Виртуальные контексты в Ideco NGFW Novum:

архитектура, кластеризация, планы развития

Изоляция, отказоустойчивость и высокопроизводительная обработка трафика

ideco

Зачем нужны виртуальные контексты

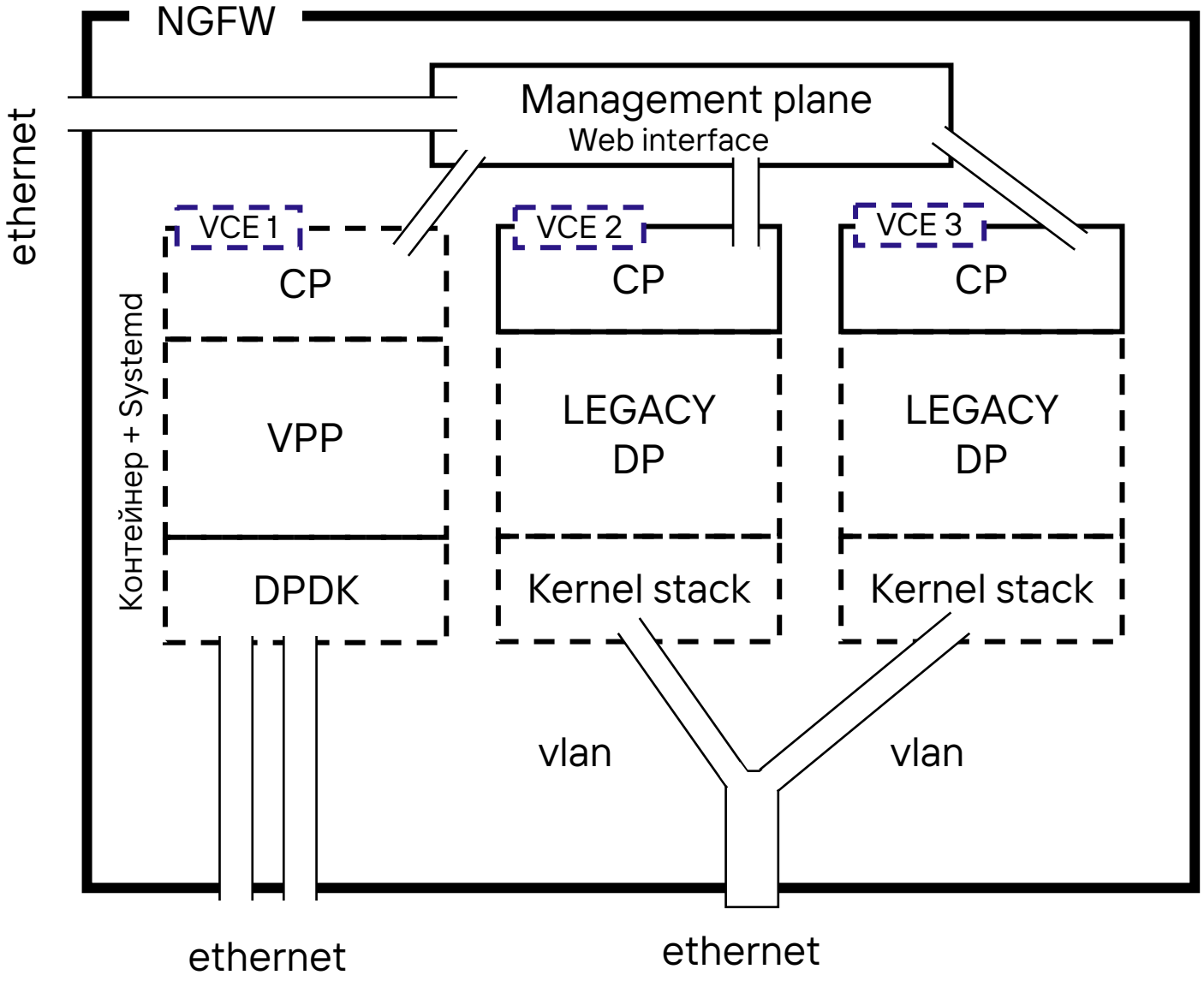
ideco

- Пересечение IP-адресов
- Изоляция и безопасность
- Масштабирование
- Отказоустойчивость
- Минимизация рисков конфигурационных ошибок
- Разделение ресурсов

