

Интеграция сервисов безопасности в SDN-фабрику современного ЦОД

Ермилов Леонид le@b4com.tech

Ведущий менеджер по продуктам ЦОД B4com Tech

Команда системных инженеров B4com Tech: rs-se@b4com.tech

О компании – В4com Tech



«Бифорком Тек» – компания-разработчик сетевого оборудования для бизнеса и телекоммуникаций

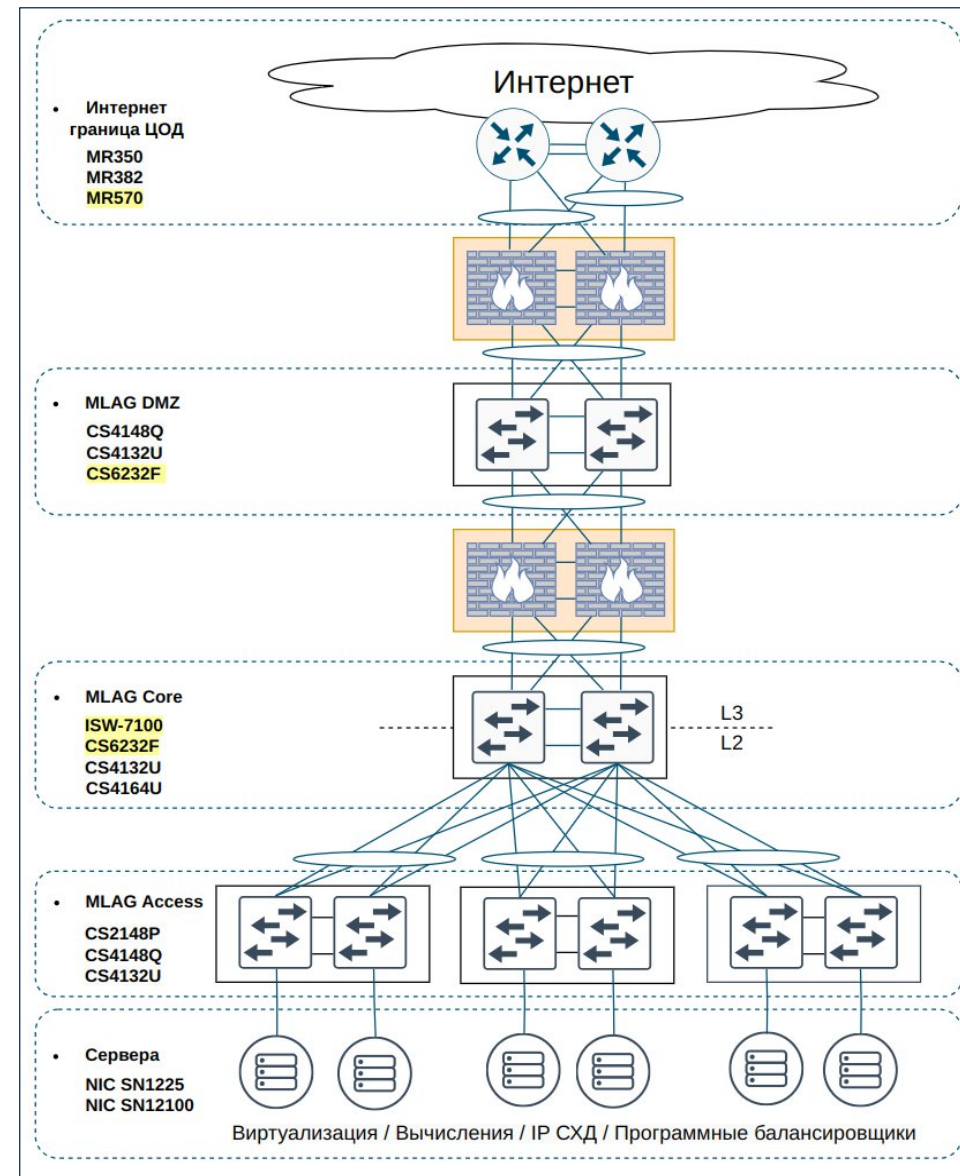
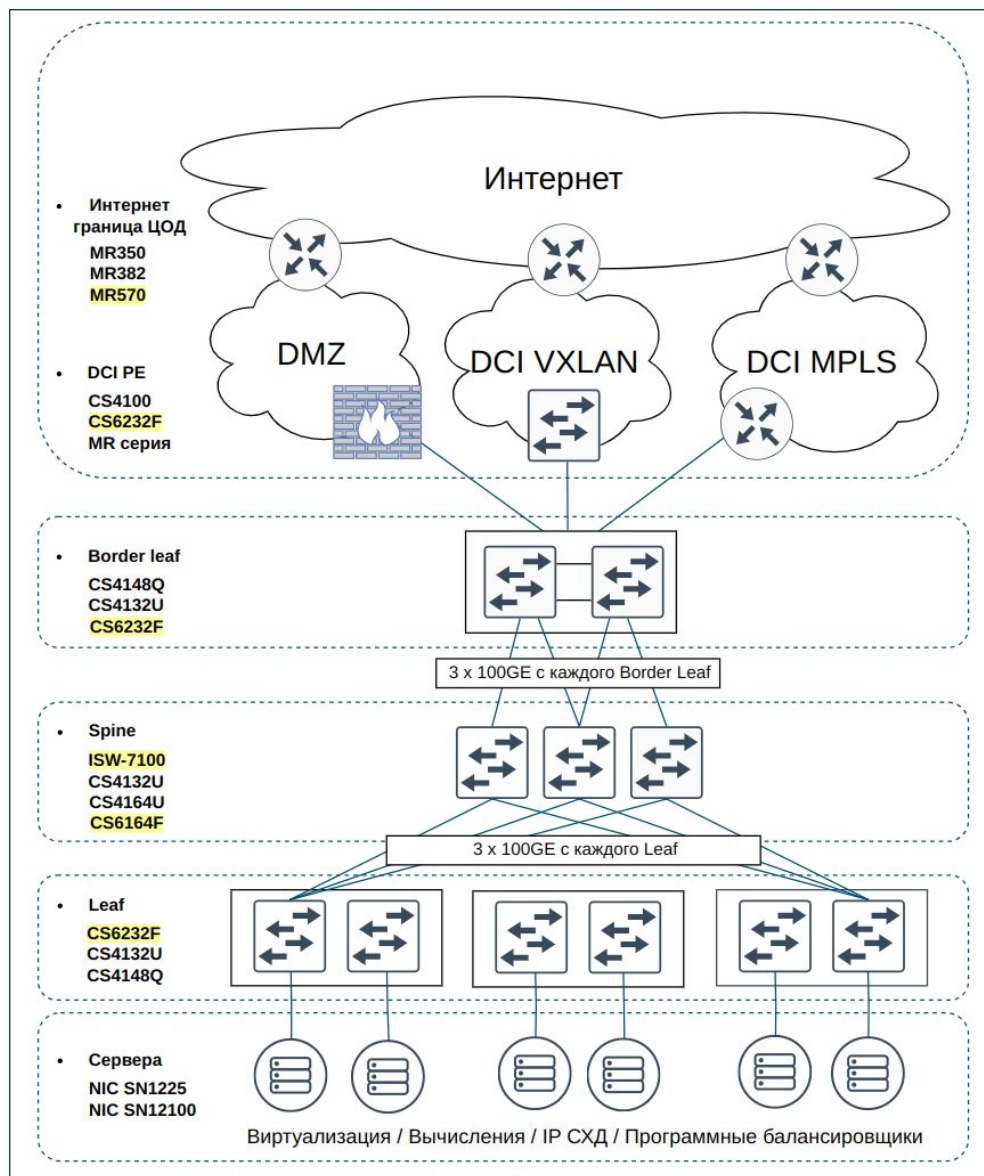
- Год основания – 2015, резидент ОЭЗ «Технополис г. Москва»

