NIAGARA NETWORKS

Обзор решений Niagara Networks

Александр Грачев

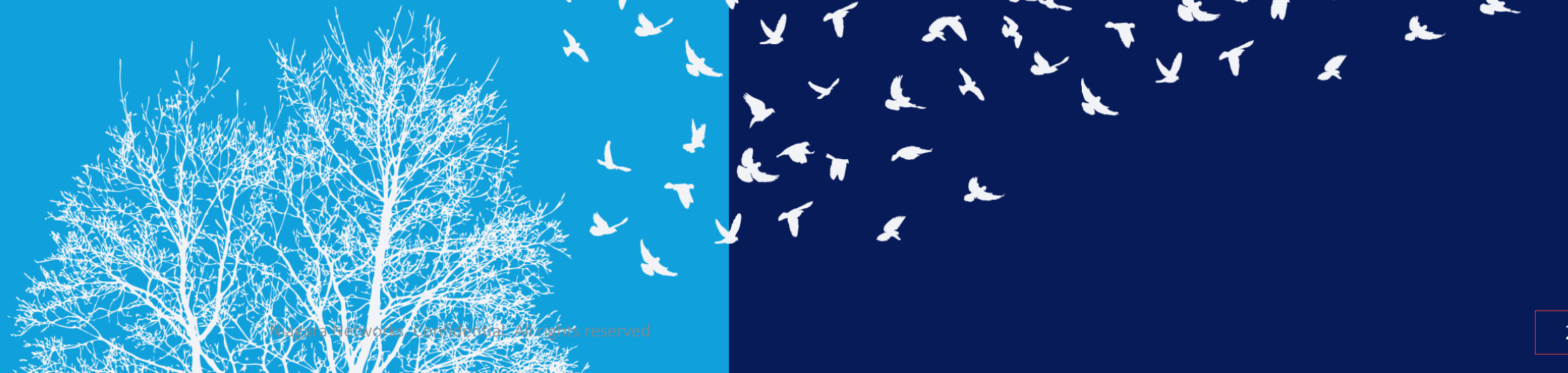
BDM Netwell

Niagara Networks

provides high performance

Network Visibility Solutions

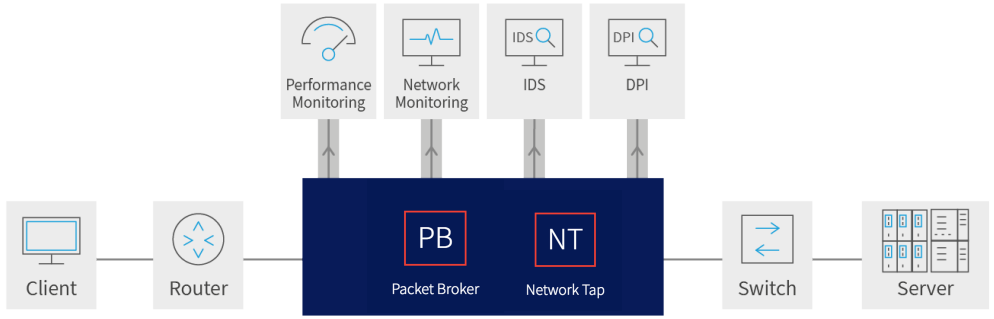
to allow seamless administration of **security** solutions, **performance** management and network **monitoring.**



Портфолио продуктов

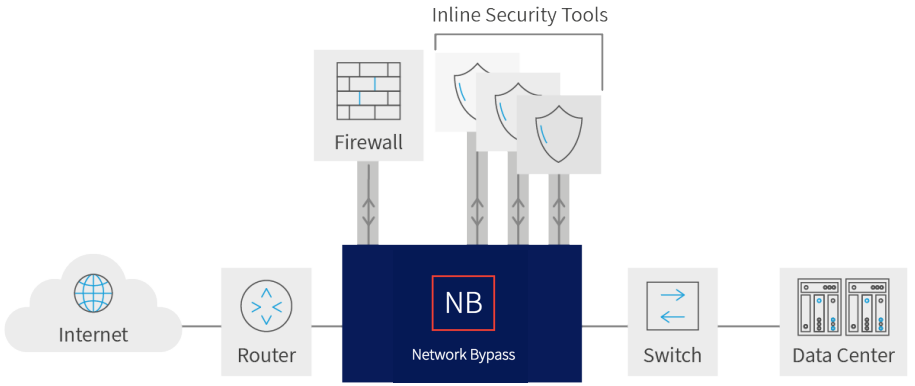
2 Основных решения

Копирование и фильтрация трафика (Packet Broker)



- ✓ TAP, безопасно и надежно копируют трафик из сетевых каналов.
- ✓ Пакетные Брокеры – агрегируют и консолидируют копии трафика
- ✓ Передают только нужный трафик каждому получателю
- ✓ Распределяют копии трафика между множеством получателей
- ✓ Снимают ограничения по количеству систем анализа, мониторинга, безопасности работающих в сети.

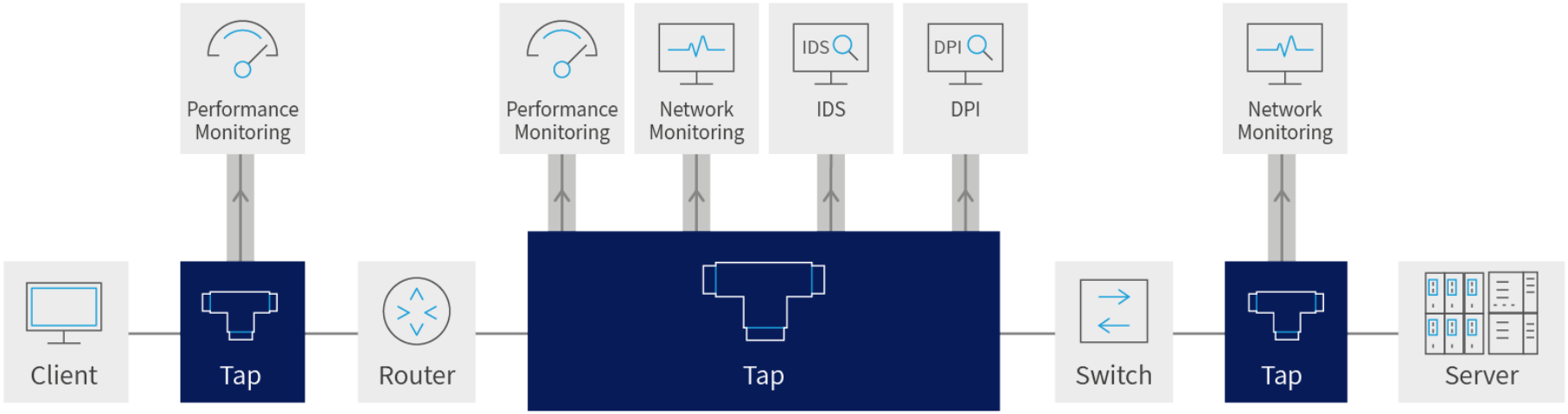
ByPass – подключение активных средств ИБ



