Gigamon®

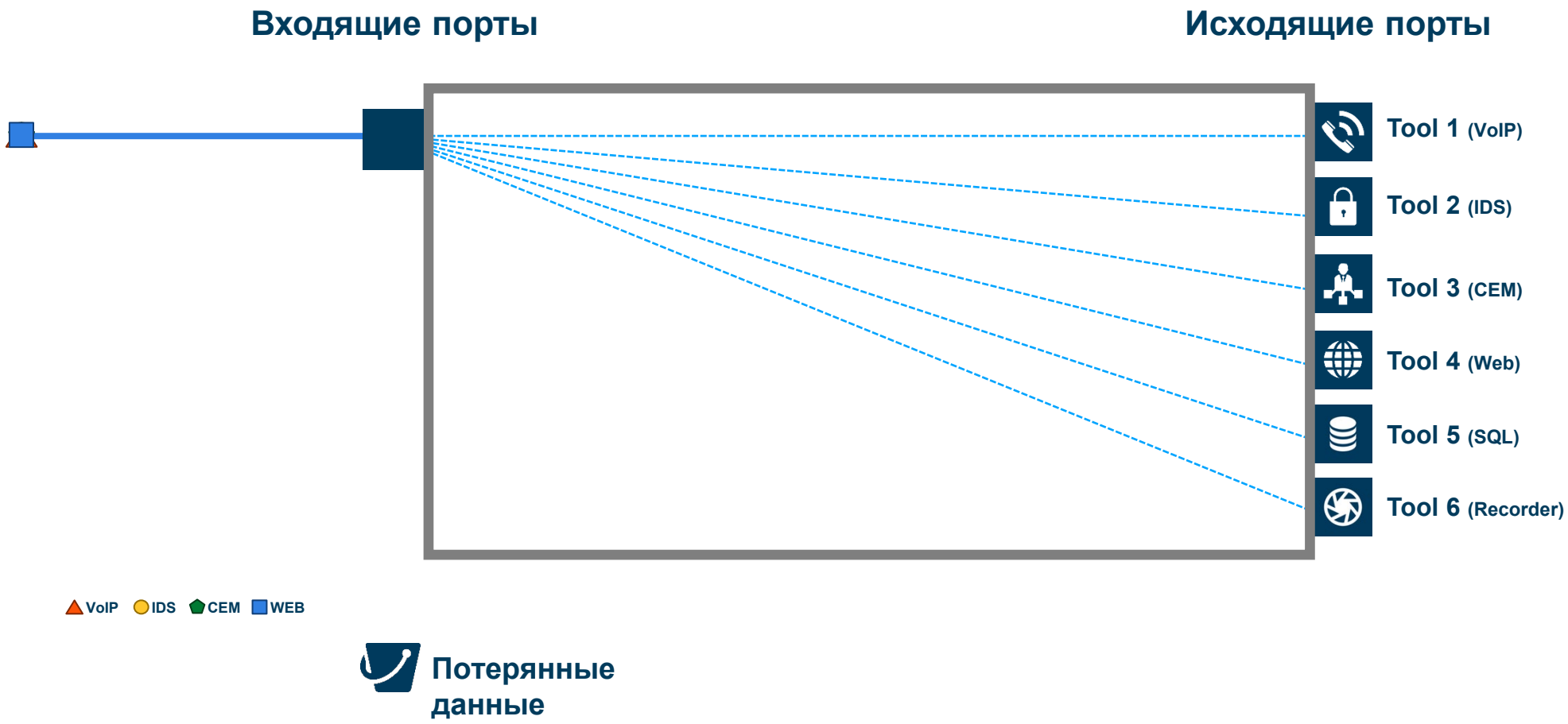
Gigamon. Копирование и фильтрация трафика. Как доставить копию трафика получателю