Интеграция сетевой инфраструктуры и МСЭ



- МСЭ с L2 MLAG или L2 EVPN-VXLAN
- МСЭ с L3 MLAG
- МСЭ с L3 EVPN-VXLAN
 - Статическая маршрутизация
 - BGP+BFD на каждый IP VRF
 - BGP+BFD с Central Services VRF
 - Георезервирование МСЭ
- Программно-определяемая инфраструктура (IaC)

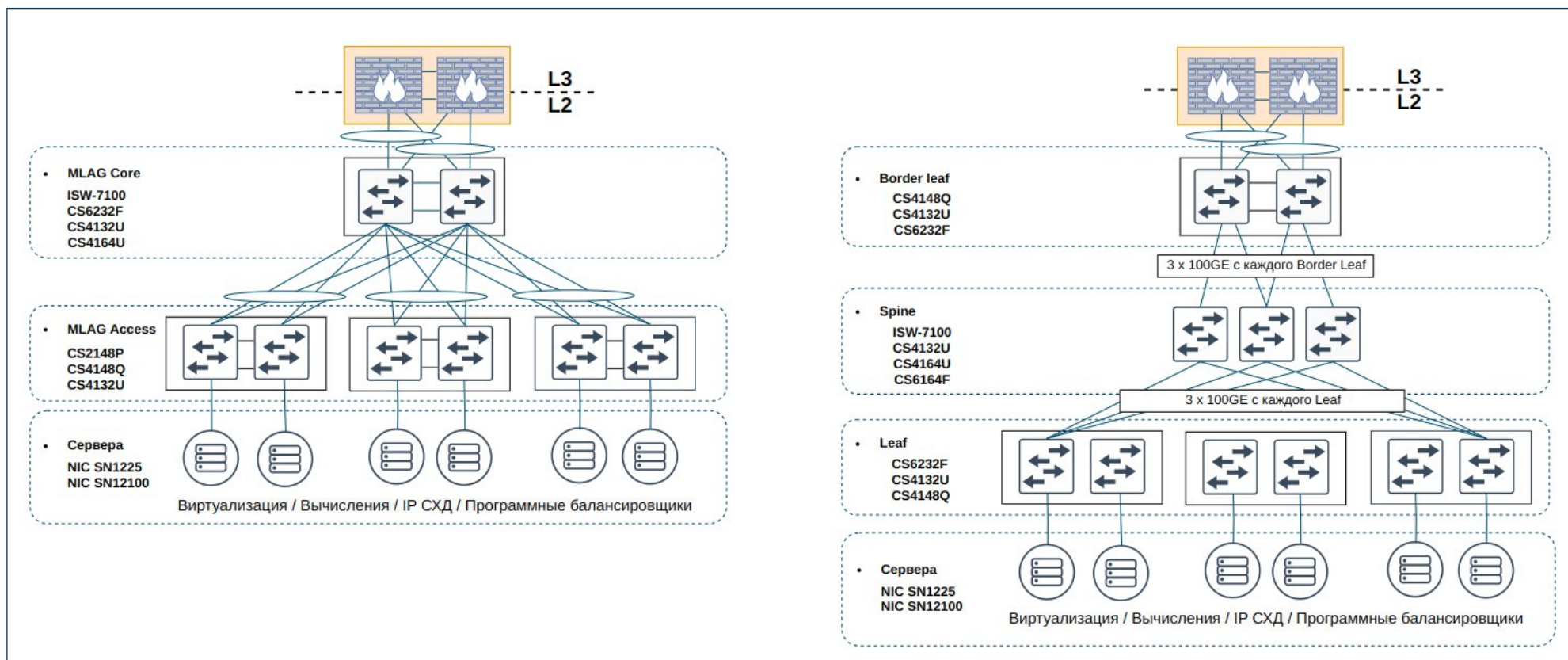
