Network Visibility:
Цели, Возможности, Проблемы

Павел Нестеров
Технический Директор
nesterov@web-control.ru

Идея Network Visibility

Что делать?

1. Собрать статистику сетевого взаимодействия во всех доступных точках (активное сетевое оборудование поддерживающее экспорт NetFlow/IPFIX/sFlow)

2. В точках мониторинга, не поддерживающих экспорт статистики, а так же в случае необходимости более глубокого анализа установить специализированные зонды

3. Обеспечить оперативный доступ к статистике

4. Применить алгоритмы анализа с целью выявления инцидентов

Результат

1. Картина сетевого взаимодействия не привязана к топологии сети

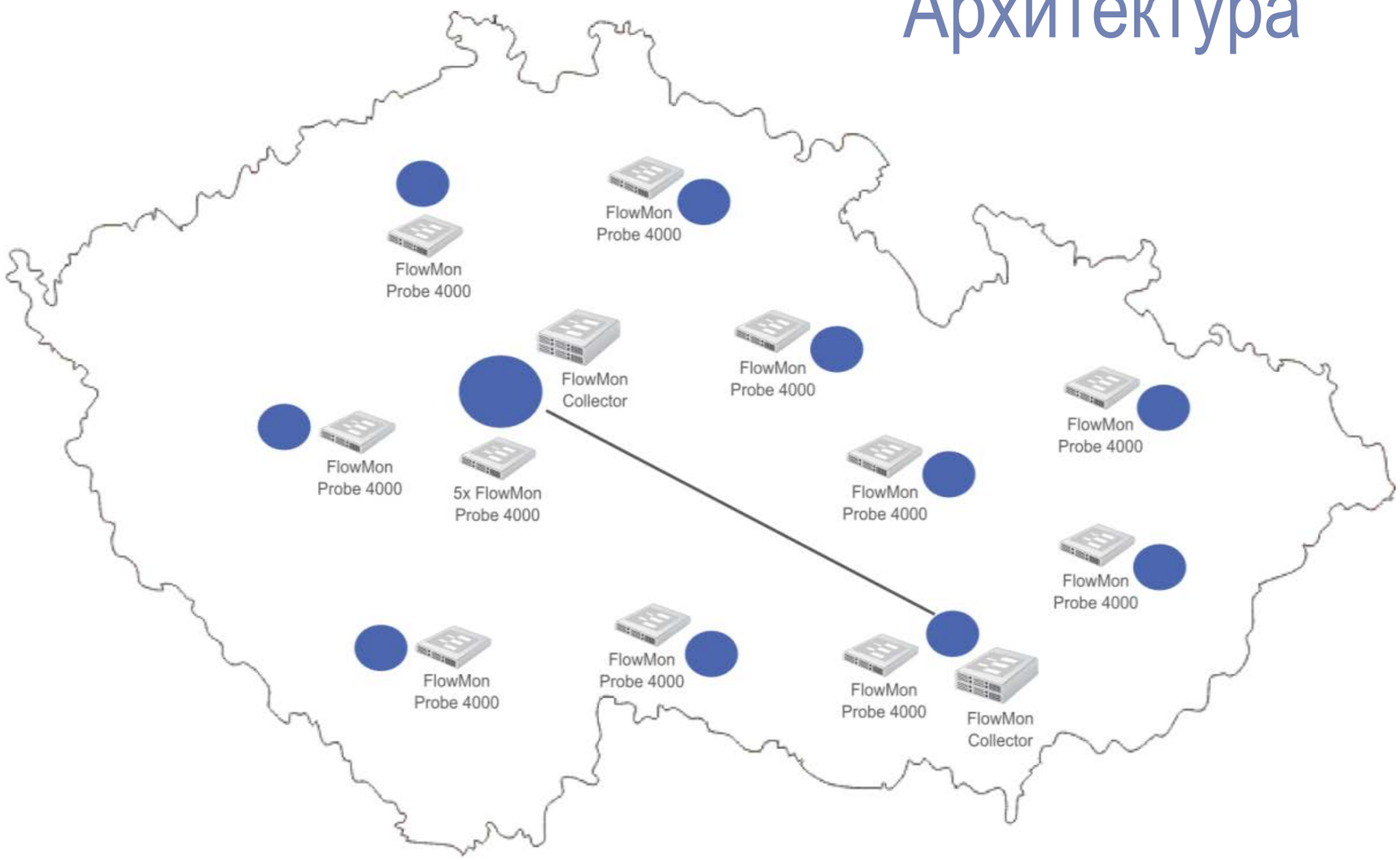
2. Сетевое взаимодействие (в том числе удаленных площадок) анализируется централизованно