- ✓ ByPass – отказоустойчивое средство подключения активных средств безопасности
- ✓ Упрощает интеграцию Inline устройств в сеть (нет необходимости согласования подключения с сетевиками)
- ✓ Горизонтальное масштабирование Inline устройств, распределение нагрузки между несколькими устройствами
- ✓ Возможность пропускания только нужного трафика через Inline устройство
- ✓ Подключение нескольких Inline устройств через один ByPass

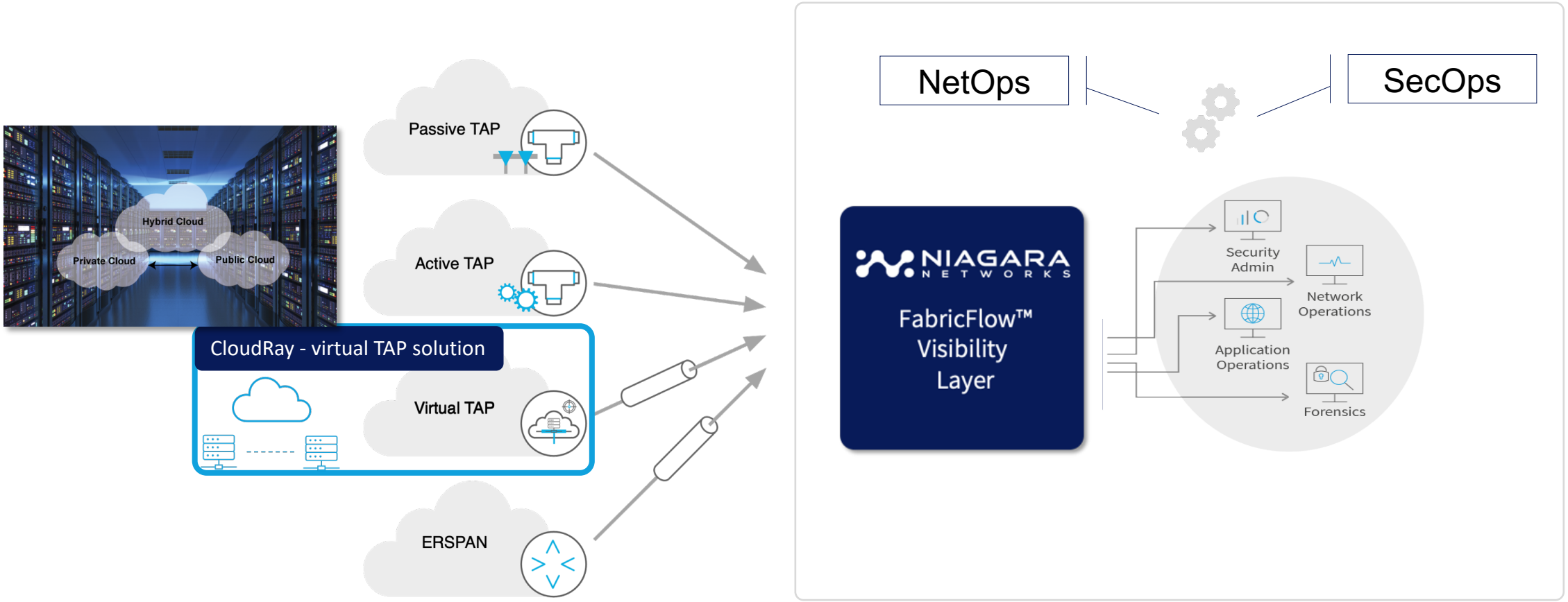
Подключение средств мониторинга

Делаем доступным трафик каждого сетевого интерфейса



Решения Niagara Networks для копирования и фильрации трафика

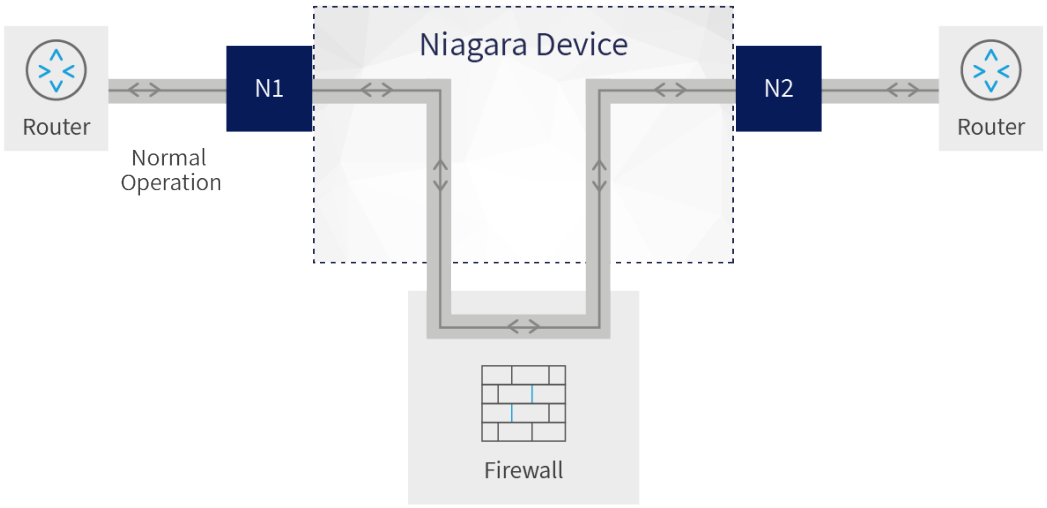
Полный набор универсальных инструментов для копирования трафика из любой точки сети.