Александр Грачев

Менеджер по развитию бизнеса
Нетвелл

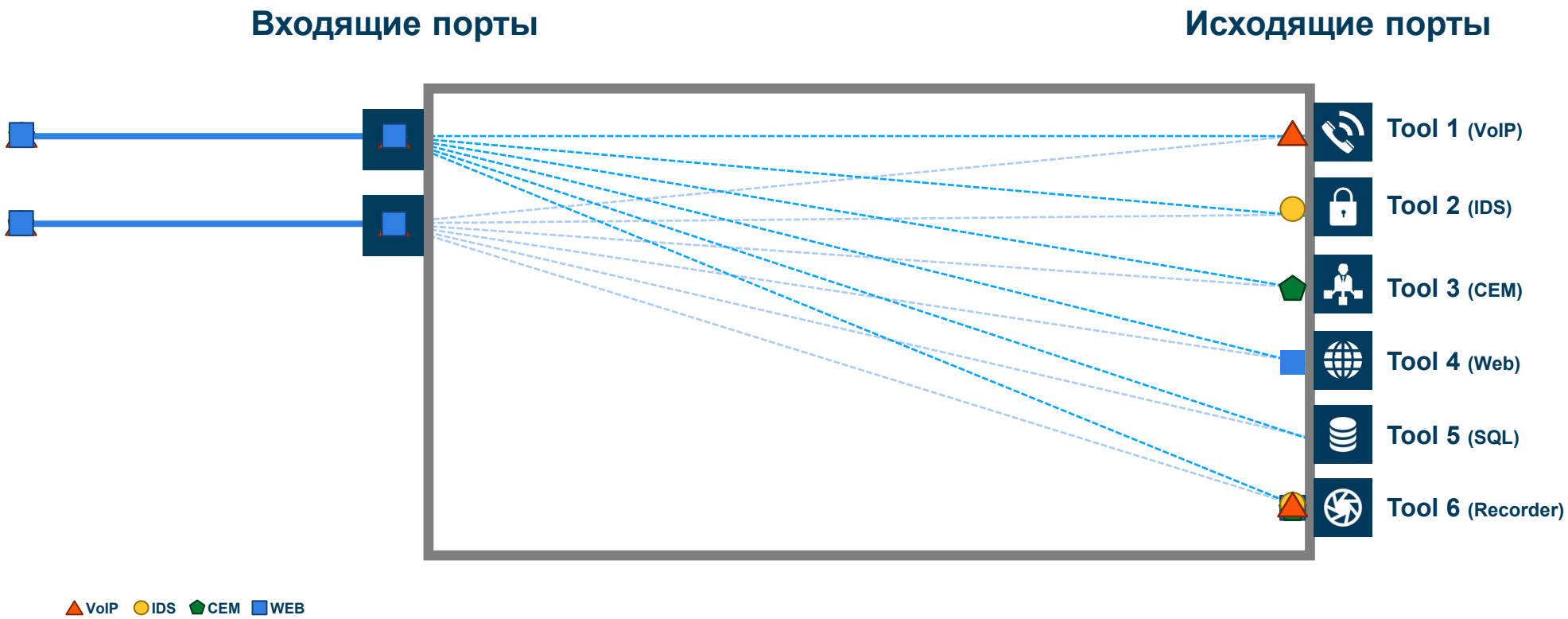
Фильтрация на входящих портах

Проблема с созданием уникальных копий трафика для каждого получателя



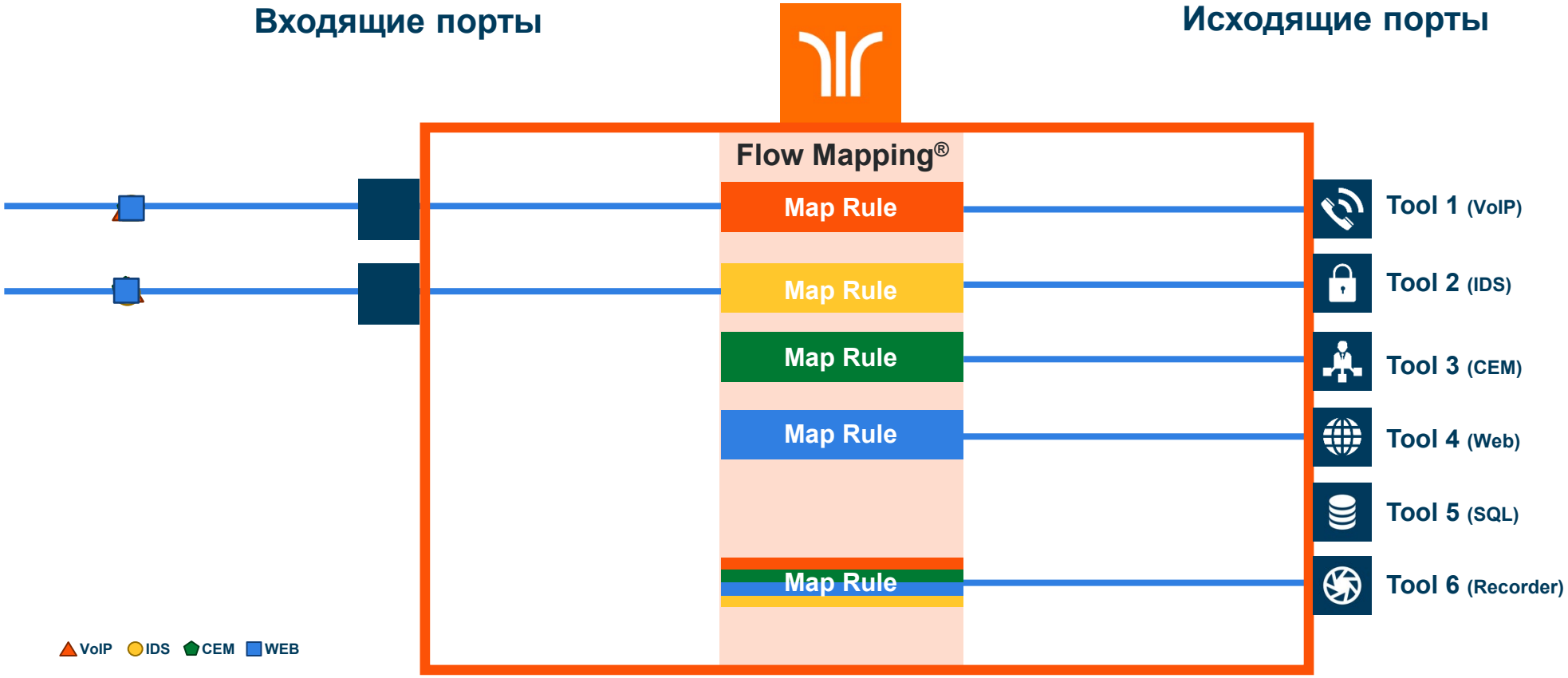
Фильтрация на исходящих портах

Высокий риск переподписки



Gigamon Flow Mapping®

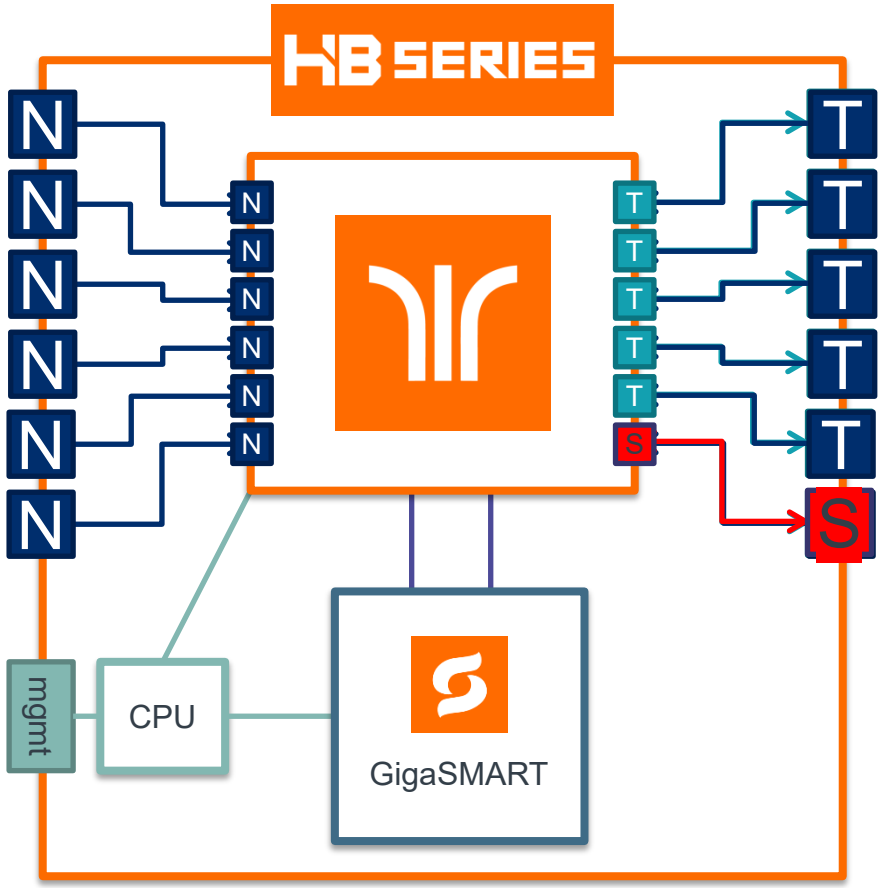
Каждый получатель получает только нужный ему трафик



