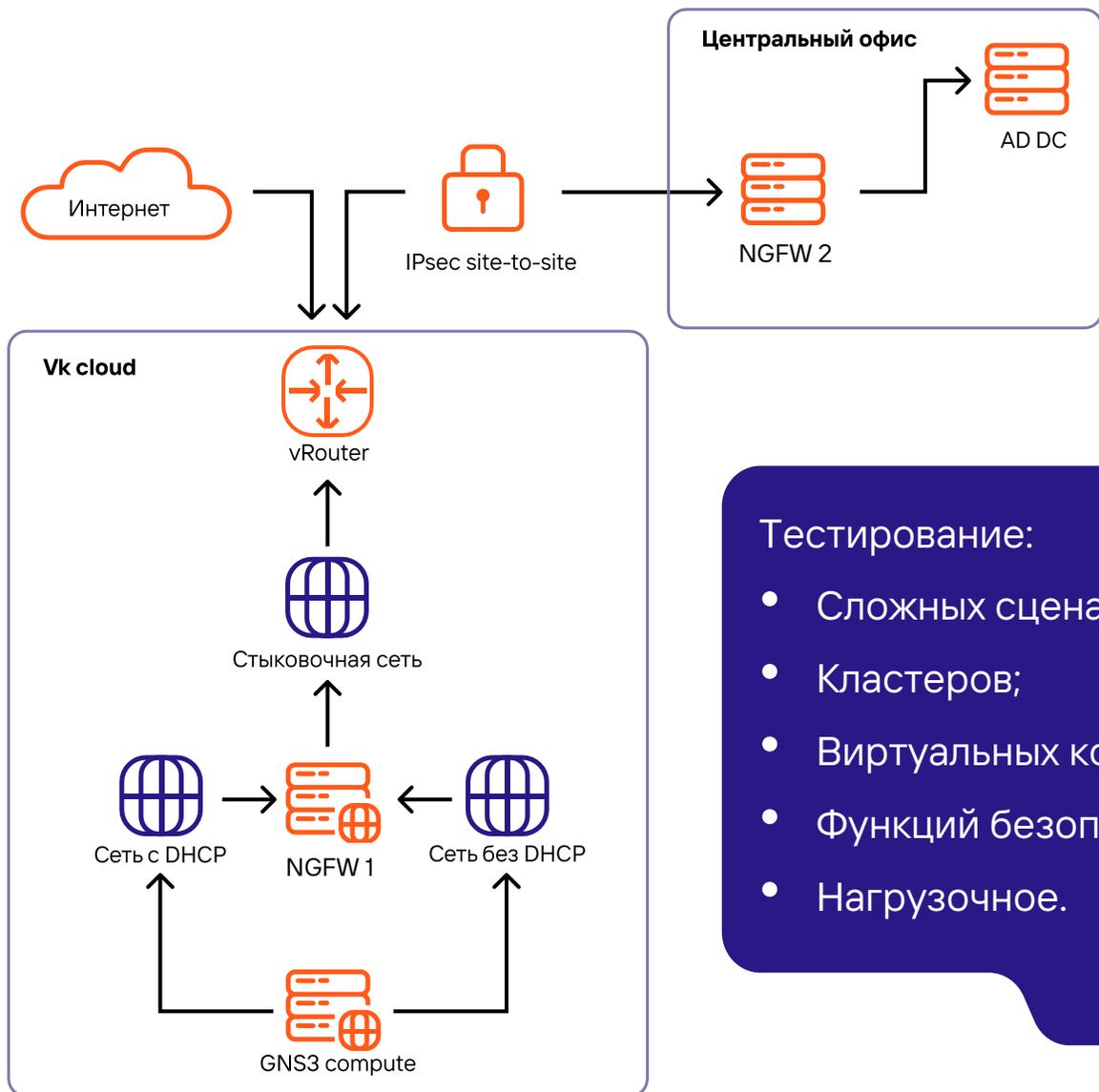
Регрессионное тестирование ngf...
Статус: **Завершён**
Описание: Regression id: 788802ef-31b9-4f1d-a84f-544f221dffa8
Источник запуска: Autotest server
Дата создания: 12.02.2026
Автор: autotest NOT_SN
Вебхуки: Запуск автотестов 21_release +2
Конфигурации: ideco-ngfw-21-12-335-devel