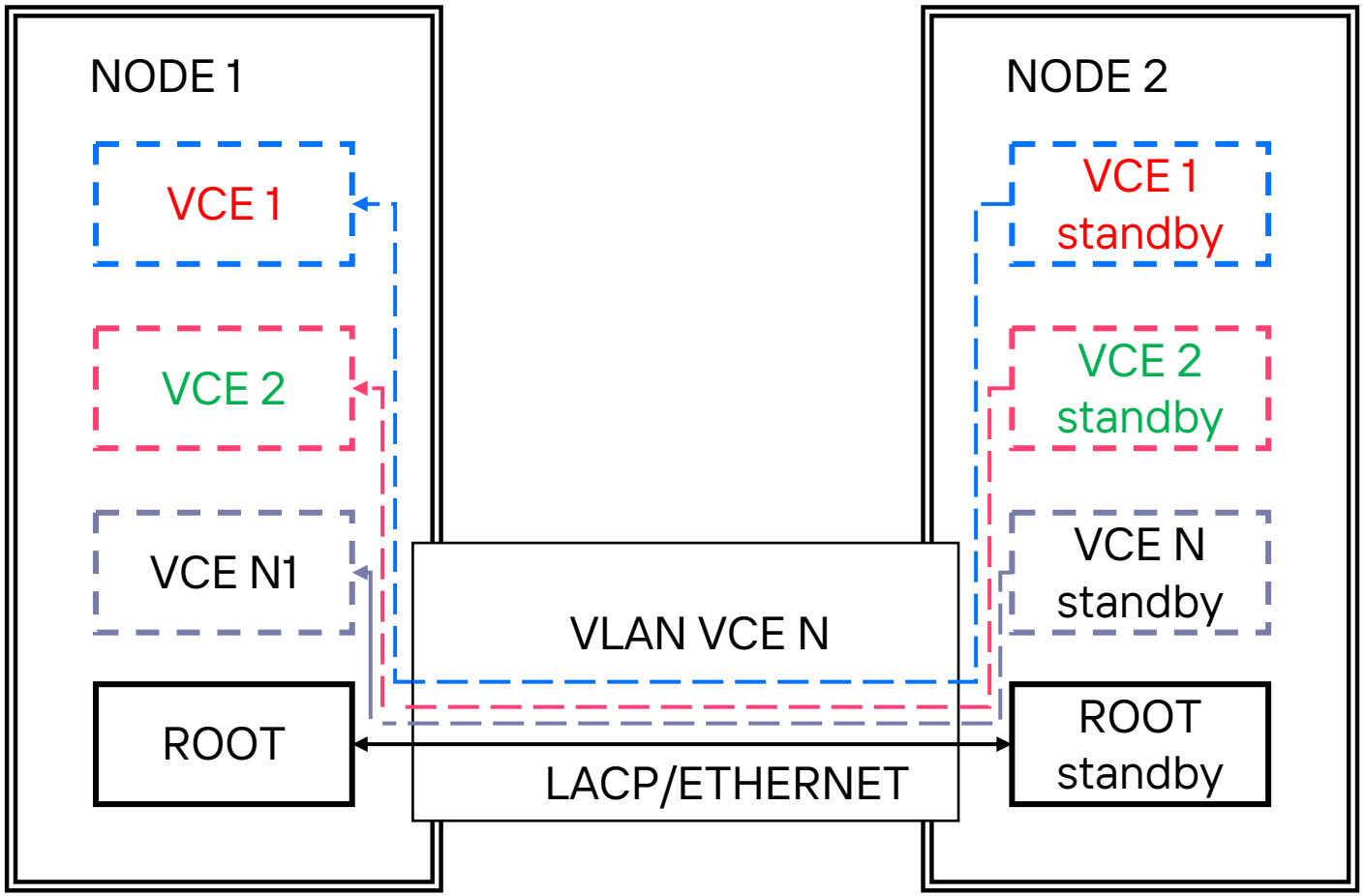
Архитектура NGFW с контекстами

(верхний уровень)