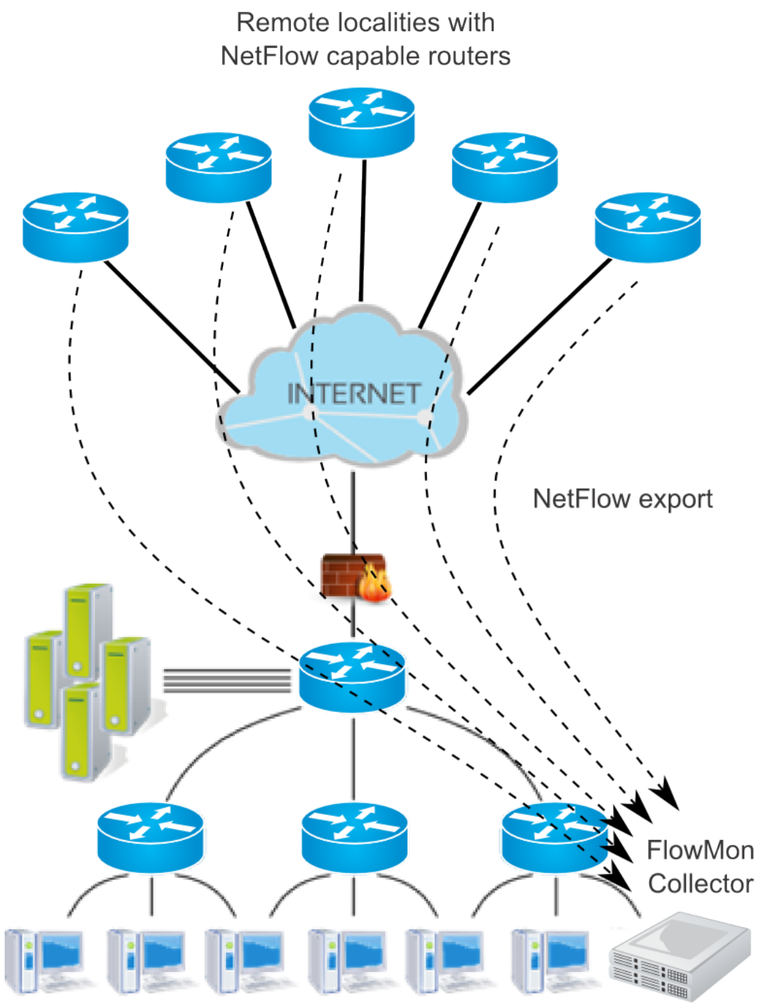
3. Возможность оперативной генерации отчетов с целью расследования инцидентов, планирования развития ИТ-инфраструктуры