Настраиваемые политики фильтрации не зависят от объемов трафика и портов источников/получателей

Структура оборудования

ГДЕ ЧТО НАХОДИТСЯ



- 40Gb\80Gb: HC2
- 2 x 100Gb: HC3
- 20Gb: HC1

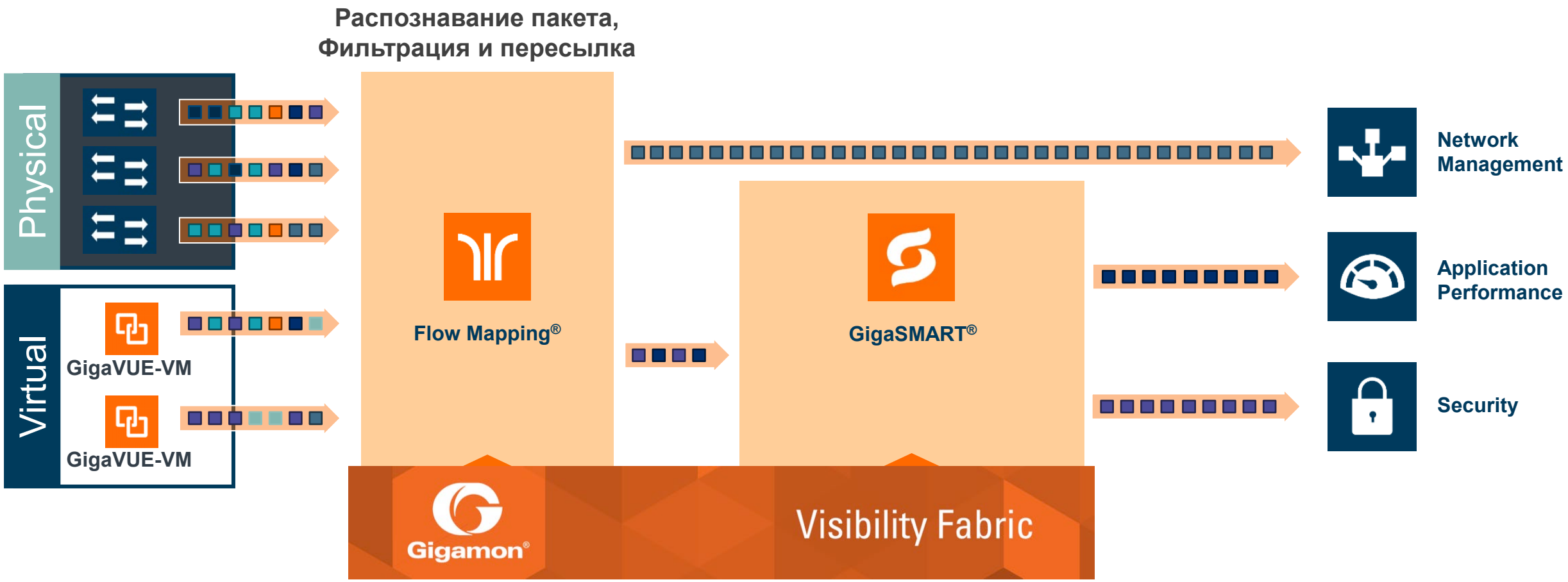
Программная обработка трафика

- Ограниченна ресурсами процессоров
- Добавляет задержку в прохождение пакетов

Дополнительное «железо»

- Для SSL Decryption
- Можно пропустить трафик через удаленное оборудование по Stack Links

Путь пакета от источника к получателю



Какие бывают типы портов, группы портов и бандлы портов

Самые часто используемые типы это Network, Tool, Hybrid. Но это далеко не все порты с которыми вы можете встретиться:

- Network Port
- Tool Port
- Hybrid Port
- Circuit ID Port
- Tool GigaStream
- Stack Port
- ~~Gateway Port~~
- GigaSMART Engine
- Network Port Group
- Tool Port Group
- Hybrid Port Group
- Circuit ID Port Group
- Hybrid GigaStream
- Stack GigaStream
- GigaSMART vPort
- Network Tunnel Port
- Tool Tunnel Port
- Hybrid Tunnel Port
- Circuit ID Tunnel Port
- Circuit GigaStream
- Network Port Pair

- Inline Network Port
- Inline Tool Port
- Inline Network
- Inline Tool
- Inline Network Group
- Inline Tool Group
- Inline Tool Serial

Gigamon

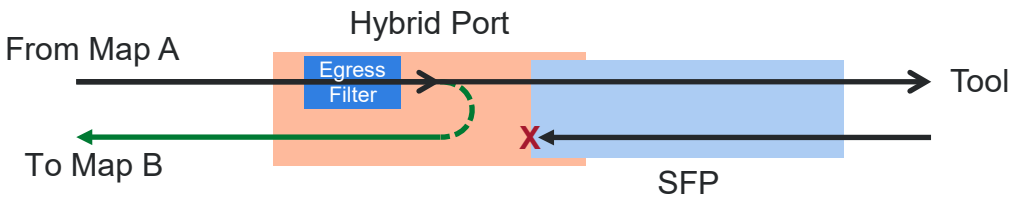
Типы портов

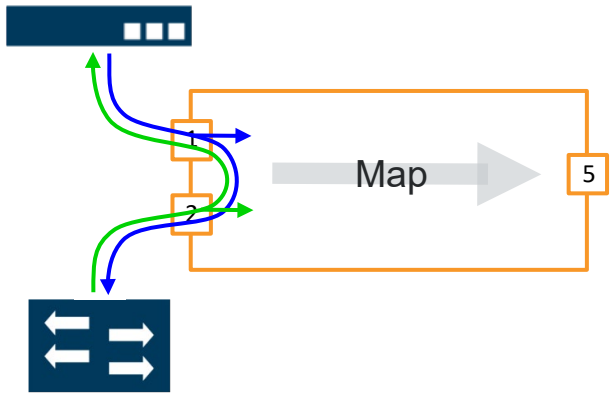
Port Type		Description
Network	N	Входящий порт
Tool	T	Исходящий порт
Hybrid	H	Исходящий порт с внутренним заворотом
Stack	S	Для кластера (не меньше чем 10G)
Circuit	C	Для некоторых видов тунелей и Fabric Maps
Inline Network	iN	Для Bypass. Интеграция в сетевое соединение
Inline Tool	iT	Для Bypass. Подключение Inline устройств
Engine	E	Порт модуля GigaSMART.