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

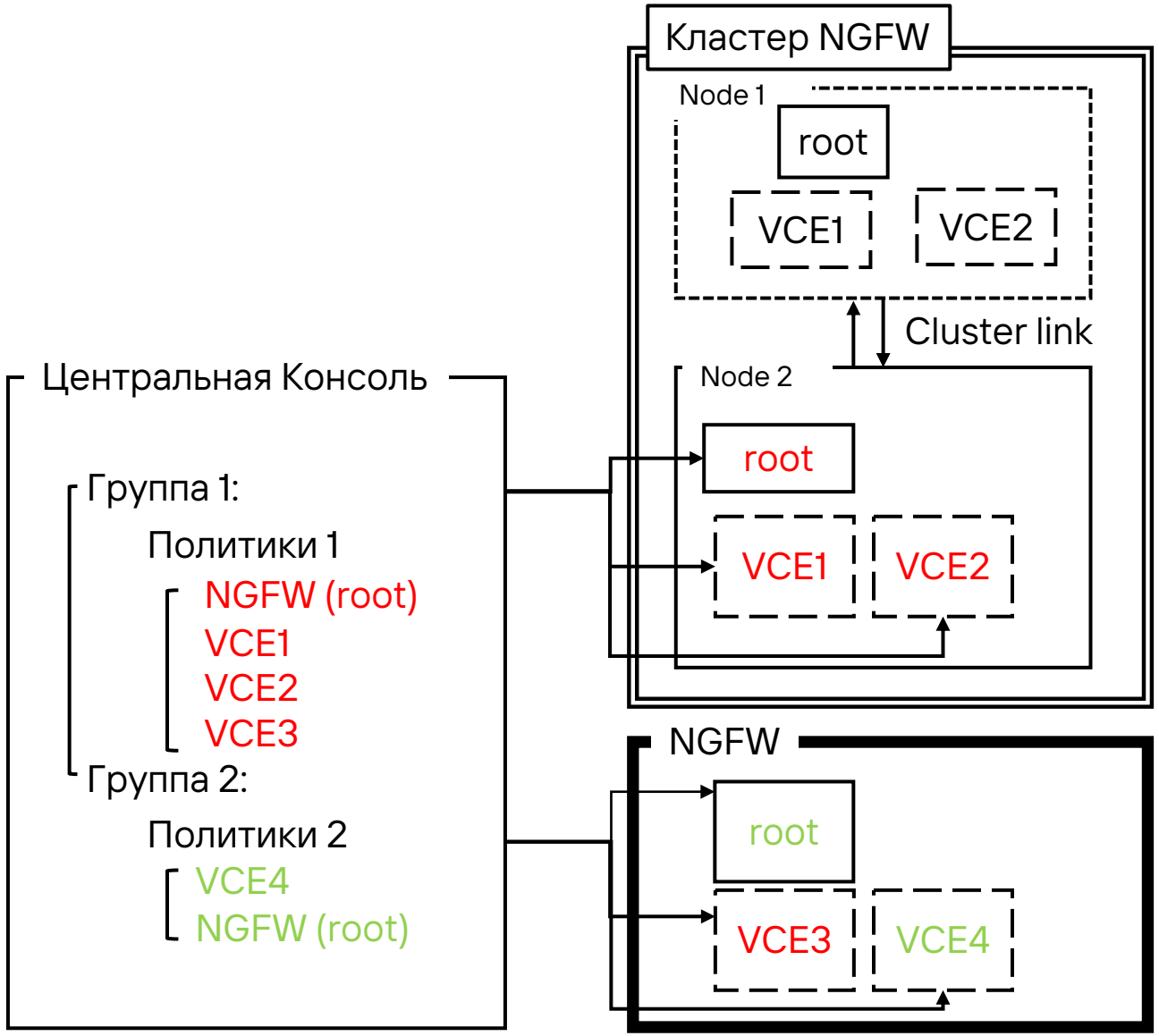


Кластеризация контекстов (as-is)



