

Tap into your NETWORK®



ТОВ «ІНКОТЕЛ СІСТЕМ»

вул. Архітектора Городецького, буд.11-Б, м. Київ,
Україна, 01001 т. +38044 3613708 т/ф +38044 500 1830
E-mail: info@inkotel.com.ua Web: www.inkotel.com.ua

Заказчики

- 82% списка Fortune 100
- 5 новых заказчиков еженедельно

Примечательные факты

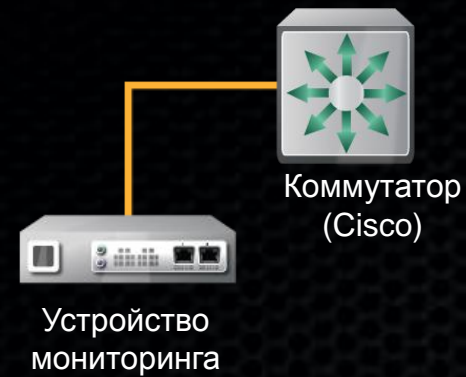
- Основана в 1996 г. , США
- 60 кварталов роста и прибыльности
- Частная компания без венчурного финансирования

Технологические достижения

- Инновации Net Optics (функция Zero Delay, регенерирующие ответвители, обходные коммутаторы и агрегаторы каналов, динамическая балансировка, Virtual Tap)