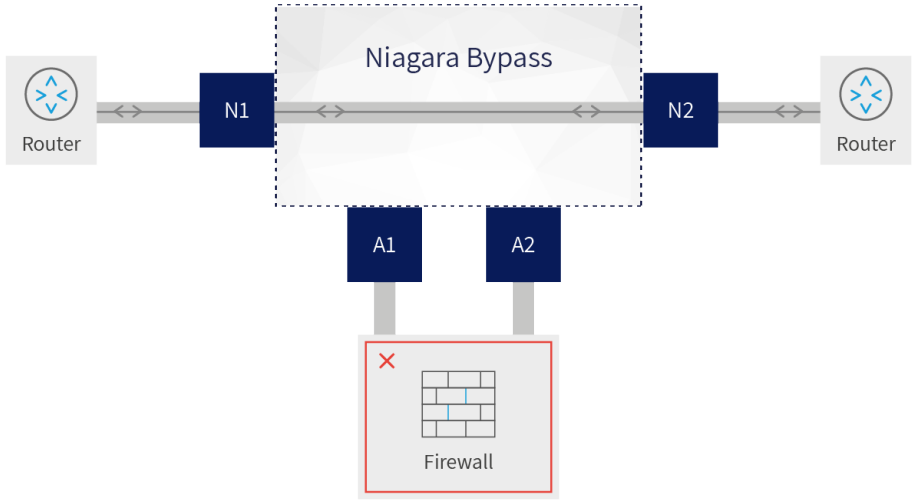
Копирование, фильтрация, агрегация и модификация копии трафика

ByPass

Защищаем сеть от сбоев средств ИБ



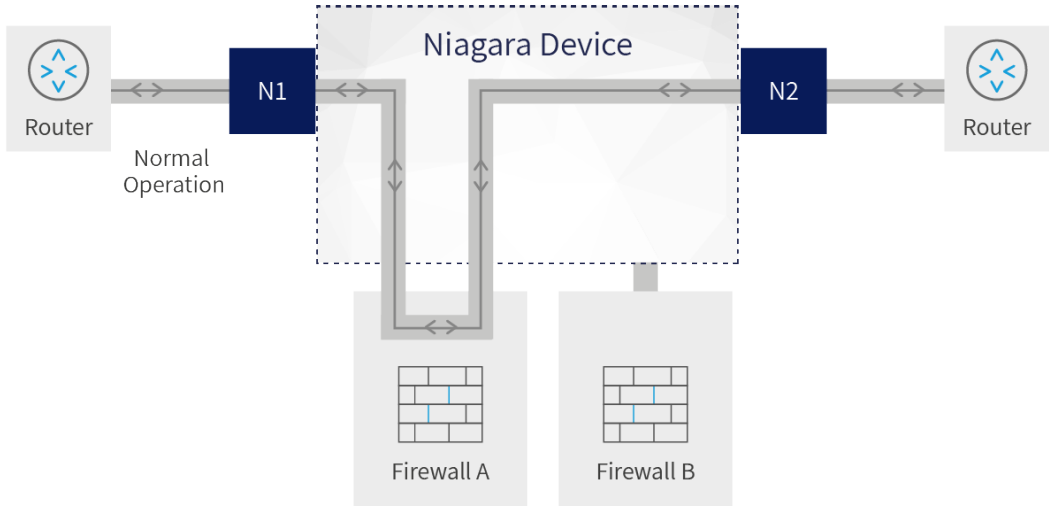
Обычный режим работы

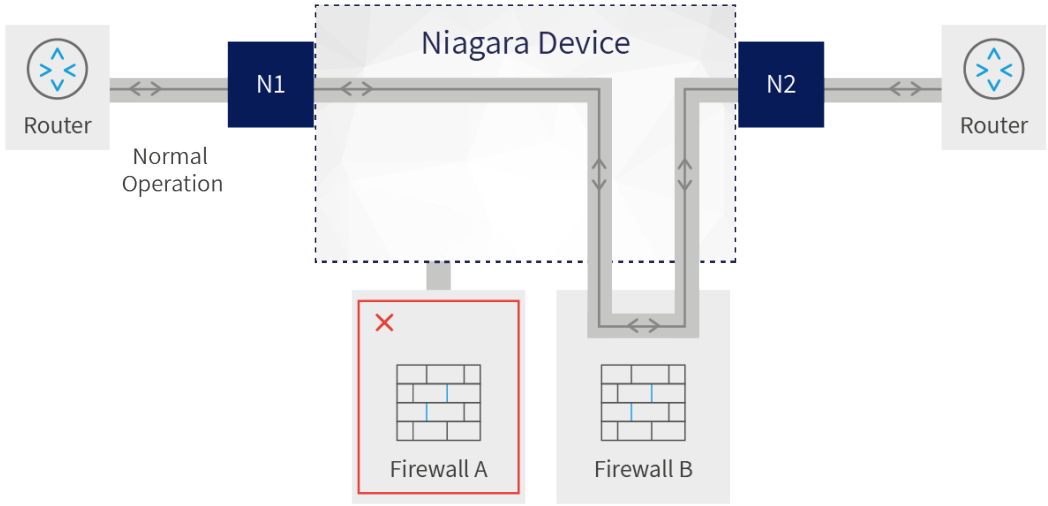


Bypass Mode

ByPass (2)