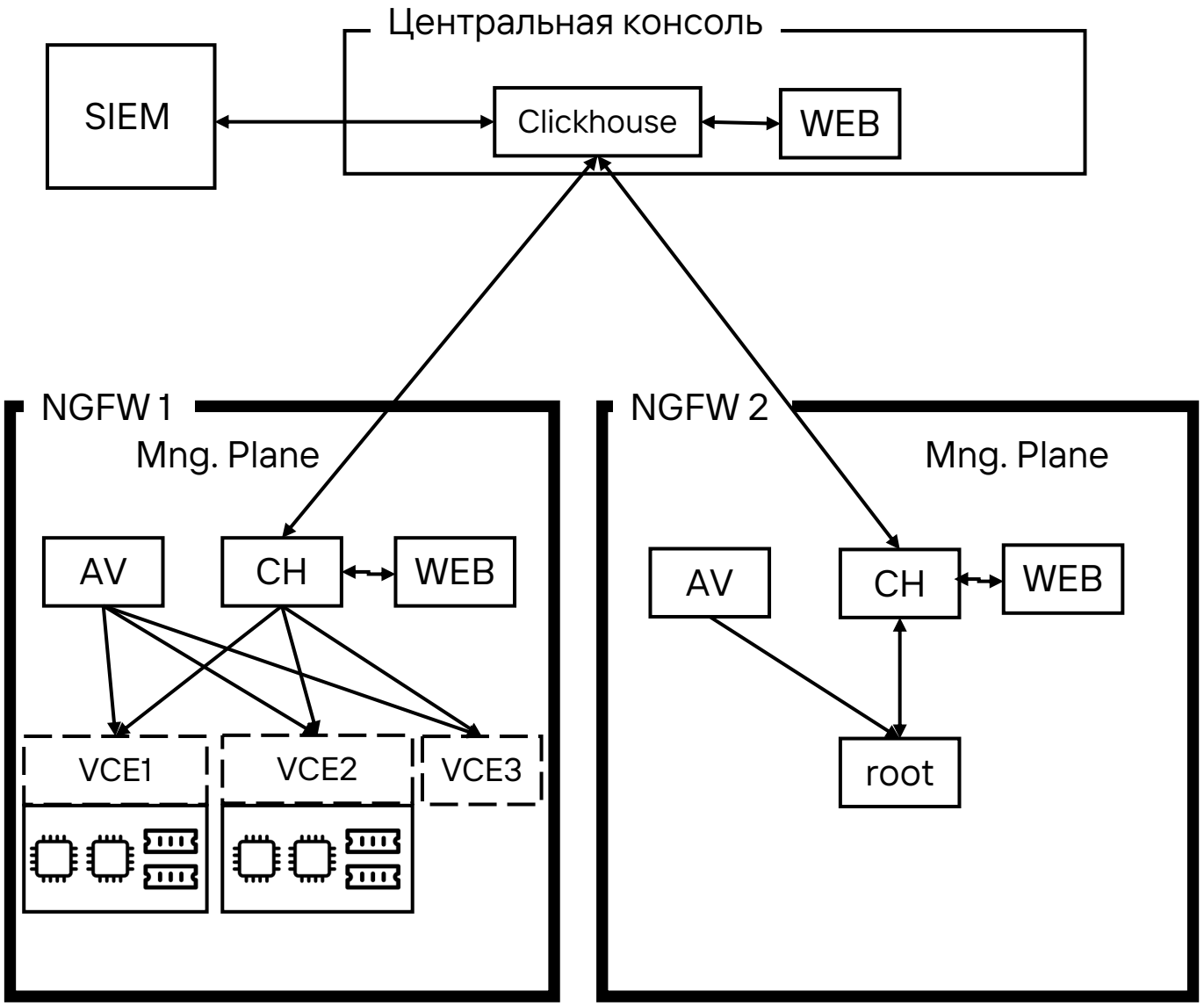
- Active/Standby на уровне нод
- VCE наследуют состояние ноды в кластере
- Связь VCE ↔ VCE через отдельные VLAN
- Root участвует в cluster link

Интеграция с центральной консолью



- Контексты видны в ЦК как отдельные сущности
- Группируем по логике использования
- As-is: ручная регистрация каждого контекста
- To-be: автоматическая регистрация всех VCE при добавлении NGFW