Дополнительная информация о портах

Как порты взаимодействуют с внешним оборудованием:

- Network Port: только для входящего трафика и ничего не передает обратно
- Tool Port: Только передает трафик, весь входящий трафик отбрасывается
- Hybrid port: Такой же как и Tool port, но трафик передаваемый через этот порт можно использовать для других сессий фильтрации. Это позволяет создавать параллельные ветви фильтрации и копирования. Если карта использует Hybrid port как источник, то она не зависит от состояния линка в этом порту. В нем даже может не быть вставлен трансивер.
- Stack port: не допускается подключения к коммутаторам или маршрутизаторам т.к. Используется модифицированный ethernet
- Network Port Pair: Два Network порта можно объединить в пару и сделать из них логический TAP. Медиаконверция разрешена.

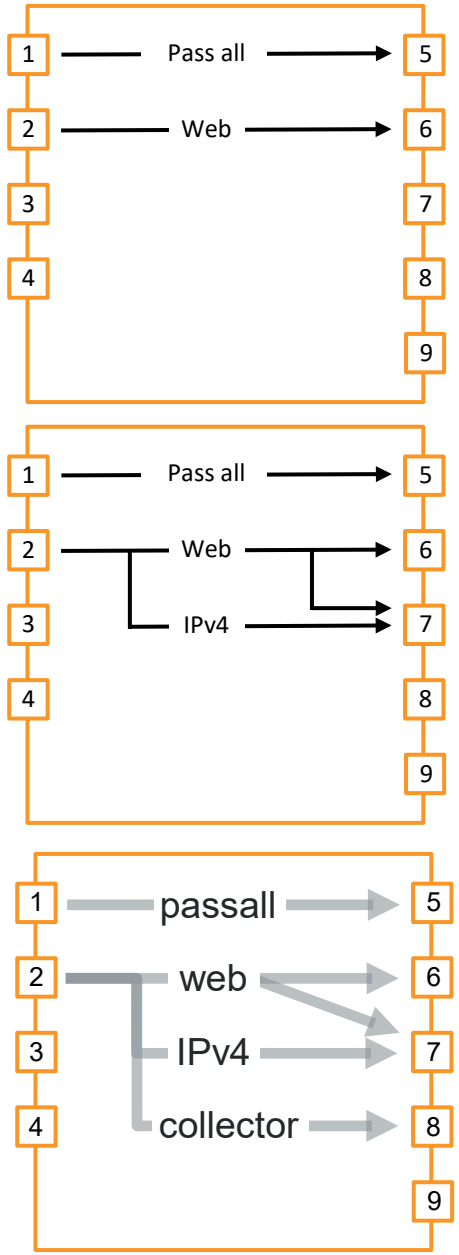




Flow Mapping - основы

Типы карт фильтрации (subtype):

- Pass all: копирует весь трафик. Может работать параллельно с другими картами
- ByRule – позволяет копировать трафик согласно политикам
  - Карты ByRule конкурируют за пакет, то первого срабатывания
  - Если карта ByRule использует один набор входящих потов, то другая карта ByRule не сможет использовать один или несколько портов из этого набора, только все порты.
- Collector: позволяет копировать весь трафик, который не описан другими картами ByRule. Не может существовать ранее созданных карт ByRule