Коммутаторы ЦОД. Позиционирование



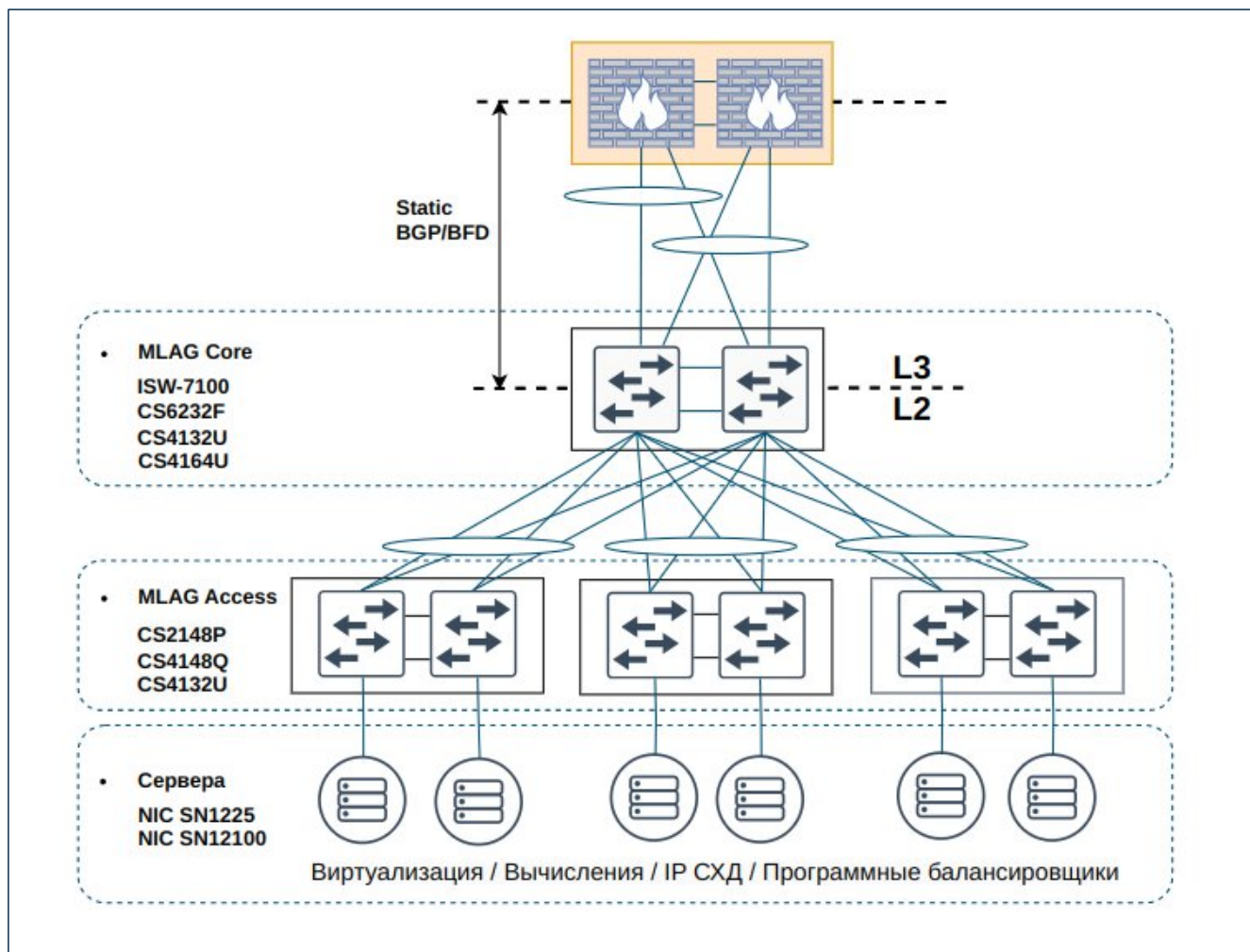
МСЭ с L2 MLAG или L2 EVPN-VXLAN

Шлюз подсетей располагается на кластере МСЭ – преимущественно, госпроекты

- Сетевая фабрика работает в режиме L2
- Кластер МСЭ подключается 2мя MLAG port-channel (или EVPN ES-LAG)