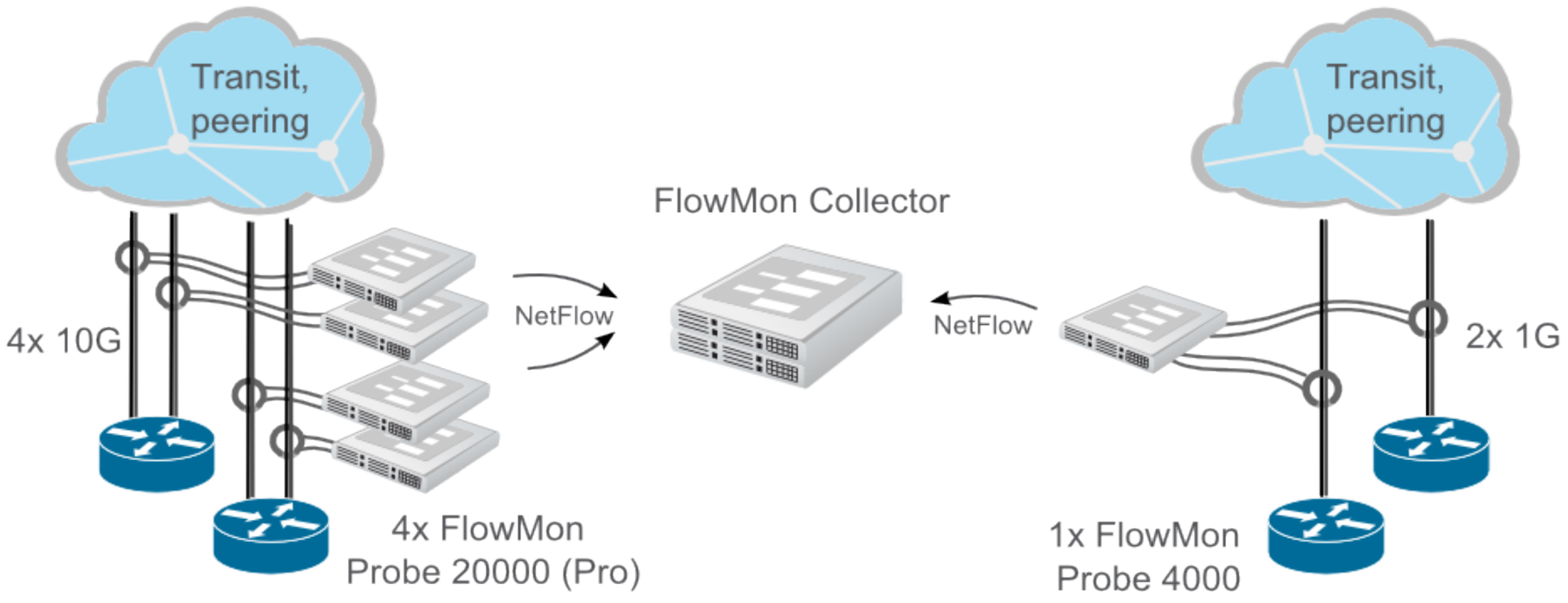
4. Генерация потока событий о возникновении инцидентов (как ИБ так и ИТ)

5. Возможность автоматического, автоматизированного или ручного реагирования на инциденты

Архитектура







webcontrol

Цели и задачи ИТ, ИБ:

1. **Обеспечение непрерывности бизнеса**

- Противодействие атакам
- Сокращение времени восстановления после сбоев
- Планирование развития ИТ-инфраструктуры

2. **Снижение издержек**

- Предотвращение утечек информации
- Оптимизация использования ИТ-ресурсов
- Сокращение времени расследования инцидентов