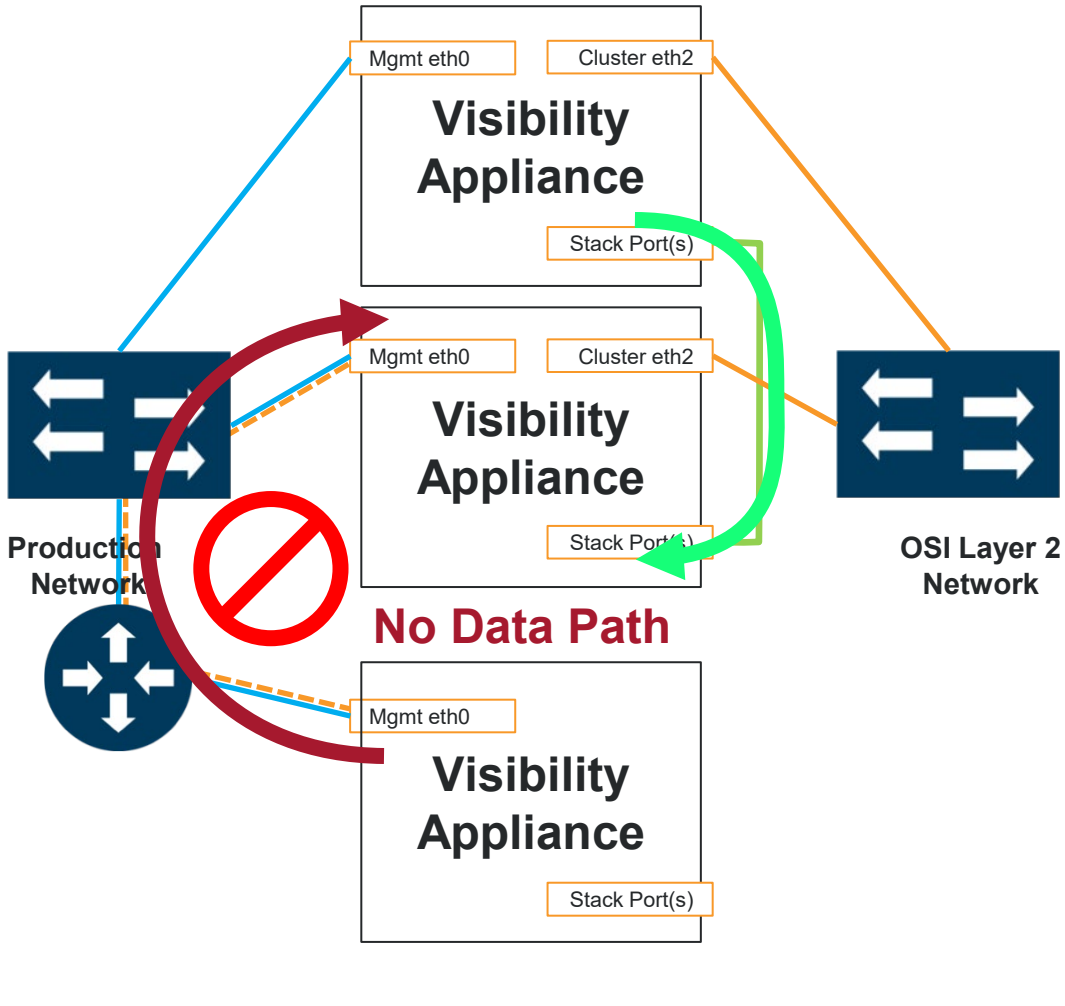


Кластер Out-of-Band

Out-of-Band Cluster

Out-of-band

- Предпочтительный ТИП кластера
- Control plane и Data Plane проходят по разным интерфейсам
- Только Master и Standby должны иметь адреса управления из одной подсети, остальные члены кластера могут быть из других подсетей.
- Наиболее стабильный тип кластера
- Поддерживаемые топологии – цепь, звезда, смешанная цепь+звезда



Кластер Inband

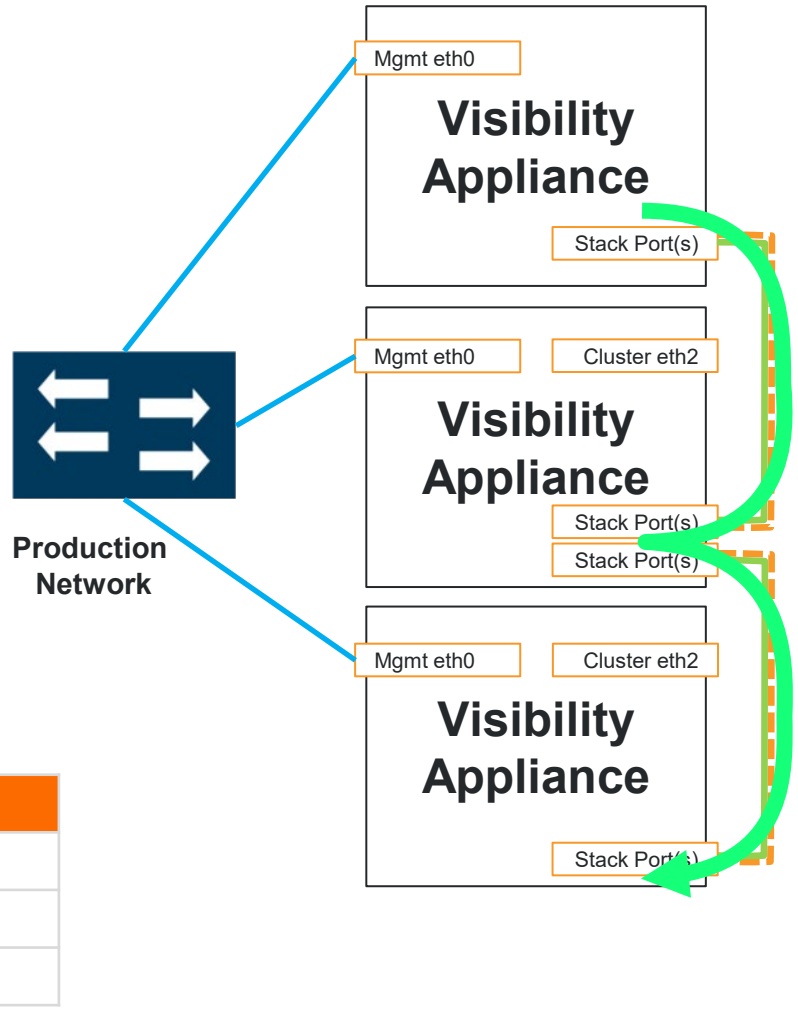
Inband Cluster

Choose a cluster architecture

There are three general cluster architectures to select from.

1. Out-of-band
   - Preferred
   - Single path between appliances
   - Supports remote nodes

2. Inband
   - Control plane и Data Plane проходят по разным интерфейсам
   - Поддерживаемые топологии – цепь, звезда, смешанная цепь+звезда