СПОСОБ

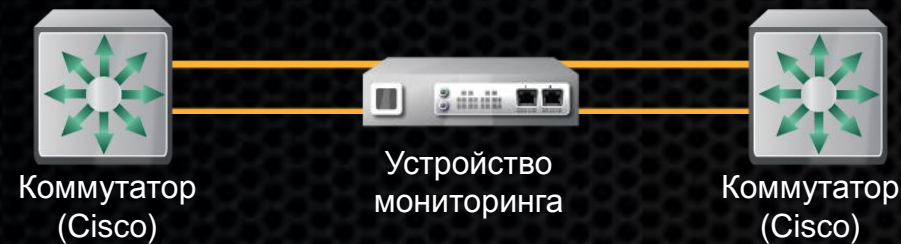
Через Span-порт



НЕДОСТАТКИ

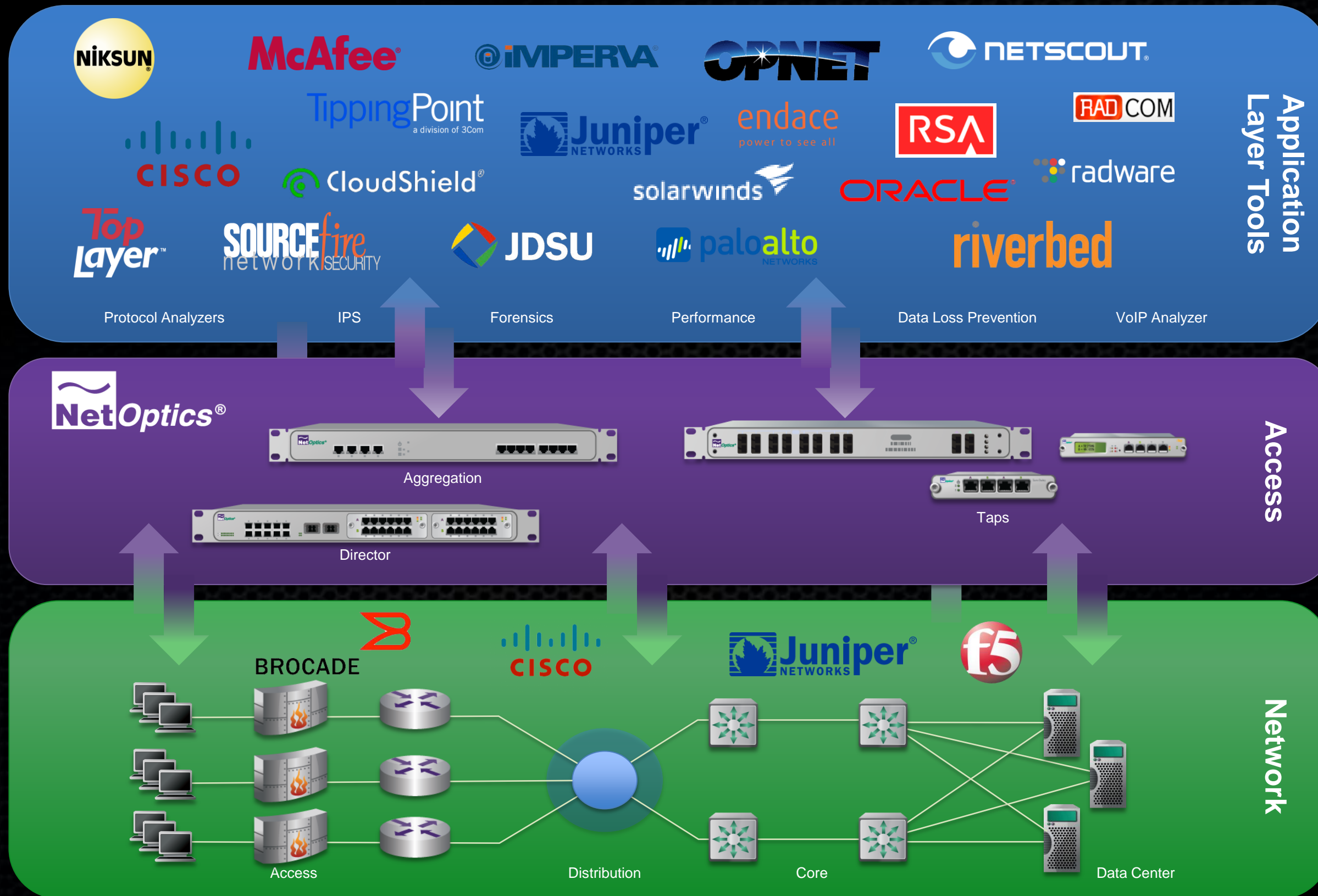
- Возможна потеря пакетов, когда коммутатор перегружен.
- Не передаются пакеты с ошибками на уровнях 1 и 2.
- Необходимо затрачивать время и деньги на переконфигурирование коммутаторов.

В разрыв канала
(in-line)



- Возможное место отказа.
- Дорогое решение типа одно устройство мониторинга на один канал.
- При перемещении устройства мониторинга неизбежен разрыв канала.