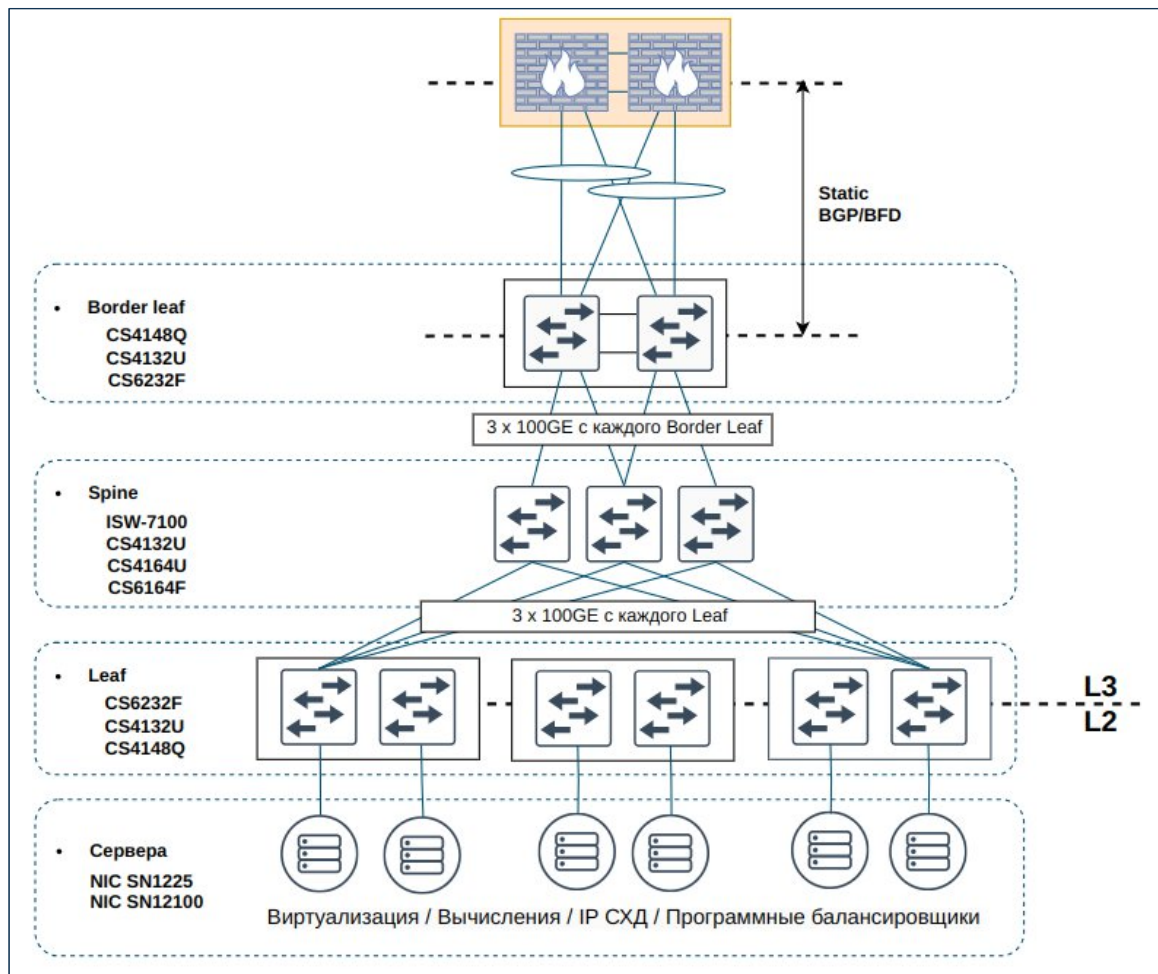


MCЭ с L3 MLAG Core



- L3 SVI с VRRP Active-Active
- Динамическая маршрутизация поверх peer-link
- VRF-lite: p2p VLAN SVI на каждый VRF
- Маршрутизация с MCЭ:
 - Static
 - BGP+BFD (RM: set NH = VRRP VIP)