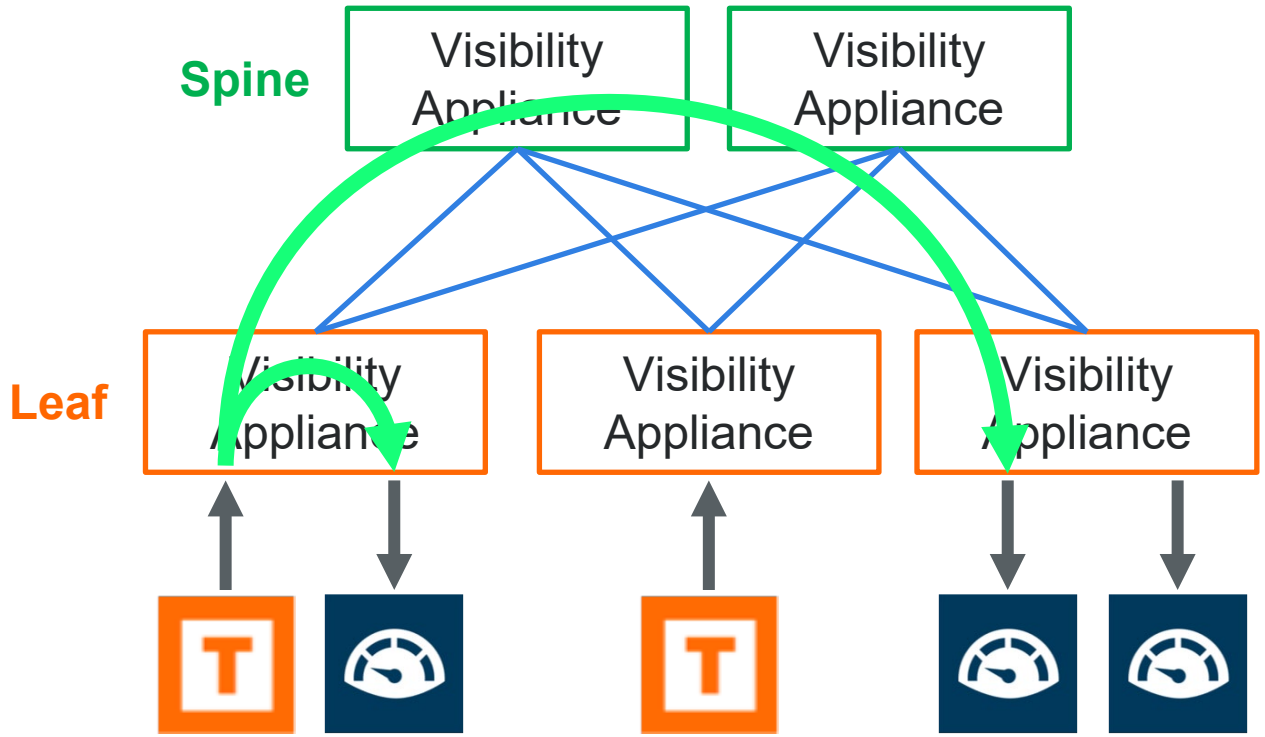


Кластер Spine Leaf

Choose a cluster architecture

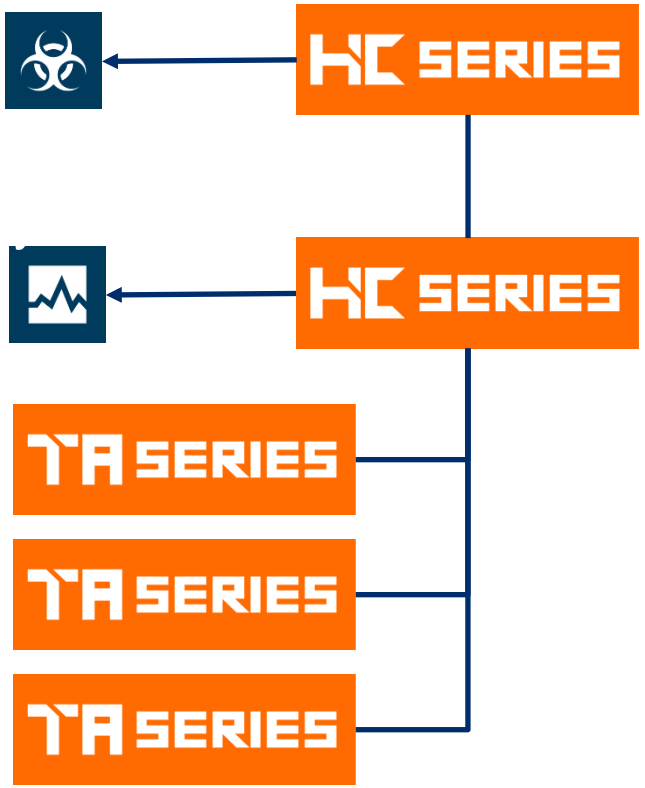
There are three general cluster architectures to select from.

1. Out-of-band
   - Preferred
   - Single path between appliances
   - Supports remote nodes
2. Inband
   - Supports only local nodes
   - Single path between appliances
3. Leaf and Spine
   - Развитие кластера Out-Of-Band с резервированной архитектурой



Традиционный кластер

ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ДЛЯ ОБЪЕДИНЕНИЯ УСТРОЙСТВ



Преимущества:

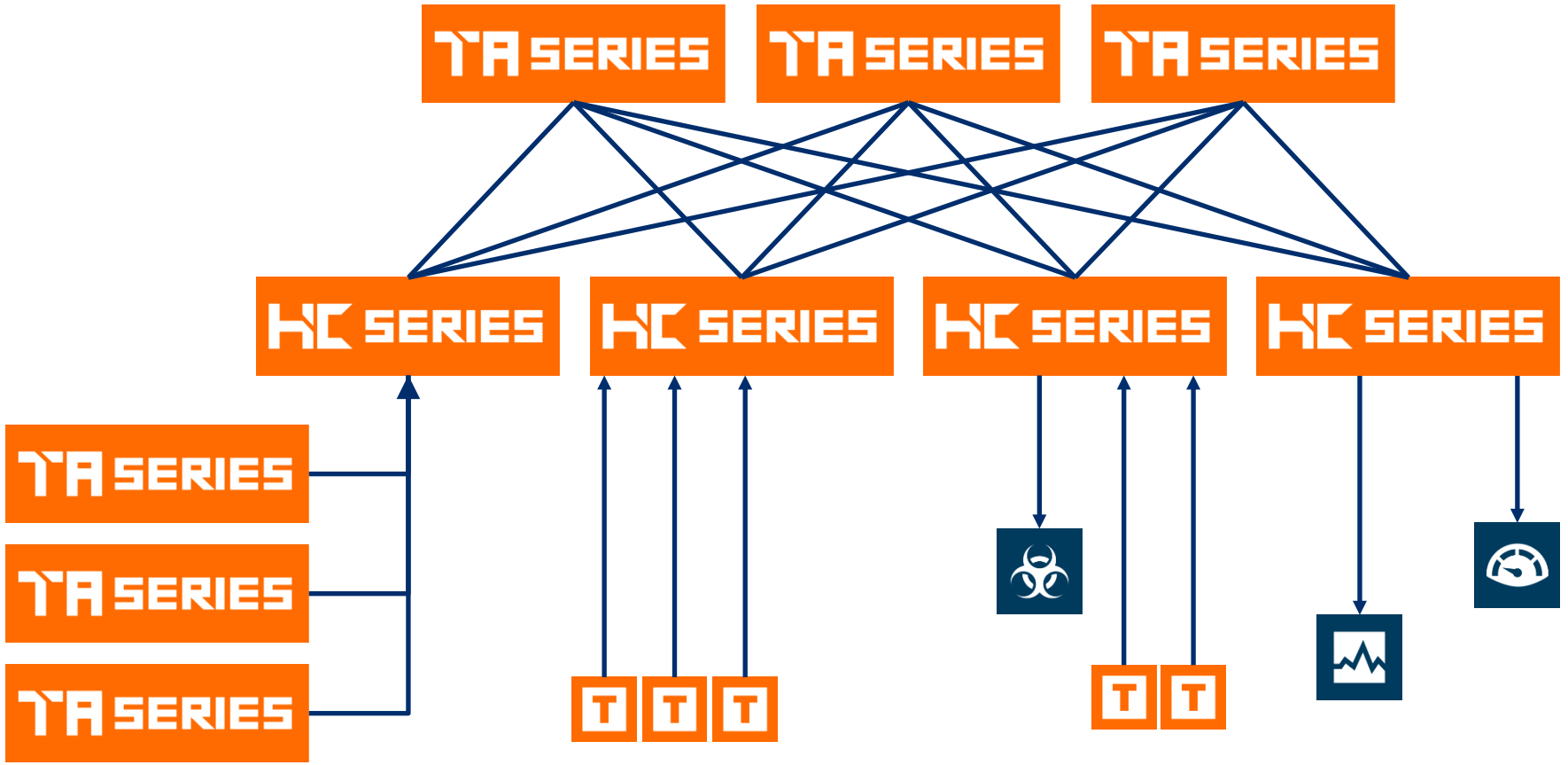
- ✓ Устройства объединенные в кластер имеют единое управление и работают как единая платформа.
- ✓ Возможность использования функций GigaSMART для всех устройств в кластере, при наличии соответствующего модуля и лицензий хотя бы на одном устройстве.
- ✓ До 32 устройств в одном кластере.
- ✓ Наилучший способ обмена трафиком между устройствами Gigamon