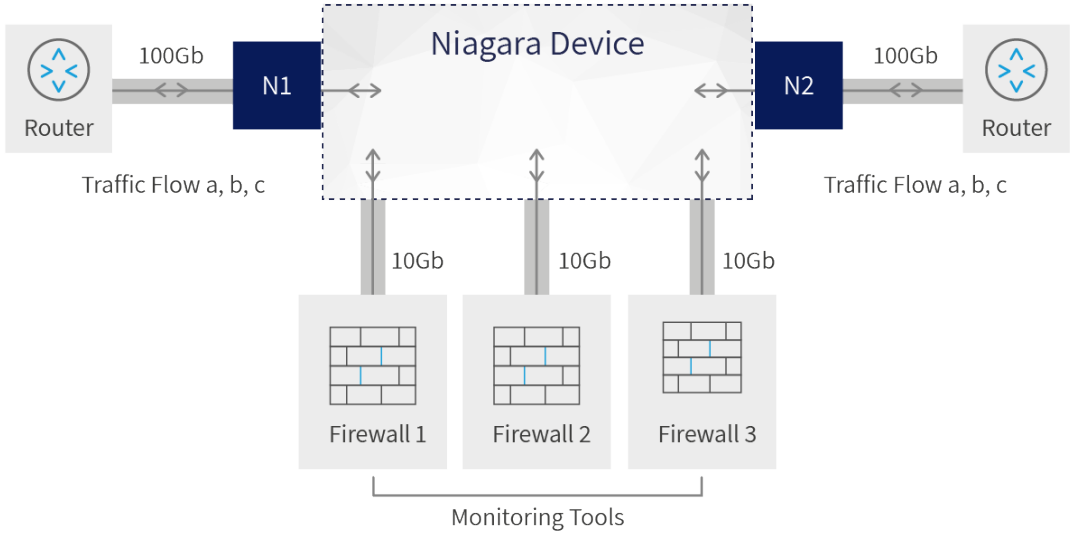
Резервирование средств ИБ



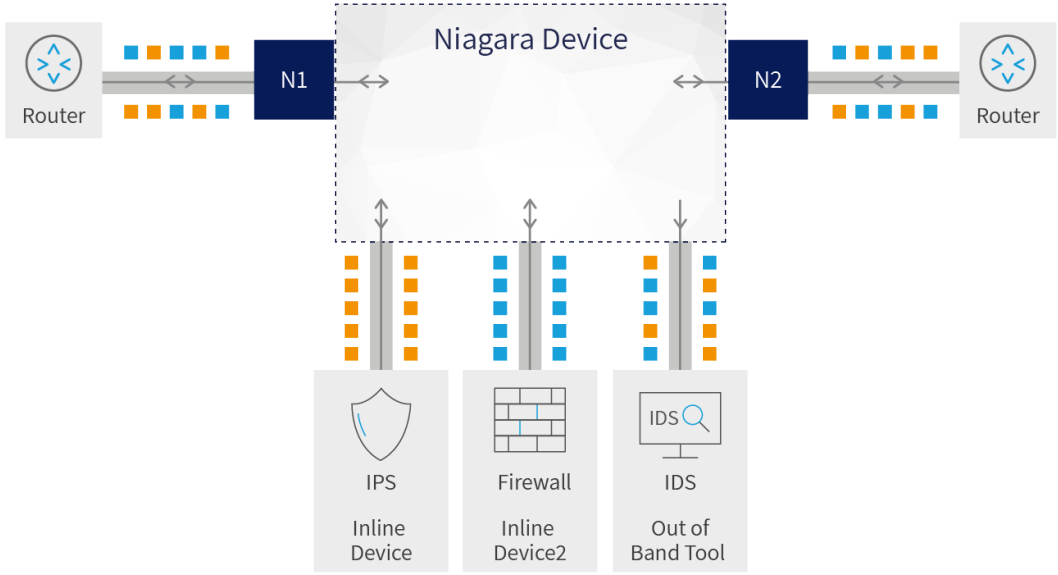


ByPass (3)

Масштабирование и интеллектуальное подключение



Балансировка трафика



Каждое устройство работает только с нужным трафиком

Портфолио

Линейка продуктов

Пакетные Брокеры

ByPass свичи

TAP Сетевые ответвители


2845


2847

N2 SERIES


2825


3299


2818

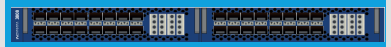
BYPASSP2


4432


4248-6XL


4272

FIXED BROKERS


3808

Brocker & Bypass


3225

PASSIVE TAPS

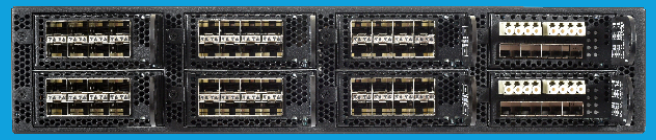
Niagara Visibility Controller

Универсальная система управления

N2 серия – Модульные устройства

- Пакетный брокер и ByPass в одном устройстве
- 4 слота для установки модулей с возможностью горячей замены
- Модули с интерфейсами 1/10/40/100G
- Неблокируемая архитектура
  - 160Gbps на слот
  - 1.2Tbs внутренняя шина
- Модуль модификации трафика - Packetron

2845



- Пакетный брокер и ByPass в одном устройстве
- 8 слотов для установки модулей с возможностью горячей замены
- Модули с интерфейсами 1/10/40/100G
- Неблокируемая архитектура
  - 160Gbps на слот
  - 2.4Tbs внутренняя шина
- Модуль модификации трафика - Packetron

2847

NIAGARA NETWORKS

Packetron #1 Модификация трафика

Инструменты, делающие копию трафика еще удобнее для получателя

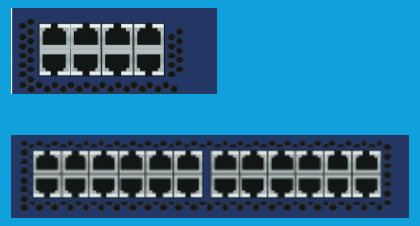
- **Packet Slicing** - обрезка поля данных для уменьшения объемов копии трафика (объем трафика уменьшается в 5 и более раз), а так же предотвращения передачи важной информации на нецелевые системы.
- **Deduplication –** удаление дублированных пакетов, для уменьшения нагрузки на получателя и снижения количества ложных срабатываний.
- **Data Masking –** маскирование пользовательских данных для предотвращения передачи важной информации на нецелевые системы, с сохранением объемов трафика.
- **Netflow\IPFIX Metadata –** генерация Netflow и IPFIX из копии трафика с возможностью обогащения метаданными. Позволяет снизить загруженность сетевого оборудования (как источника Netflow) и передавать данные для систем мониторинга и безопасности.
- **Tunnel Support –** отправка копии трафика удаленному получателю через L3 тоннель. Так же возможность получать копию трафика через L3 тоннель.

Packetron #2 Модификация трафика

Инструменты, делающие копию трафика еще удобнее для получателя

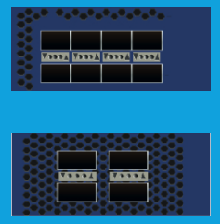
- **SSL\TLS Decryption –** дешифрация трафика SSL\TLS для передачи его в виде копии на пассивных получателей, а так же пропускание дешифрованного трафика через инструменты подключенные Inline. Для сценариев Inline выполняется атака MitM. Возможна дешифрация копии трафика в пассивном режиме, для определенных алгоритмов шифрования.
- **Application filtering –** фильрация копии трафика по DPI сигнатурам, позволяет выделить копию трафика отдельного приложения или нескольких приложений.
- **Header Stripping –** удаление заголовков сетевых тоннелей (VXLAN, GTP, GRE, MPLS …) для облегчения анализа копии трафика.
- **RegEx Filtering–** фильтрация копии трафика по регулярным выражения.
- **GTP Correlation –** корреляция GTP-C и GTP-U трафика абонентов мобильной сети. Выполнение балансировки абонентских сессий между получателями, фильтрация по IMSI, MSISDN, APN, QCI, IMEI … . Поддержка сетей 2/3/4/5G