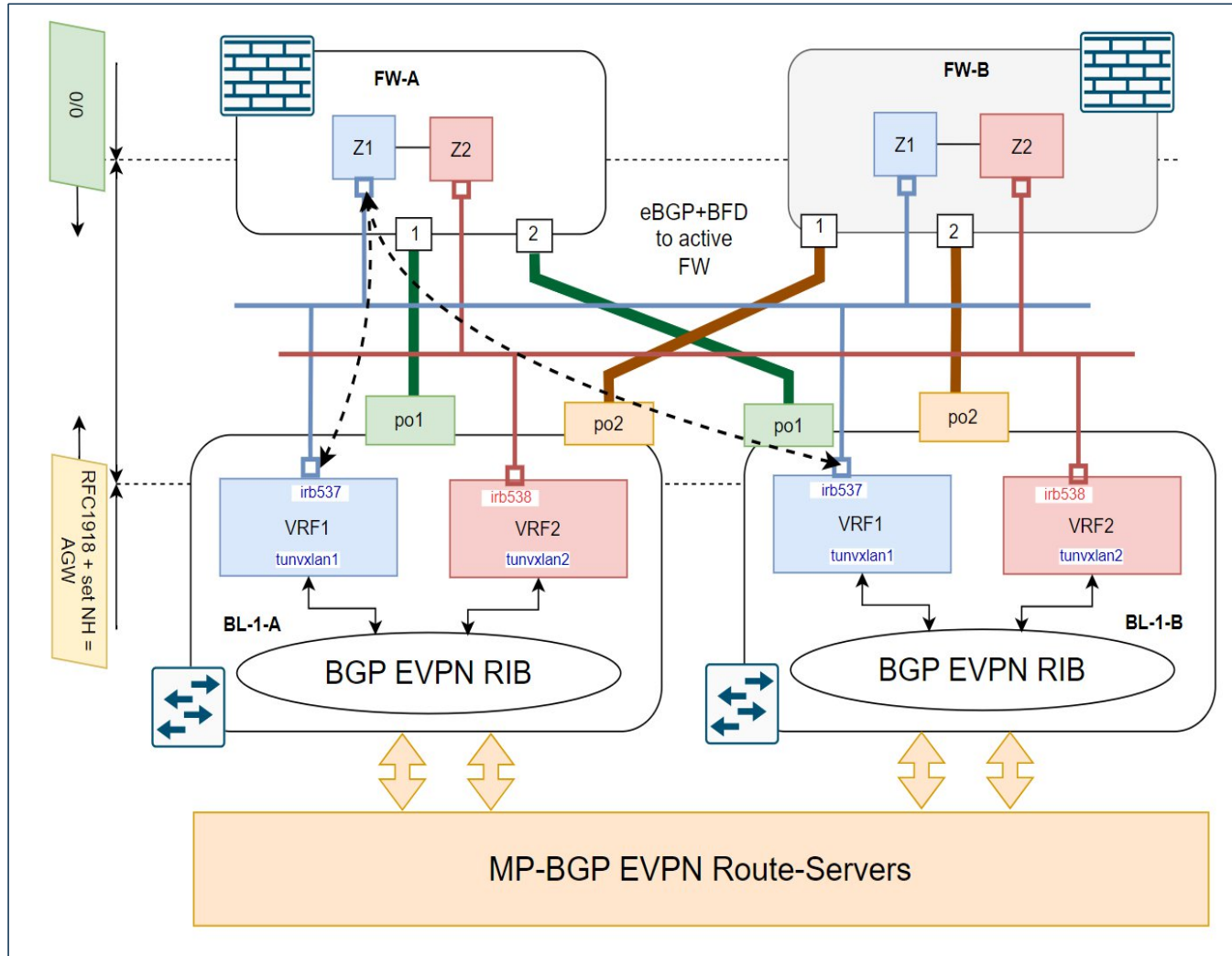
МСЭ с L3 EVPN-VXLAN - 1 Зона : 1 IP VRF



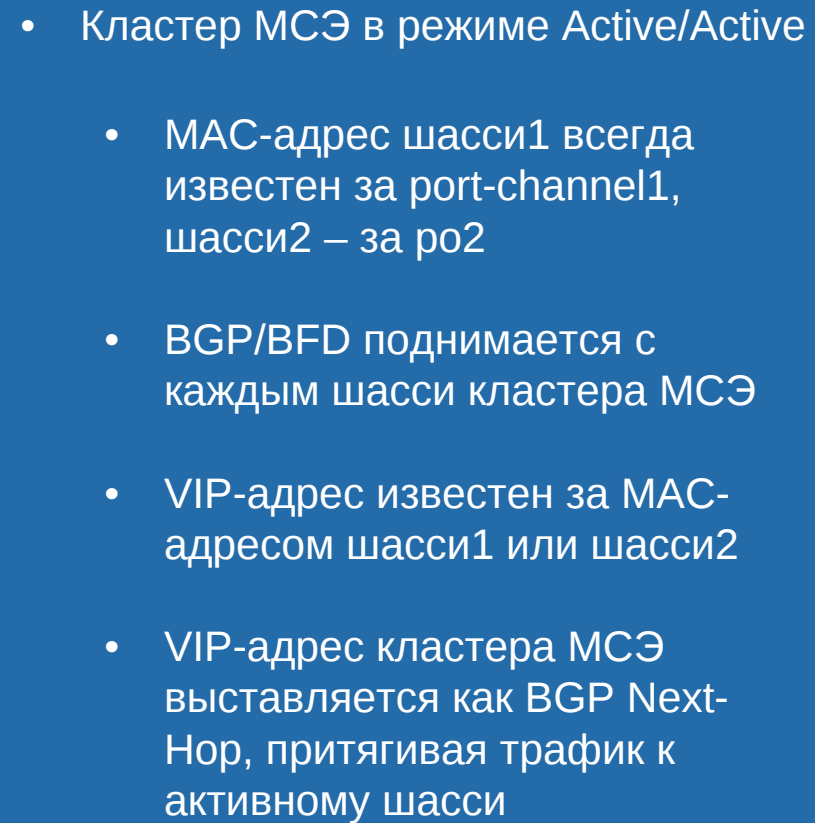
- Distributed GW AIRB/SIRB
- EVPN All-Active Multihoming
- L3-out VRF-lite
- IP VRF RT Route-leaking
- Маршрутизация с FW:
 - Per-VRF BGP через ES-LAG
 - Single-hop BGP/BFD на IRB-интерфейсы
 - Multihop BGP на Io интерфейсы, статика для Io на FW
 - RM set NH = AGW