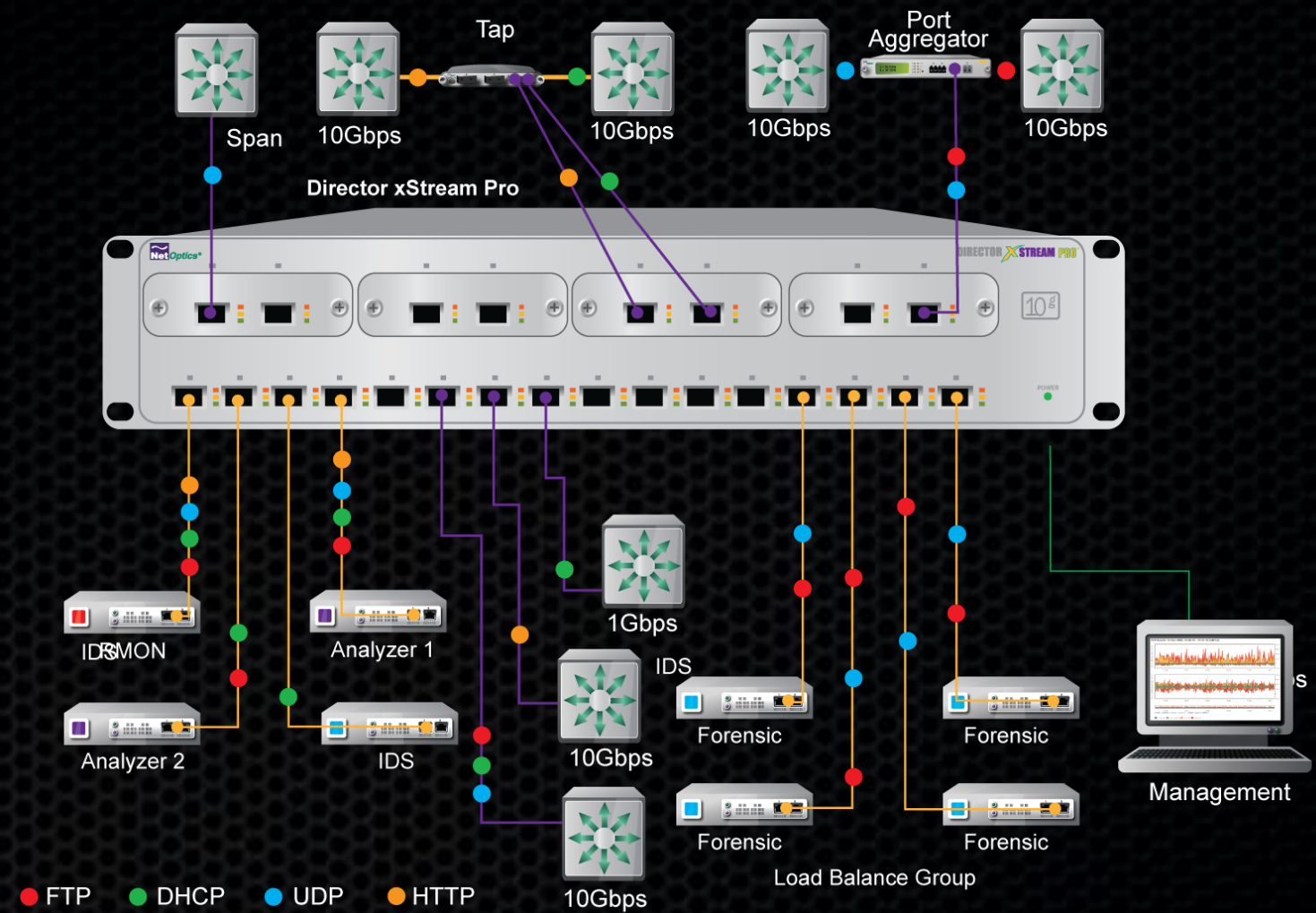
Архитектура интеллектуальной системы доступа и мониторинга



Решение – средства доступа для сетевого мониторинга



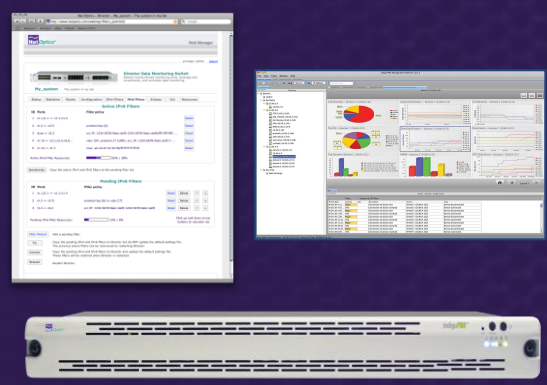
- 100%-ный контроль трафика вашей сети.
- Пассивная отказоустойчивая работа; нет единственной точки отказа.
- Развертывается как инфраструктура.
- Рекомендуются всеми известными производителями средств мониторинга.



Администрирование

Управление трафиком

Доступ



- ПО Indigo
- CLI
 - Web UI
- Платформа Indigo Pro
- Collector Pro
 - Manager Pro