Решение FlowMon

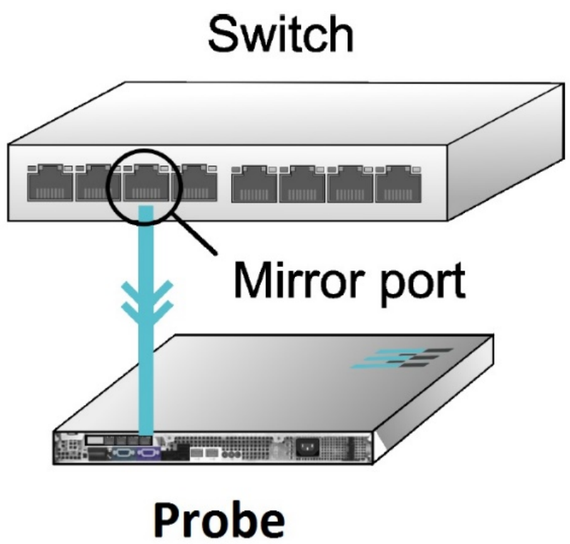
FlowMon: **Комплексное решение**

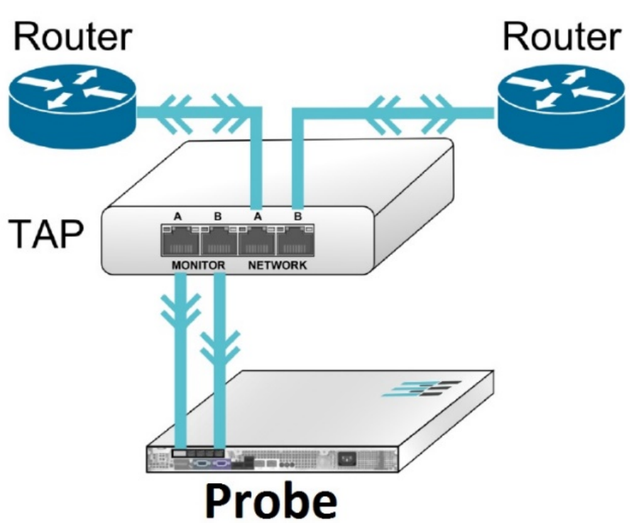
Flow Monitoring	Network Security Monitoring	On Demand Packet Capture	Network/ Application Performance	DDoS Protection
FlowMon Monitoring Center	FlowMon ADS	FlowMon Traffic Recorder	FlowMon APM	FlowMon DDoS Defender