N2 серия – доступные модули

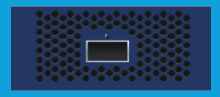


- 8x 1G/10GBaseT
- 24x 1G/10GBaseT

TAP / Bypass / NPB

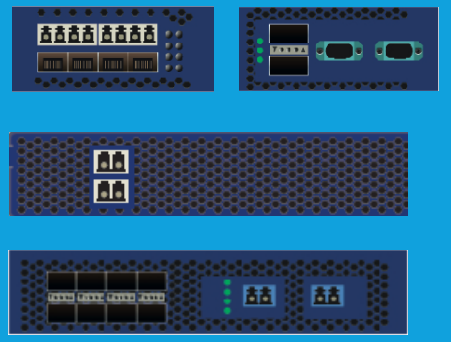


- 8x 1G / 10G
- 4x 40G



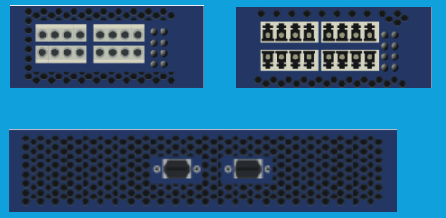
- 1x 100G NBP

Bypass / NPB



- 2x 1G / 10G
- 1x 40G
- 1x 40G / 100G
- 1x 100G + 8x10G

Bypass / TAP



- 4x 100FX
- 4x 1G / 10G
- 1 x 100G

TAP

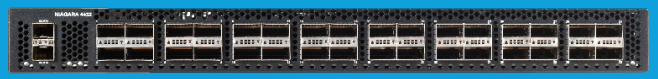
Фиксированные пакетные брокеры

- 72 порта SFP+
- Лицензируется на 36 или 72 порта

4272 – 72x 1G / 10G

- 48 портов SFP+ s
- 6 портов 40G QSFPt
- Схема лицензирования
  - 8 - 16 портов
  - 17 - 24 портов
  - 25 - 48 портов
  - 40G порты

4248-6XL – 48x 1G/10G + 6x 40G

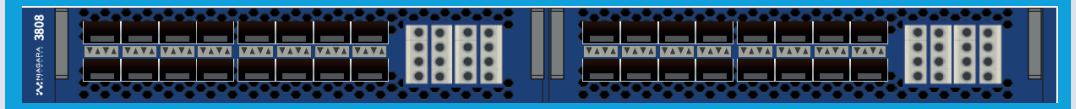


- 32 порта QSFP28 40G или 100G
- Возможность разветвлять 40G порты на 4 порта 10G
- В первой половине 2020 доступность разветвления на 25G порты
- Лицензируется на 16 или 32 порта

4432 – 32x 40G / 100G

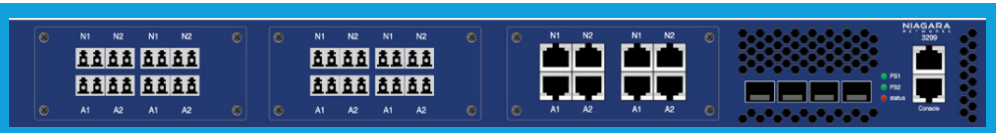
NIAGARA NETWORKS

Пакетные брокеры с ByPass



- 1/10/25G ByPass сегменты и порты брокера
- SR / LR
- До 8 сегментов ByPass на шасси
- До 32 портов SFP+ или SFP28
- Агрегация, копирование и фильтрация трафика по L2-L4 критериям
- Гибкая схема балансировки трафика
- Heartbeat для inline устройств
- Поддержка Rest API

3808: BYPASS и Пакетный брокер в одном шасси

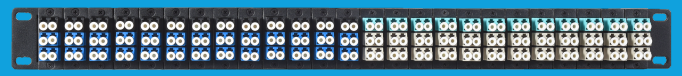


- До 6 bypass сегментов на шасси
- SX / LX / Copper
- До 12 медных TAP на шасси
- 4 порта SFP+ для передачи копии трафика
- Агрегация, копирование и фильтрация трафика по L2-L4 критериям
- Передача копии трафика через тоннель
- Безвентиляторное устройство
- Поддержка Rest API

3299: BYPASS\TAP с функцией агрегации и фильтрации

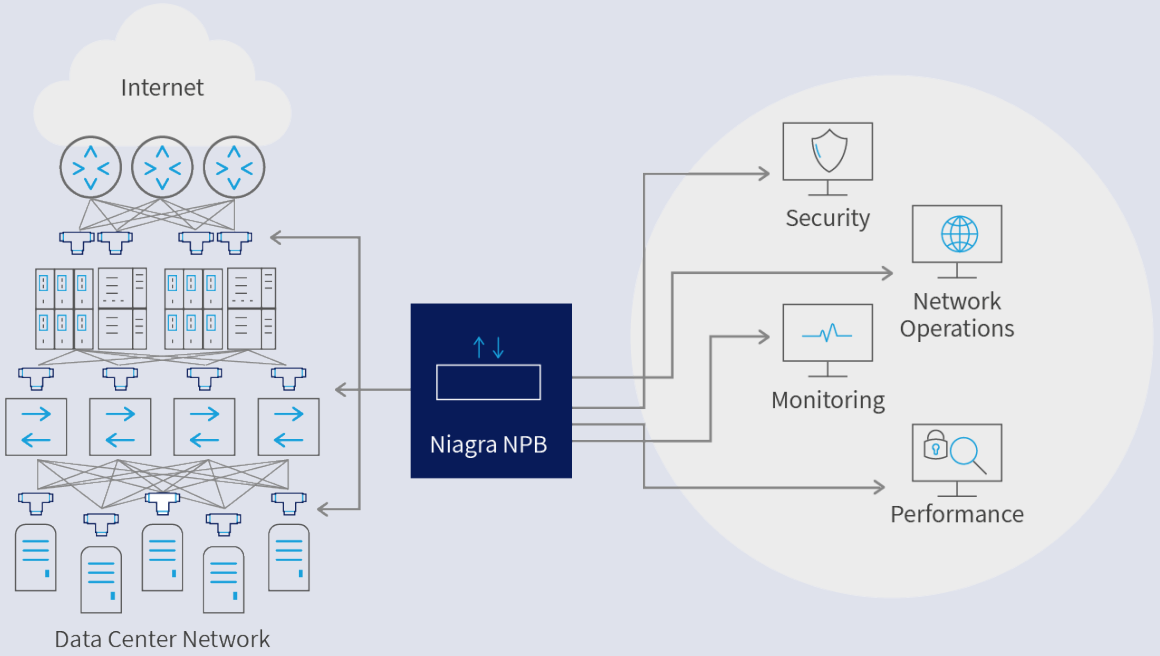
NIAGARA NETWORKS

Сетевые ответвители TAP



- Single mode / multimode
- SR / LR / LR4 / SR4 / SR10
- SR4 and SR10 use MPO connector
- Доступные степени деления
  - 90/10
  - 80/20
  - 70/30
  - 60/40
  - 50/50