МСЭ с L3 EVPN-VXLAN - 1 Зона : 1 IP VRF

Немного деталей

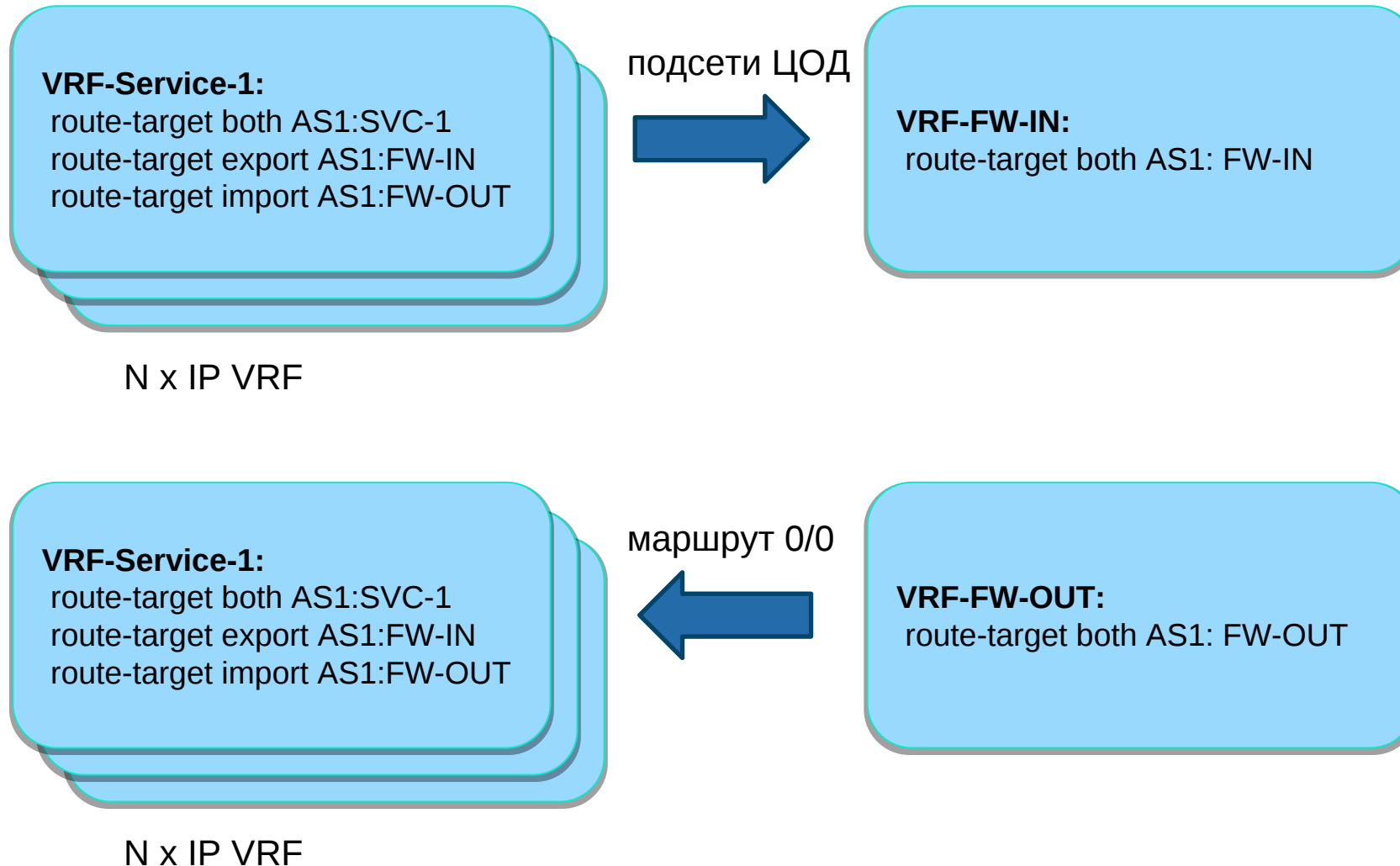


- Во избежание неоптимального прохождения трафика используется Route-Map с Set NH = AGW
- Кластер МСЭ в режиме Active/Standby
 - Единый MAC-адрес МСЭ переезжает между port-channel на сетевой фабрике
- BGP/BFD строится с активным шасси МСЭ
- Переход активного шасси в кластере МСЭ требует дополнительной сигнализации (BGP Graceful-Restart)