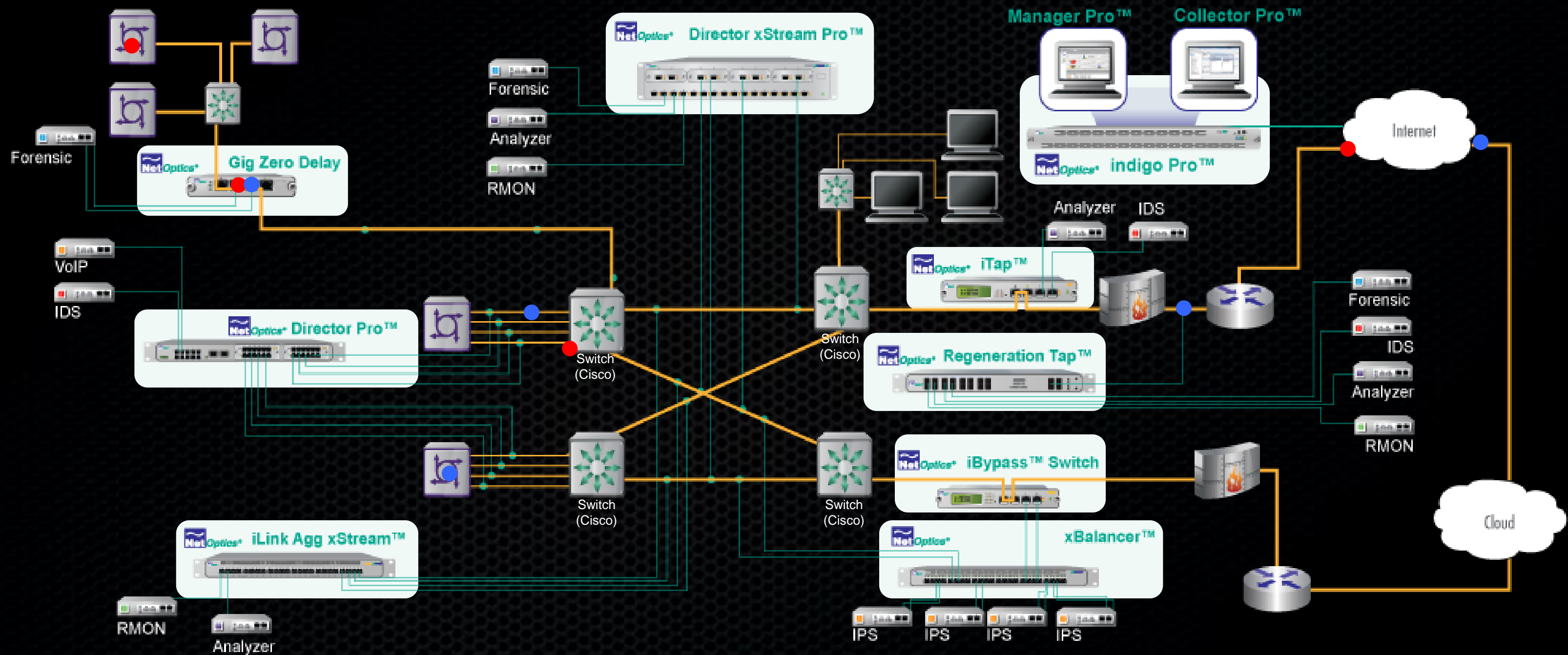


- Director xStream Pro
- Director xStream
- Director Pro & Director
- xBalancer
- iLinkAggxStream
- iLinkAgg



- iBypass HD
- Коммутаторы iBypass и Bypass
- Gig Zero Delay Tap
- Сетевые ответвители