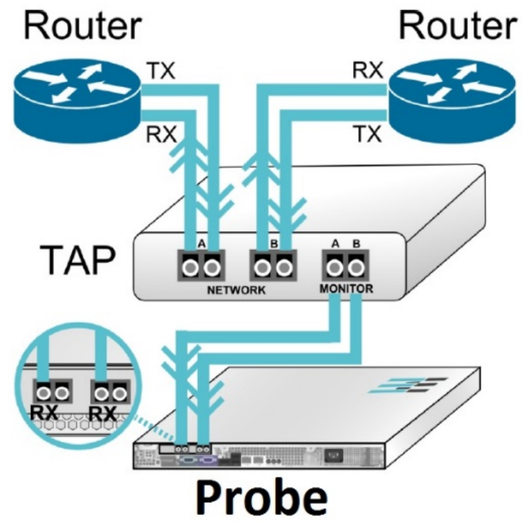
Не все так просто

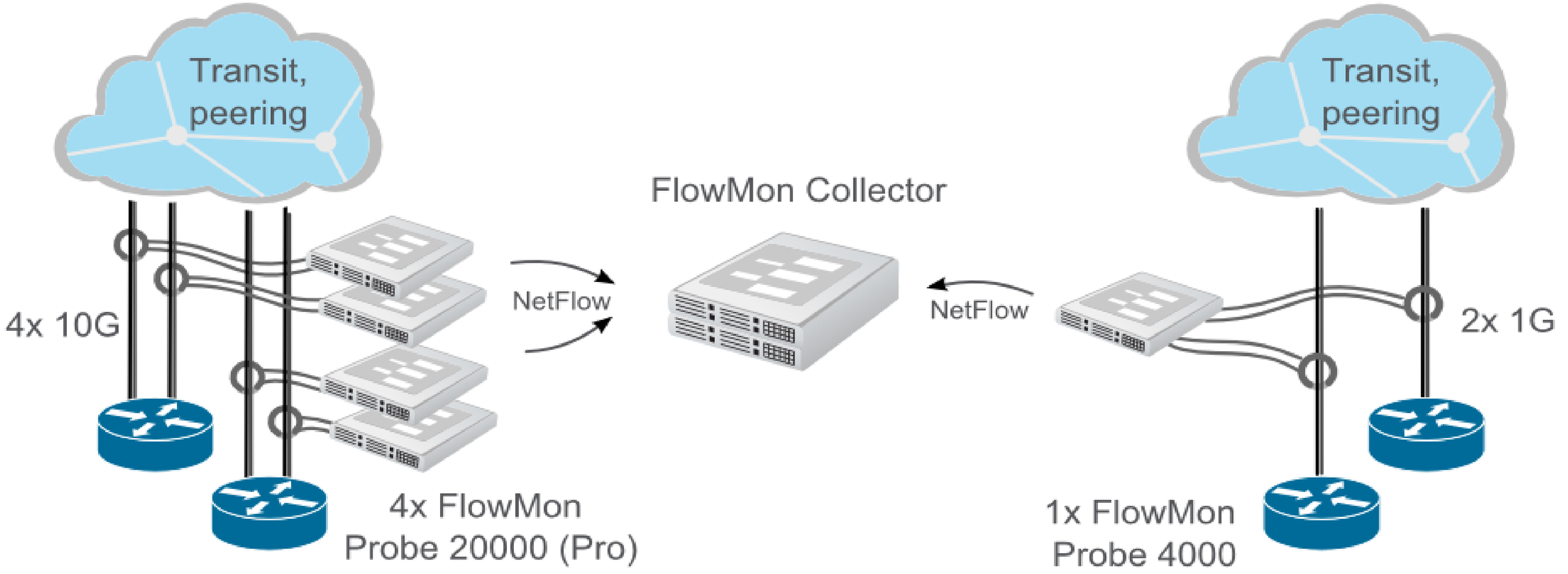
1. Обеспечить покрытие инфраструктуры точками мониторинга
2. Виртуальная инфраструктура? Облака?
3. Недостаточно данных для детального расследования
4. Зеркалирование для зондов