L3 EVPN-VXLAN - Central services

Сокращаем количество VRF/BGP

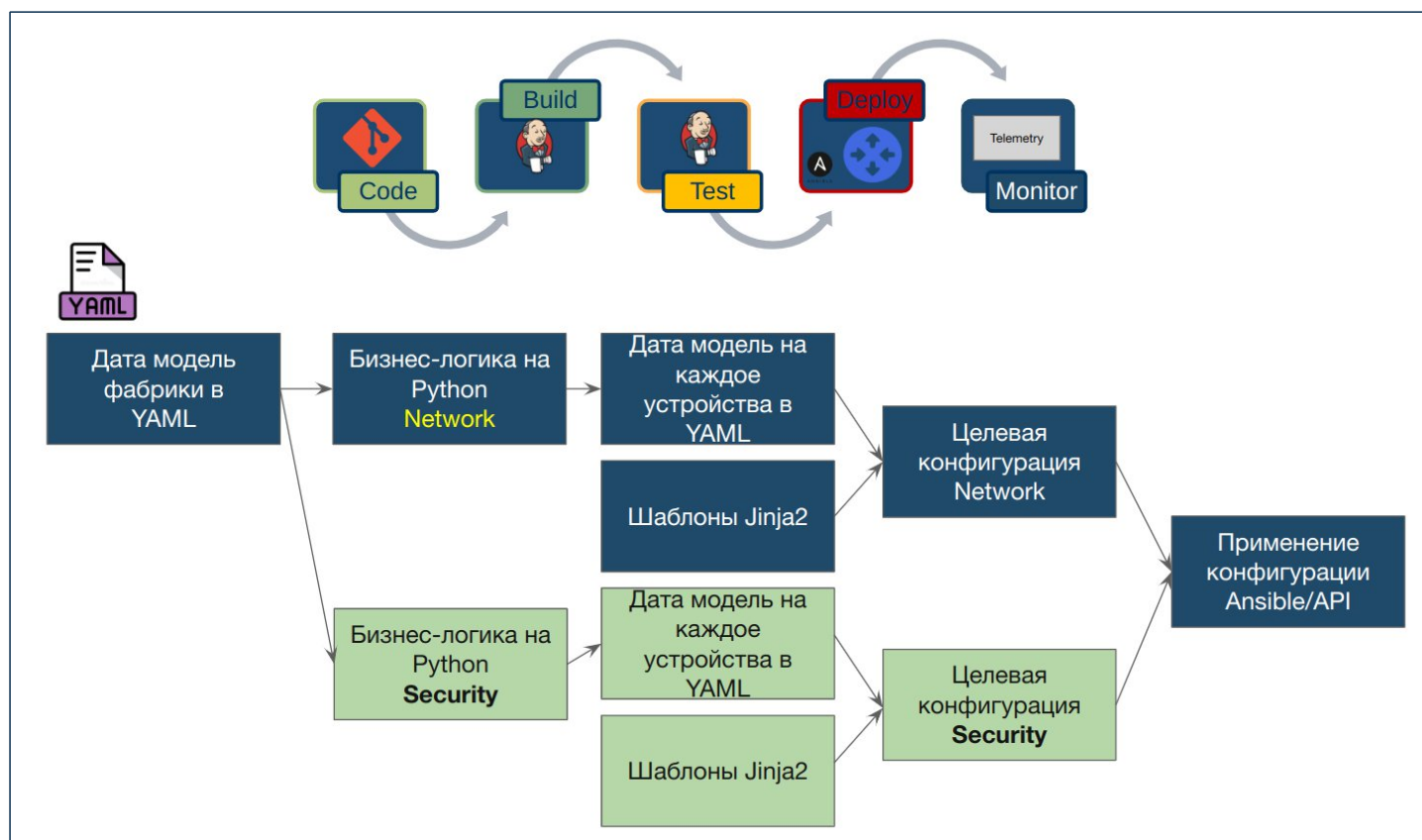


- Что делать, если хочется слишком много IP-VRF/зон безопасности?
- Central Services VRF свободит интеграцию сетевой фабрики и МСЭ к двум IP VRF – VRF IN и VRF OUT

Программно-определяемая инфраструктура ЦОД



- Infrastructure as Code (IaC) – правильный SDN на базе open-source
- Лучшая интеграция решений двух вендоров – оркестрация



Спасибо!

rs-se@b4com.tech