Распределение тестов по результатам

Анализ категорий ошибок

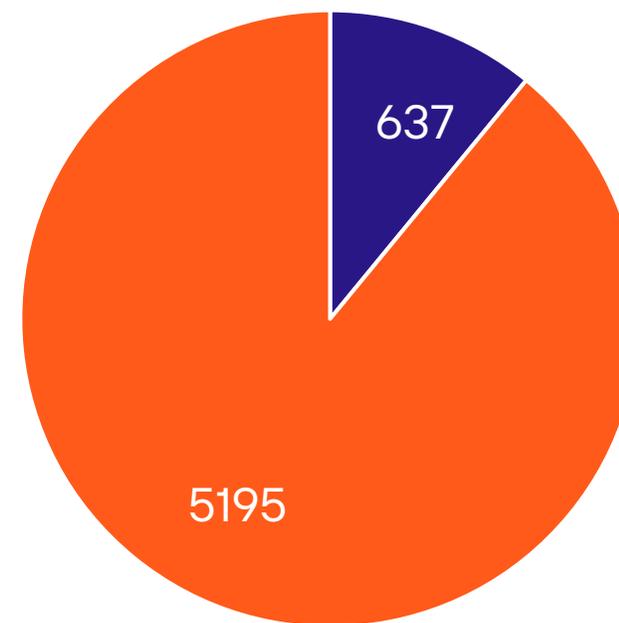
- 300 VM
- 45 потоков
- 3,5–4 часа

Тестирование



Тестирование:

- Сложных сценариев;
- Кластеров;
- Виртуальных контекстов;
- Функций безопасности;
- Нагрузочное.



■ Ручные тесты ■ Автотесты

Не только теория, но и практика



Пилоты у заказчиков

Кейсы технической поддержки

Инциденты и аварийные сценарии

Ограничения по ресурсам
и компетенциям заказчика

Иногда архитектура усложняется внутри, чтобы снизить риски и ошибки в эксплуатации.

Сертифицированное решение Ideco



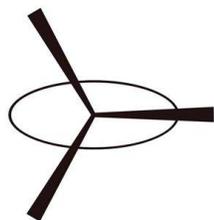
защищает сетевой периметр организаций



ФГУП «ВНИИ «Центр»



АО «Таганрогский завод «Прибой»



АО «Конструкторское бюро
промышленной автоматики»

Внутренняя инфраструктура компании



Безопасность инфраструктуры напрямую влияет на безопасность продукта

Защищаемся не только от третьих лиц, но и **от атак внутри** за счет:

- Для всех сервисов используется SSO+2FA
- Доступ по API сделан по отзываемым токенам (без использования логина и пароля)
- Сканирование безопасности внутренних сервисов проводится ежедневно (с использованием SIEM)
- SLA исправления критических уязвимостей во внутренних сервисов составляет – 24 часа
- Около 300 сервисов

Разделение Control Plane и Data Plane



1

Архитектурный принцип

- Управляющий и пользовательский трафик имеют разные модели угроз.
- Изоляция плоскостей — обязательное требование.

2

Реализация

- Контейнерная модель.
- Раздельные ресурсы и изоляция процессов.
- Сохранение управляемости при атаке на Data Plane.

3

Результат

Диагностика и изменение конфигурации возможны под нагрузкой или атакой.

Виртуальные контексты VCE



Что такое VCE

- Изолированная среда со своей адресацией, маршрутами, политиками, правилами журналирования.
- Разделение зон безопасности внутри одного устройства.
- Привязка VCE к аппаратным ресурсам

Эволюция архитектуры

До 2025 года

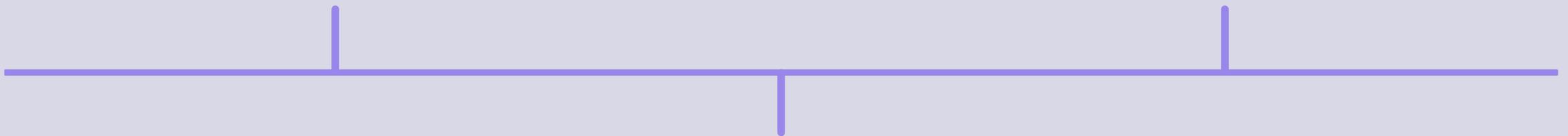
Management plane и data plane не разделены