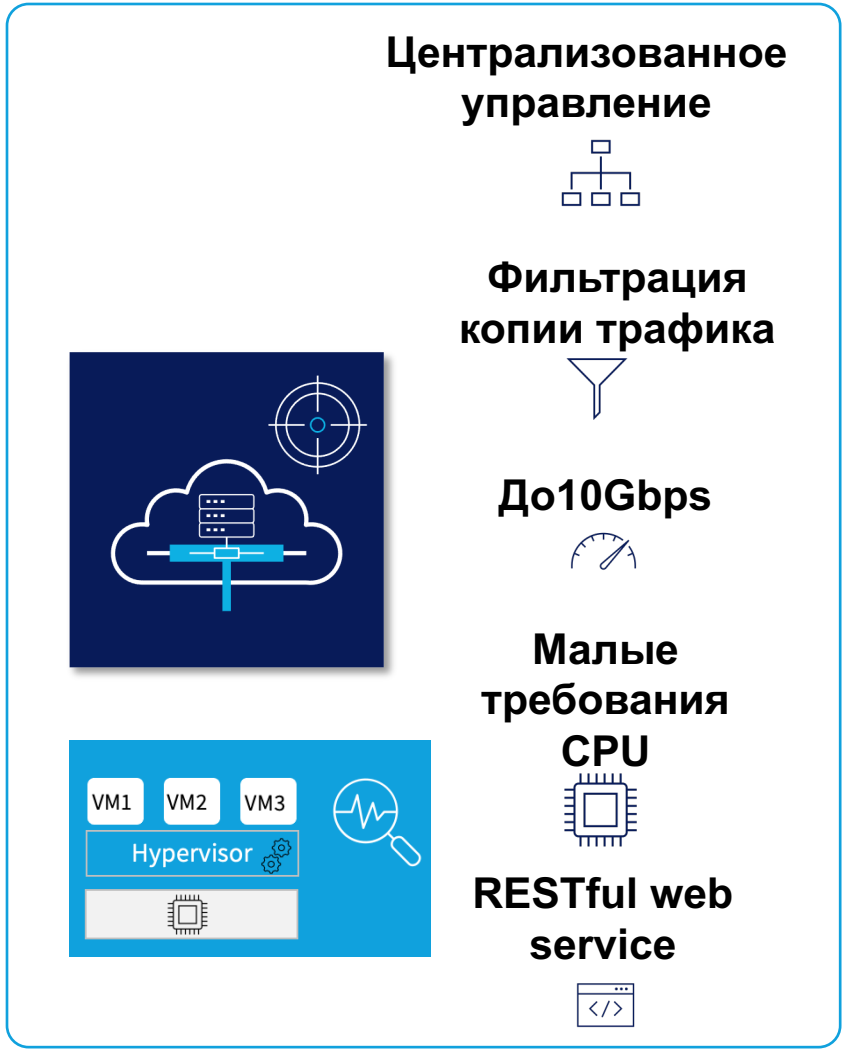
3225: до 25 TAP в шасси 1RU



NIAGARA NETWORKS

CloudRay TAP для виртуальной среды

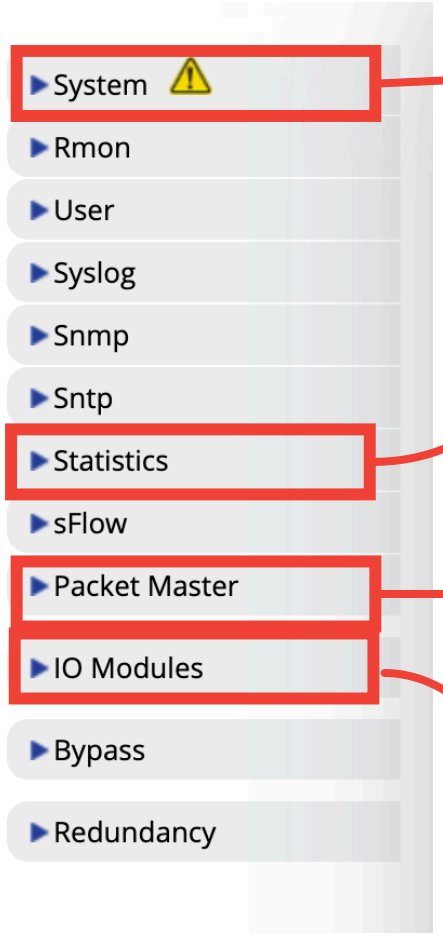
- Позволяет копировать трафик выбранных между виртуальными машинами, который не покидает пределов гипервизора
- Управление и оркестрация через CloudRay V-TAP Controller
- Отправка скопированного трафика через тонели (GRE, VLAN and VxLAN)
- Фильтрация копии трафика по критериям: (MAC, ARP, MPLS, IPv4/v6, TCP/UDP, ICMP, SCTP)
- Поддержка гипервизоров:
  - OpenStack
  - ESXi VMware
  - EC2 instances in AWS
- Northbound API
- Взаимодействие с другими решениями Ниагара Нетвокрс



Настройка оборудования

Главное меню

С чего начать?



Системные настройки

- Основные настройки устройства
- Обновление ПО
- Сохранение и экспорт конфигурации
- …

Статистика!

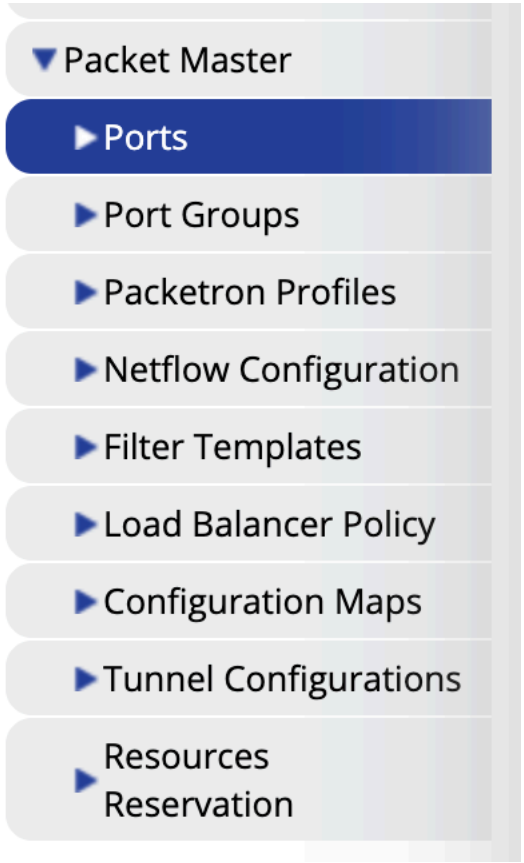
Тут проверяем как все работает

Основной раздел

- Тут настраиваем режимы работы портов.
- Создаем портовые группы
- Настраиваем политики копирования и фильтрации трафика
- Настраиваем хэш балансировки
- Управляем всеми настройками обработки трафика

Внешиний вид устройства

Настройка портов



Колонка SFP Info покажет Информацию о трансивере

Vendor : FINISAR CORP.
VPN : FTLX8574D3BCV
Capability : 1G/10G
Temperature : 29.79C
TxPower : 0.55mW | -2.61dBm
RxPower : 0.00mW | -26.99dBm
Voltage : 3.34V
Current : 8.74mA

Колонка Mode меняет режим работы порта

Normal: порт работает в обычном режиме

Force: порт всегда воспринимается как активный, даже если нет сигнала в Rx части.