Зеркалирование

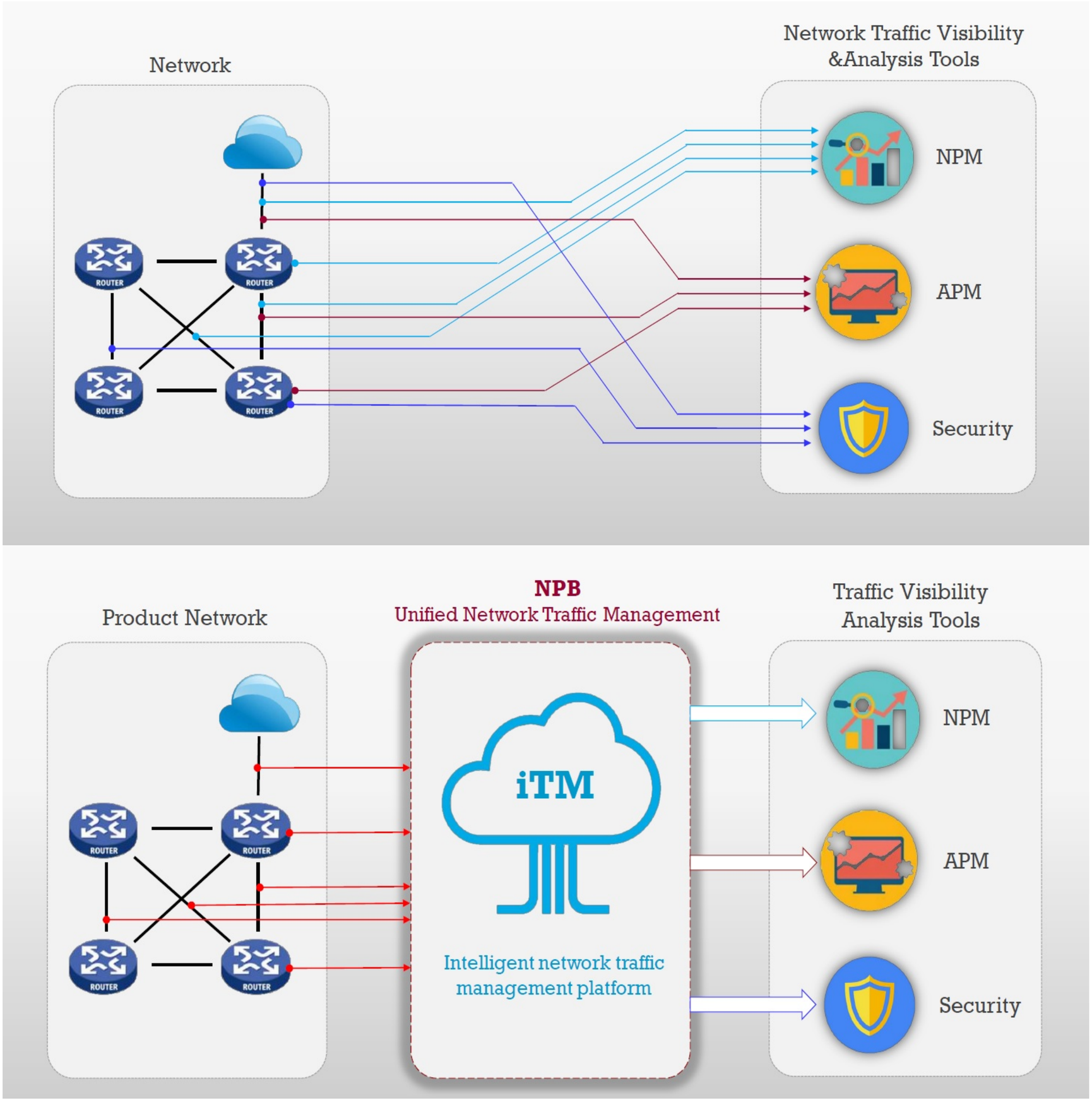




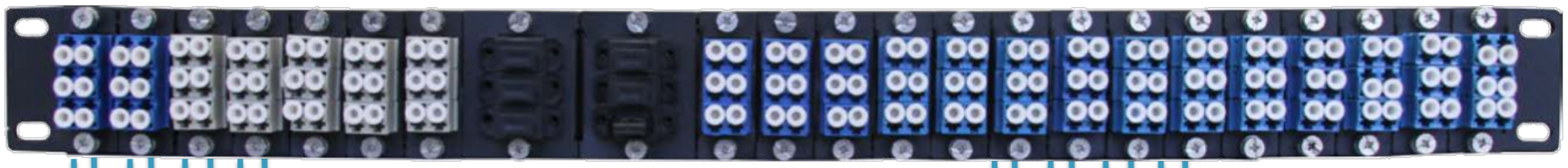




Зеркалирование



Зеркалирование: TAP + NPB



TAP layer

4 x 10G links input
(8 ports total, 2 Rx and 2 Tx)