Общие сервисы: ClickHouse, AV, Web

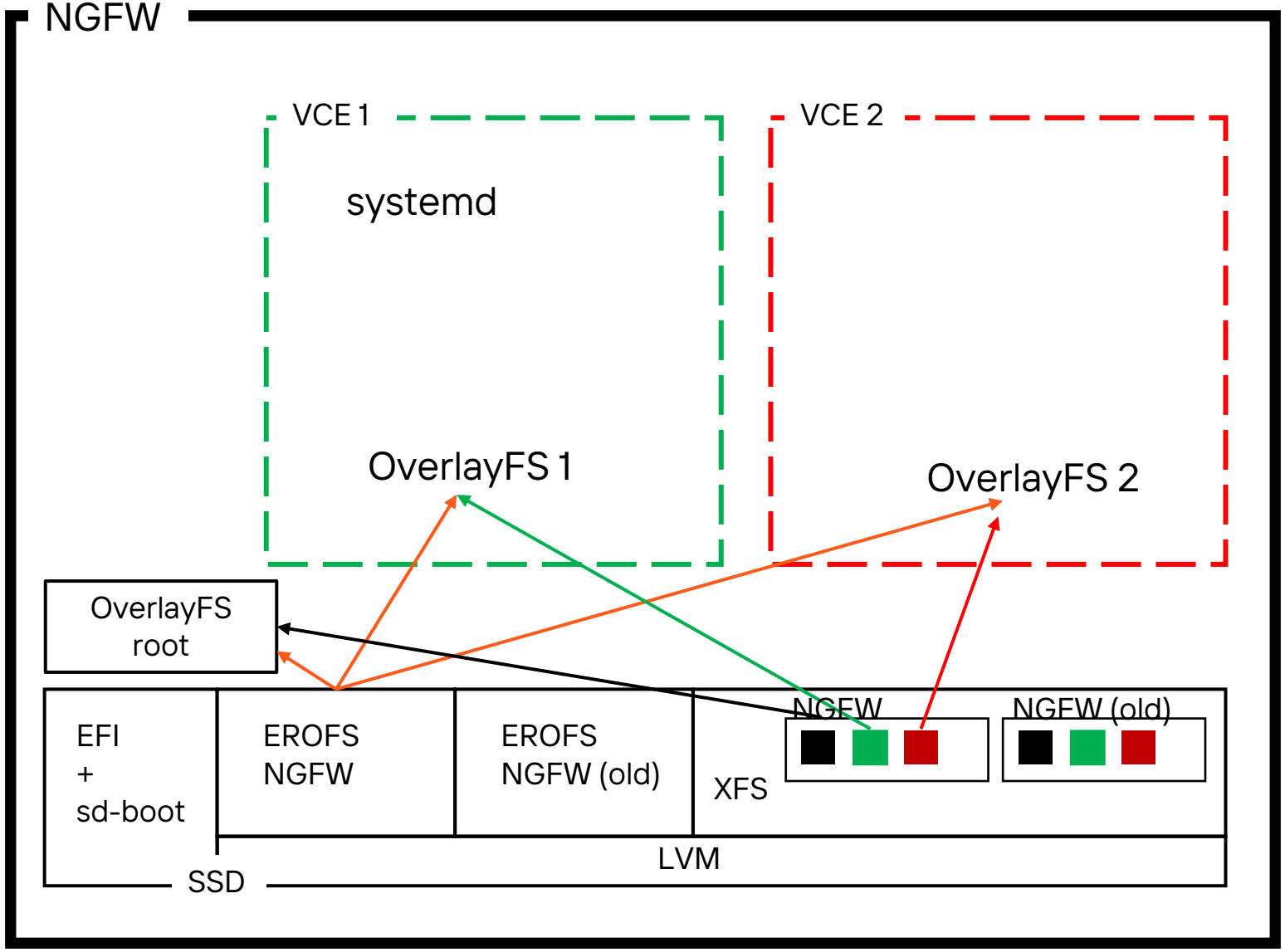


- **Сервисы с простоем становятся общими**
- DP полностью изолирован
- Ограничение: любой VCE может загрузить весь ClickHouse → Трафик не страдает, влияет только на отчётность