В 2026 году

Обработка трафика только в VCE.
Hardening служб

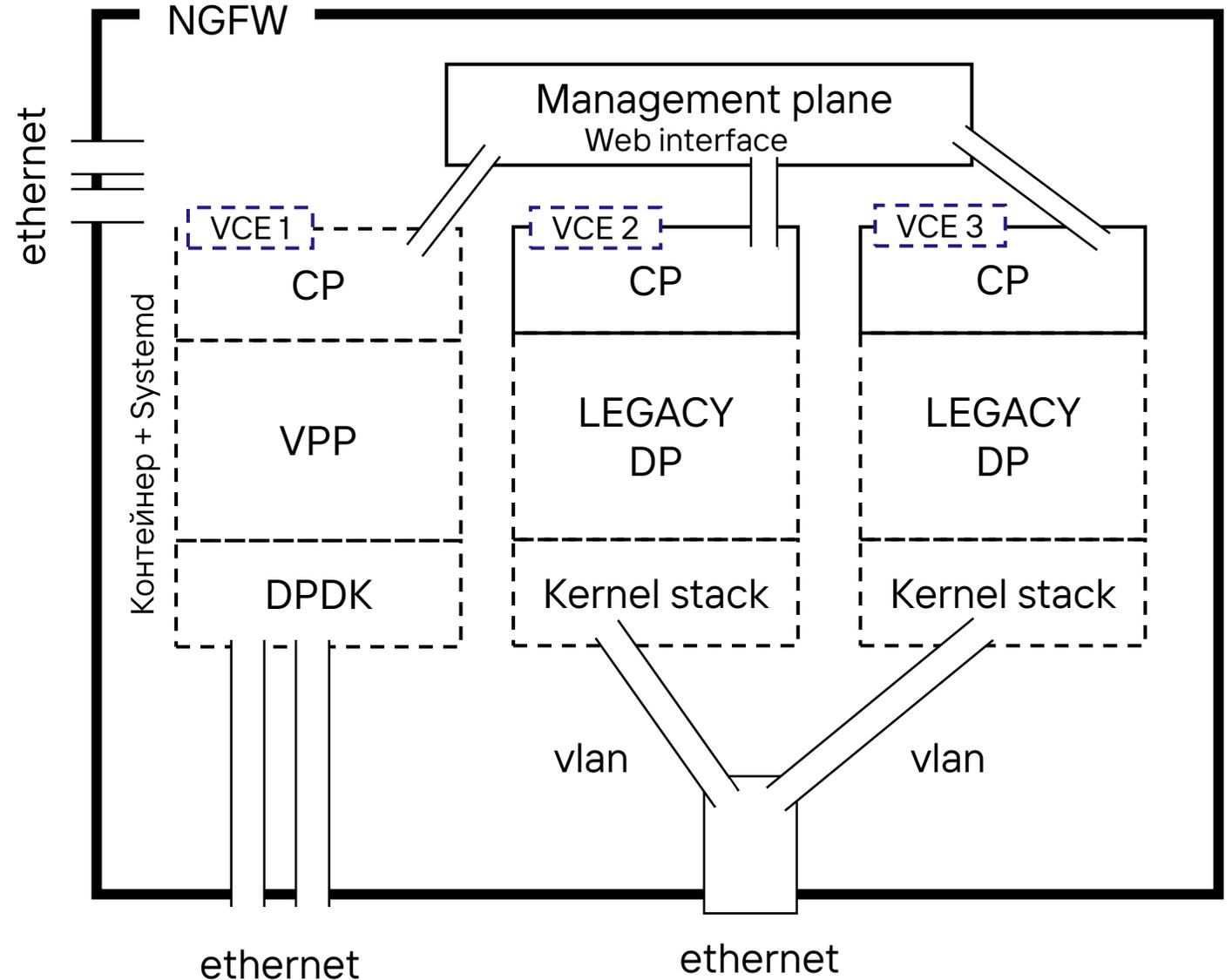
С 2025 года

Элементы management plane внутри VCE



Архитектура NGFW с контекстами

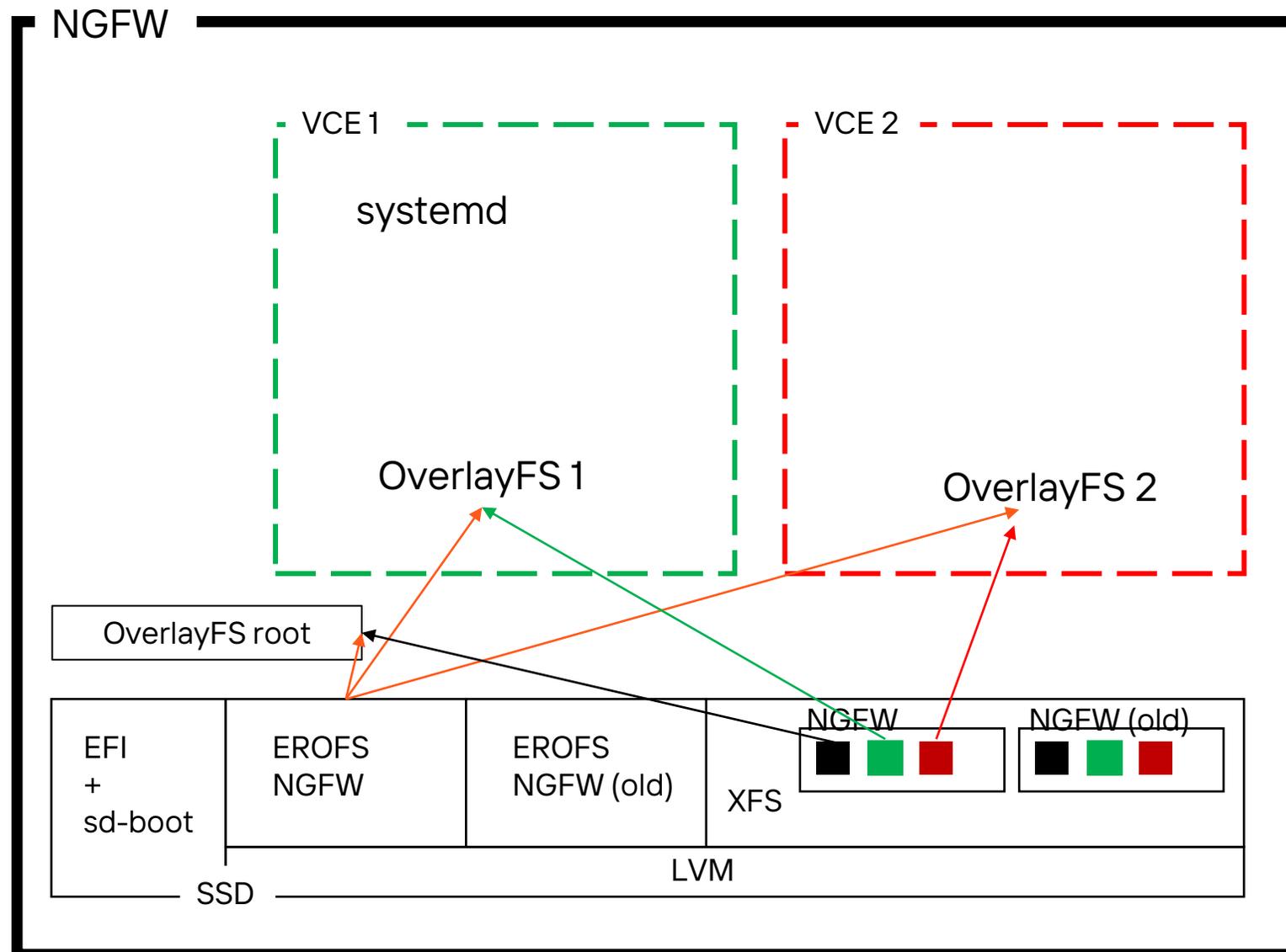
- Management plane — общий
- Несколько VCE — независимые
- Разные типы data plane (VPP/DPDK и legacy)



Файловая система: EROFS + OverlayFS + LVM



- Общий read-only EROFS
- OverlayFS для каждого VCE
- Нет отдельных контейнерных образов
- Лёгкие обновления, быстрые откаты.



Зрелый NGFW — это продукт, который строится по процессам РБПО, где качество обеспечено архитектурой, процессами и строгим контролем.

Это дополняет быстрое развитие сетевых функций, ФБ, а так же производительности продукта.

На защите ваших ценностей!

8 800 555 33 40

expert@ideco.ru

ideco.ru



ideco