Listen: порт всегда воспринимается как активный, даже если нет сигнала в Rx части. В этом режиме порт может быть только входящим

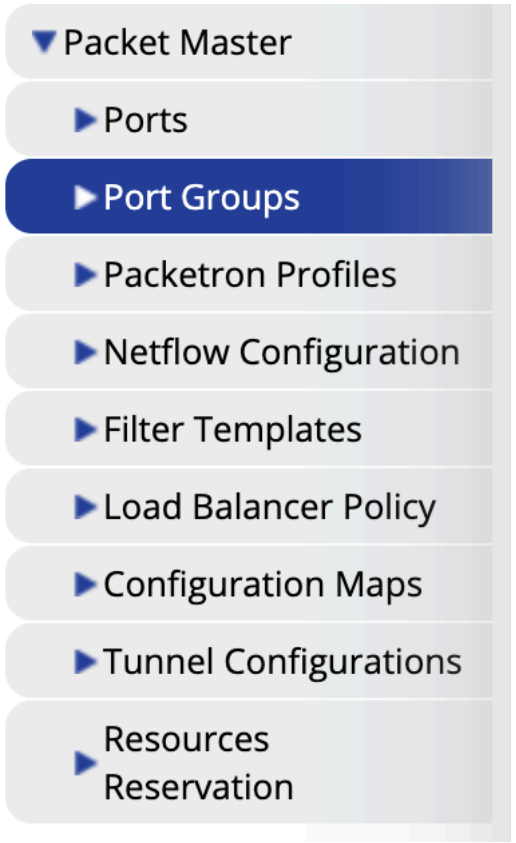
Другие важные колонки

Status – вкл\выкл порт

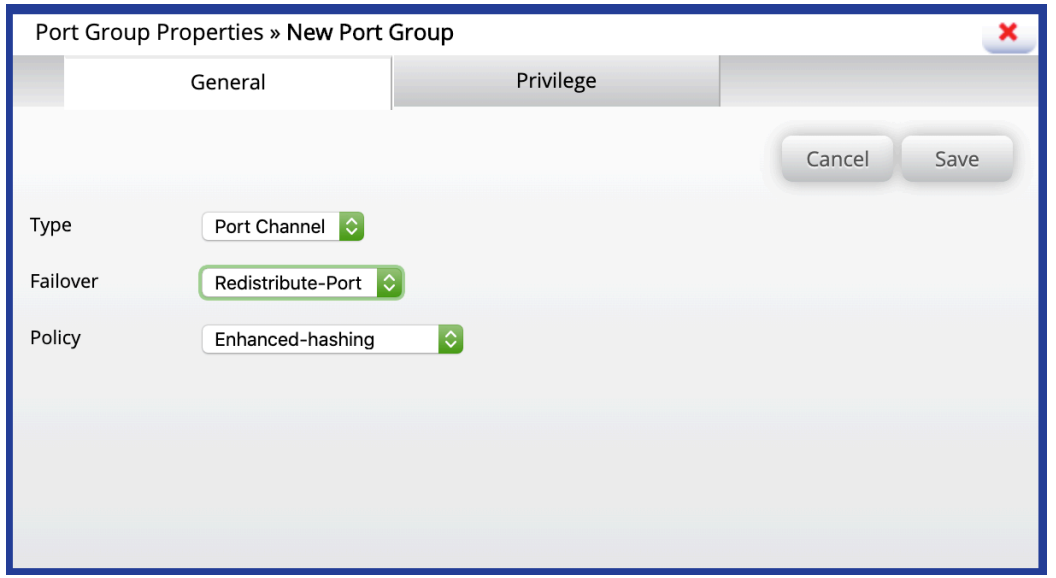
Link Status – отображает текущую работоспособность порта

SPEED – скорость порта

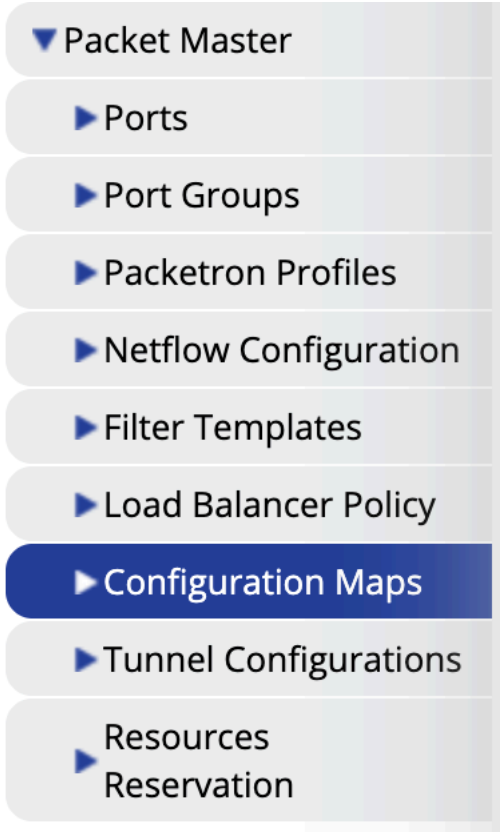
Настройка групп портов



- Здесь создают и администрируют портовые группы, для per-session балансировки трафика между портами-членами портовой группы
- Зажмите клавишу CTRL и поочередно кликайте мышкой на каждый порт, который вы хотите добавить в группу. Так будет удобнее перетащить порты в рабочее поле
- Чтобы изменить настройки балансировки, при создании порт-группы нажмите Advanced. Рекомендую следующие настройки