Файловая система: EROFS + OverlayFS + LVM

ideco

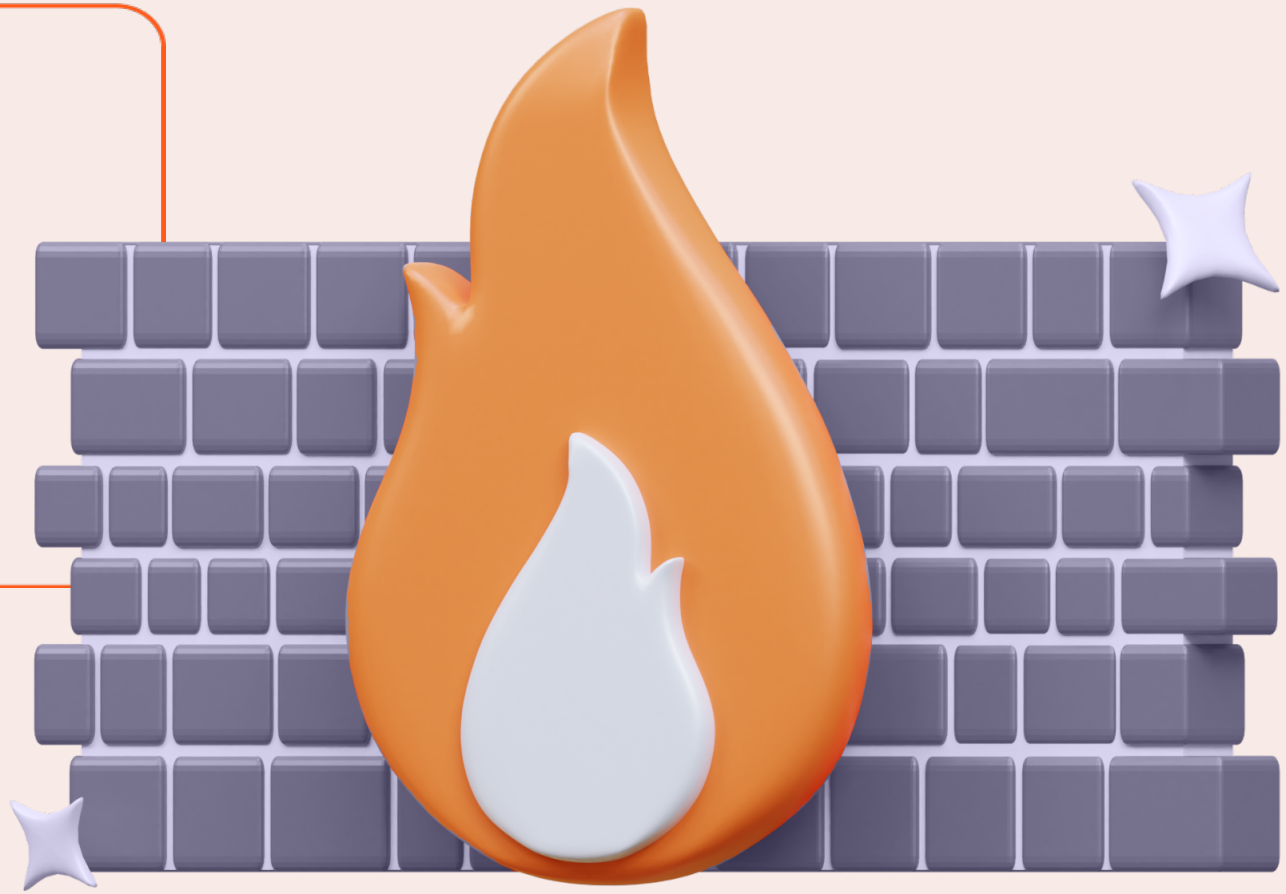
- Общий read-only EROFS
- OverlayFS для каждого VCE
- Нет отдельных контейнерных образов
- Лёгкие обновления, быстрые откаты (осуждаем)



Планы развития

ideco

- Вынесение Management Plane в отдельный контейнер
- Полный отказ от обработки трафика в root
- Multitenancy:
- Независимые VCE в кластере
- Виртуальные линки между VCE
- Полный переход на VPP/DPDK



На защите ваших ценностей!

8 800 555 33 40

expert@ideco.ru

ideco.ru

ideco