NIAGARA NPB
VISIBILITY LAYER

Database Monitoring

NetFlow Analyser

Intrusion Detection System

File security

Email security

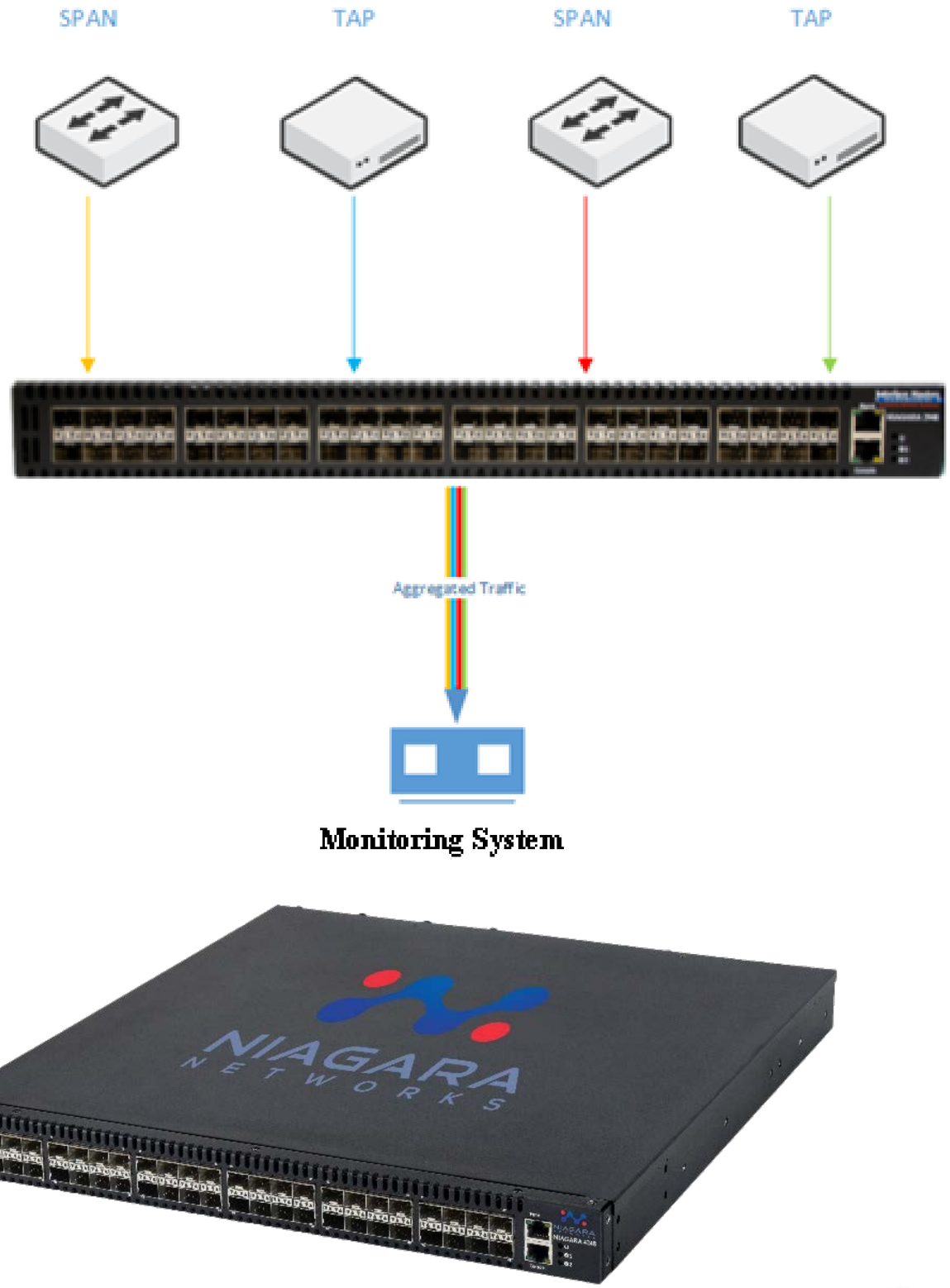
Network Visibility – N.P.B.

Niagara Packet Brocker

Network Packet Manipulation including:

- Aggregation
- Mirroring
- Filtering
- Tunnel handling
- Supports 1G, 10G, 40Gb and 100G

- Up to 72 ports of 10G/1G in 1U
- Up to 32 ports of 40G in 1U
- Up to 32 ports of 100G in 1U
- Leading Price performance



webcontrol

www.web-control.ru

Москва, ул. Электрозаводская, 24
info@web-control.ru