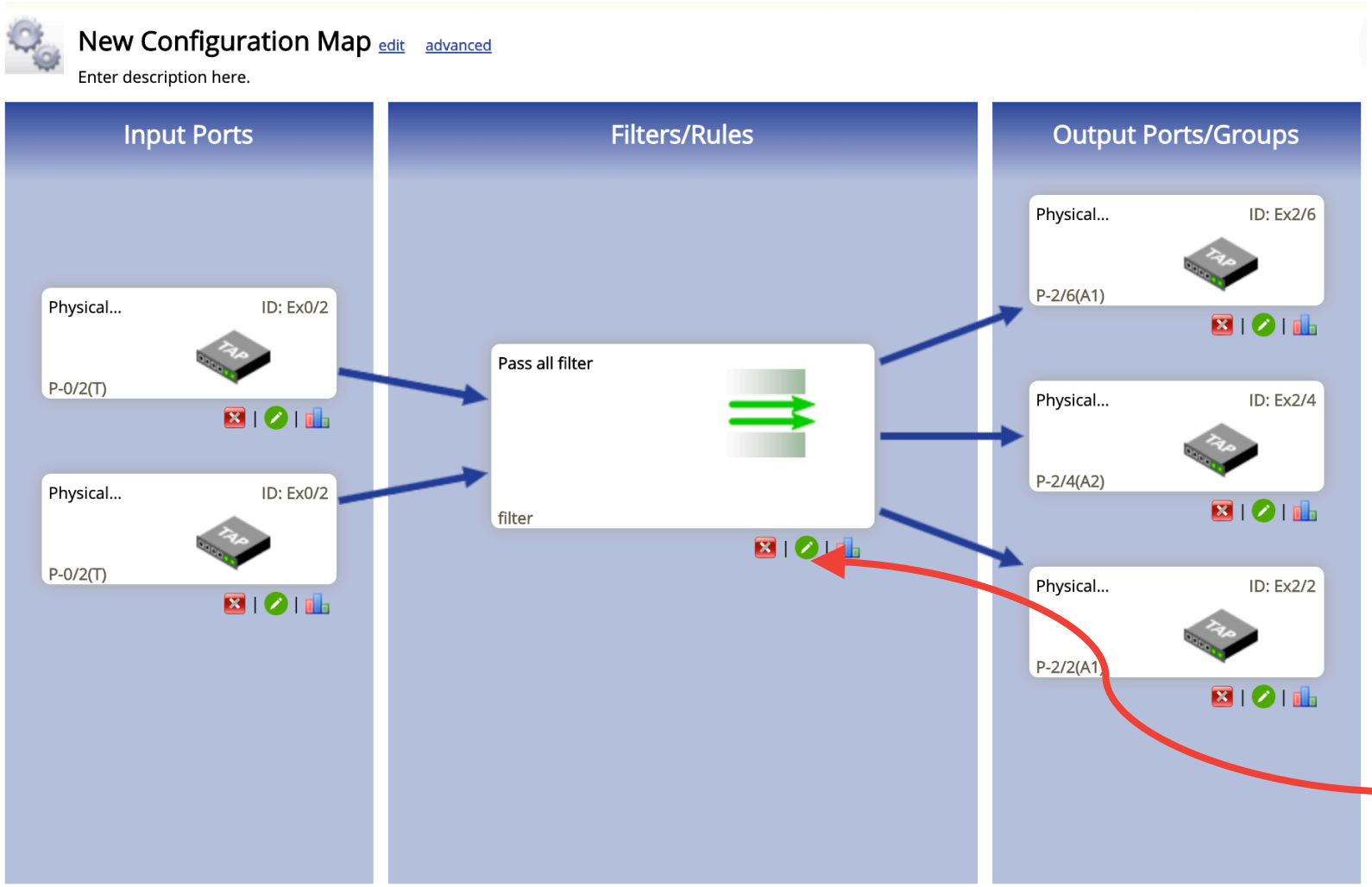


C-MAP – копирование и фильтрация трафика



- Каждая C-MAP – описывает с каких портов, на какие порты и согласно каким критериям нужно скопировать трафик.
- Можно создавать несколько C-MAP. Используя разные порты источники, и получатели. Порты между C-MAP могут пересекаться.
- Приоритет – важный параметр C-MAP. Трафик анализируется до первого срабатывания. Если пакет попадает под несколько C-MAP, то он будет отправлен той C-MAP, которой приоритет выше. Рекомендую C-MAP с наиболее специфичными критериями фильтрации ставить приоритет выше.

C-MAP – пример



Конфигурирование:

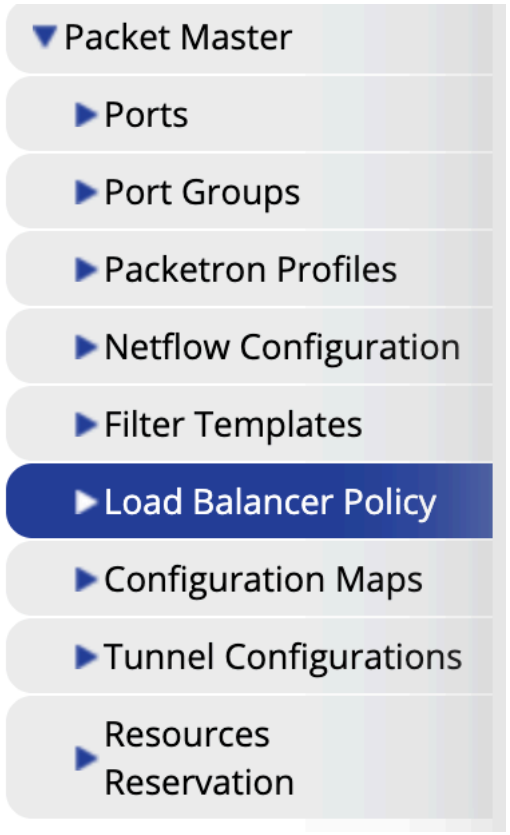
Input Ports: перетащите порты и списка вверху

Output Ports/Groups: перетащите порты и списка вверху, а так же группы из соответствующей вкладке вверху

Filters/Rules: перетащите прямоугольник default из вкладки Filter Templates

На зеленый кружок, чтобы перейти в меню конфигурирования политик фильтрации трафика

Настройка хеш балансировки трафика



Отметьте те параметры по которым необходимо выполнить балансировку. Рекомендую следующие параметры

◉	XOR IP Based	☑ IP Source ☑ IP Destination	☑ Ipv6 Destination ☑ Ipv6 Source ☑ Source L4 Port ☑ Destination L4 Port ☑ GTP Tunnel ID ☑ IPv4 Protocol ☐ IPv6 Next Header
○	XOR MAC based	☐ MAC Source ☐ MAC Destination	

Apply

System & CLI

В разделе **Display Configuration** можно увидеть конфигурацию устройства в текстовом виде

- Подключитесь к устройству через SSH или CONSOLE, чтобы выполнить конфигурацию устройства через командную строку.
- Cisco Like Interface:
  - conf t
  - show run
  - write startup-config
  - ……
- Удобно для быстрого конфигурирования устройства «из коробки», если заранее подготовить конфигурацию, можно применять по принципу copy-paste

Благодарю за внимание

Александр Грачев
agrachev@netwell.ru