Недостатки:

- – Отсутствие резервированной архитектуры.
- – Необходимо L1 соединение устройств, из-за использования расширений Ethernet

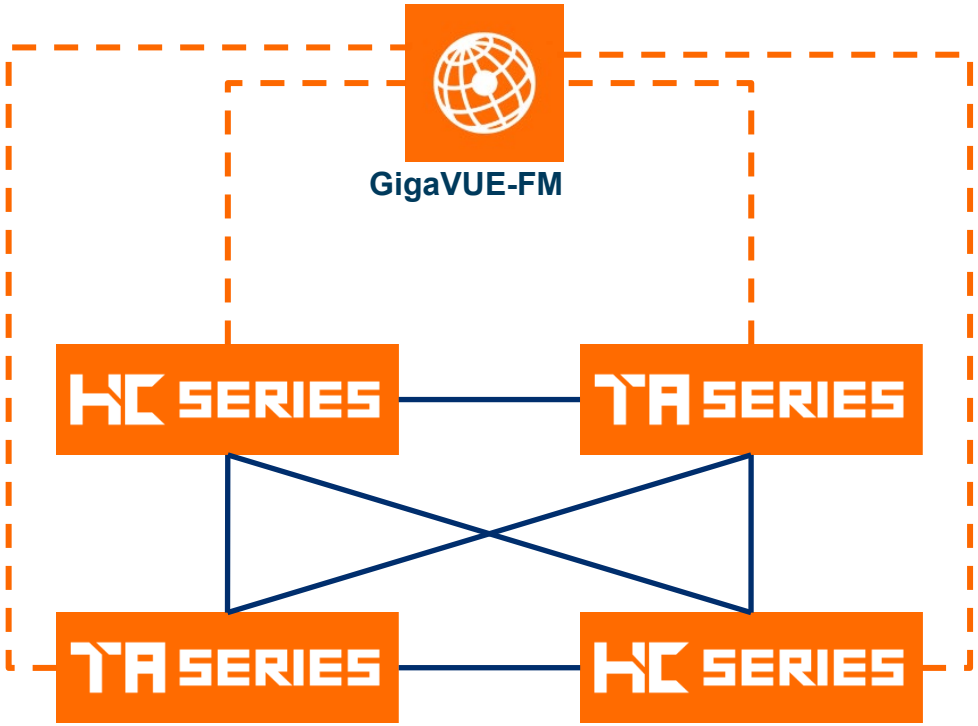
Leaf-Spine

ОТКАЗОУСТОЙЧИВАЯ АРХИТЕКТУРА



Fabric Maps

ПОСТРОЕНИЕ РАСПРЕДЕЛЕННЫХ ПОЛИТИК КОПИРОВАНИЯ ТРАФИКА БЕЗ КЛАСТЕРИЗАЦИИ



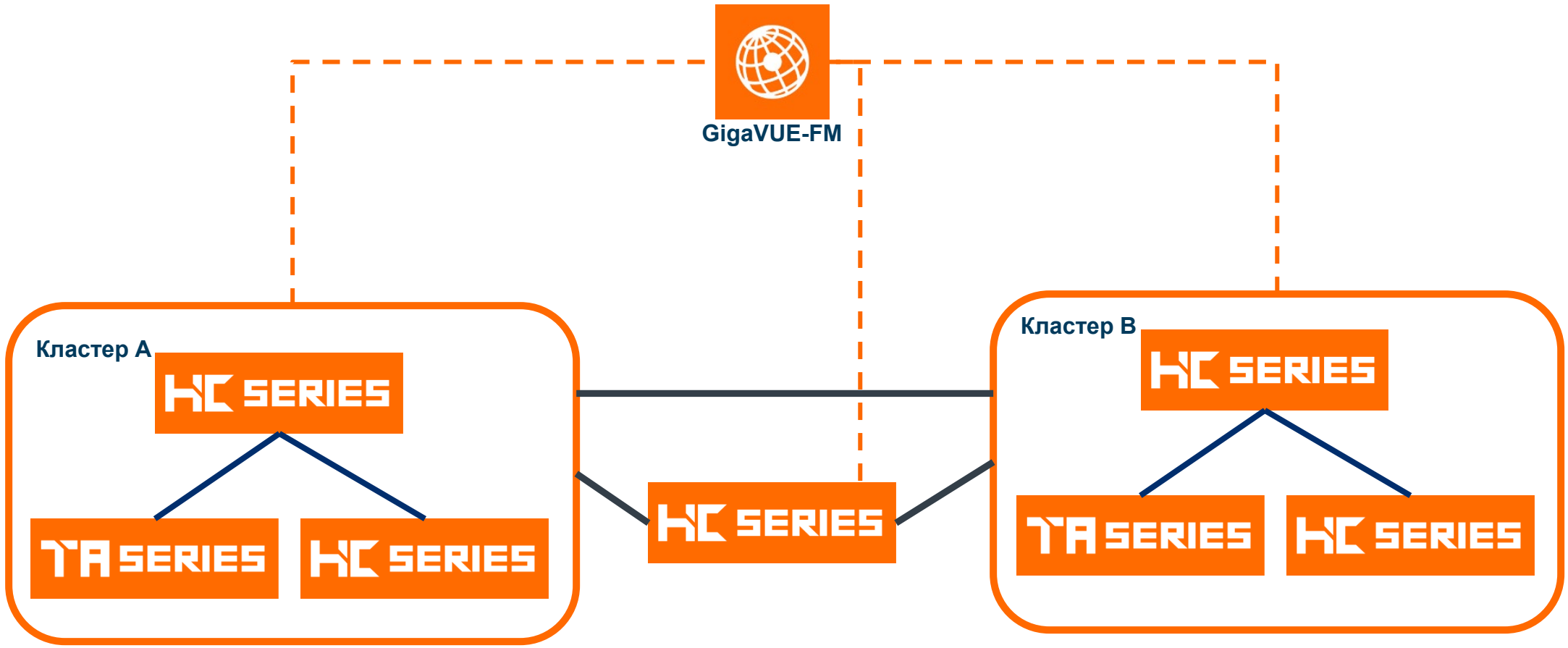
Преимущества:

- ✓ Все устройства работают в stand along режиме.
- ✓ GigaVUE-FM создает политики копирования и фильтрации на каждом устройстве.
- ✓ Вместо кластерных интерфейсов используются Circuit интерфейсы, которые работают поверх коммутируемых сетей.
- ✓ Возможность использования функций GigaSMART для всех устройств, при наличии соответствующего модуля и лицензий хотя бы на одном устройстве.
- ✓ До 200 устройств может работать совместно.
- ✓ Еще один «Наилучший способ обмена трафиком между устройствами Gigamon»
- ✓ Поддержка любой топологии соединения устройств
- ✓ В случае потери связи с между FM и пакетным брокером, политики пропускания трафика не изменяются.

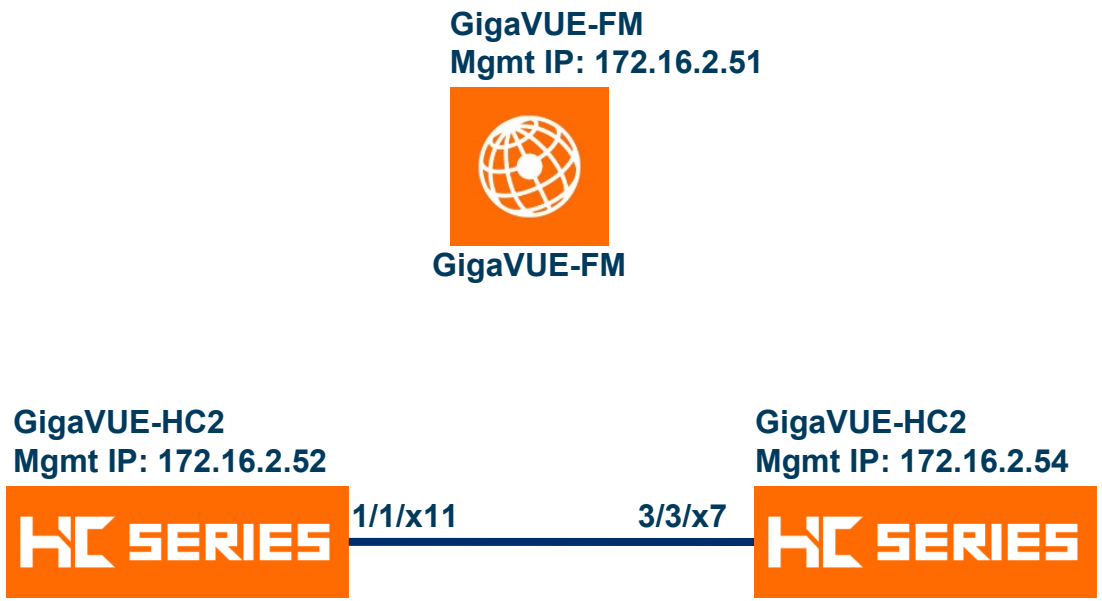
Недостатки:

- – Требуется GigaVUE-FM. Но разве это недостаток?

Комбинирование Fabric Maps и кластера



Лабораторная инталяция




```
! Custer config data
cluster ID Netwell-test
cluster name Netwell-test
Cluster master ip address 172.16.2.53 /24
```

Пример конфигурирования кластера Out-of-Band через CLI (1)

! на мастере делаем

cluster id Netwell-test

cluster name Netwell-test

cluster interface eth0

cluster master interface eth0

cluster master address vip 172.16.2.53 /24

cluster enable

!! дальнейшие конфигурации выполняем через 172.16.2.53

!! мастер переходит в кластер с активным box-ID, chassis и card

Пример конфигурирования кластера Out-of-Band через CLI (2)

! добавление нового устройства в кластер

! Выполняем на новом устройстве, его адрес управления может быть из другой подсети

cluster ID Netwell-test

cluster name Netwell-test

cluster interface eth0

no cluster master auto-discovery

cluster master address primary ip 172.16.2.52

cluster enable

!! на VIP мастера далаем

show chassis

chassis box-id 3 serial-num C027C

card all

Gigamon

Пример конфигурирования кластера Out-of-Band через CLI (3)

! Порты соединяющие устройства переводим в тип STACK

!! на VIP мастера далаем

stack-link alias HC2-HC2 between ports 3/3/x7 and 1/1/x11

План подготовки к конфигурированию Fabric Maps.

1) включаем GDP на портах между устройствами.
2) включаем GDP на шасси.
3) порты соединяющие устройства делаем TYPE=Circuit
4) создаем Gigastream из портов соединяющих устройства, даже если в каждом gigastream будет всего один порт.
5) делаем rediscovery устройств в FM.
6) теперь конфигурируем fabric maps.

Gigamon®

Благодарю за внимание!