Средства мониторинга и сетевые устройства



- Director xStream Pro
- xBalancer
- Indigo Pro
- Phantom Virtual Tap
- appTap



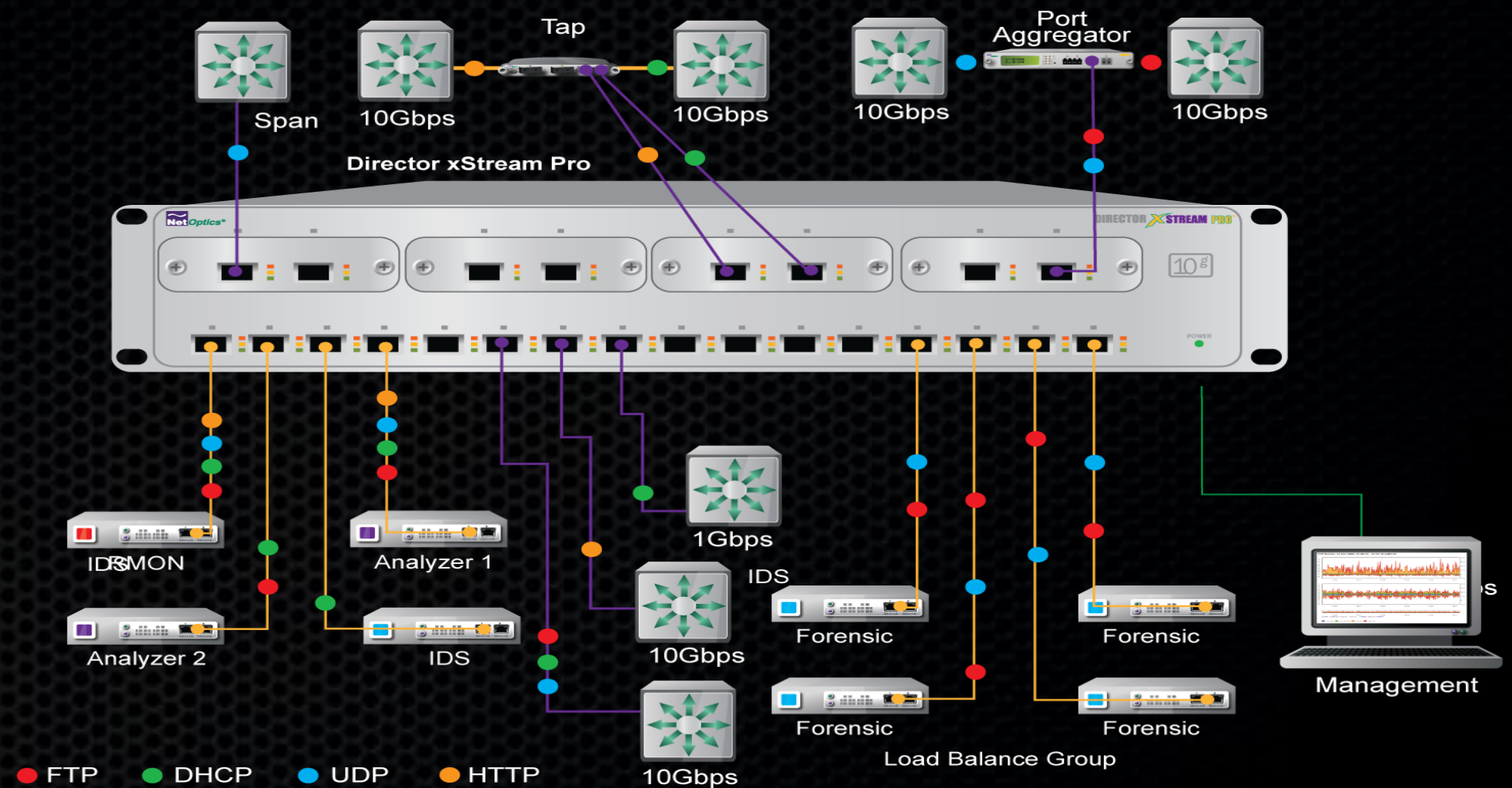
Характеристика

- Глубокий анализ пакетов (DPI).
- Динамическое выравнивание нагрузки с сохранением целостности потоков.
- Снабжение пакетов временными метками с использованием средств RTP, NTP или GPS.
- Обнаружение микровсплесков трафика.
- Измерение задержки с наносекундной точностью.
- Захват последовательностей пакетов (snapshots).
- Ежесекундное обновление информации о трафике с помощью ProPush.
- Агрегирование, регенерация, коммутация и фильтрация L2–L4.
- 24 порта SFP+ 10G/1G в формфакторе 2U.



Варианты использования

- Включение в разрыв канала (in-line) с использованием двух портов ProPort
- Получение данных напрямую от ответителя для пассивного мониторинга.
- Подключение Span-портов коммутаторов к портам ProPort для дополнительной фильтрации.
- Подключение Span-портов коммутаторов к обычным портам для агрегации, регенерации или коммутации трафика.



Возможности

- Отображение статистики RMON с ежесекундным обновлением этой информации для быстрого мониторинга трафика и обнаружения его микровсплесков.
- Можно приостановить мониторинг трафика, посмотреть текущую информацию или переместиться на ± 5 мин.
- Доступные диаграммы: объем пропущенного/отброшенного трафика, IPv4/IPv6, распределение трафика по типу протокола и размеру кадров, TCP-события.



Краткая характеристика функциональности

Функция	Описание	Полезность для пользователя
Динамическое выравнивание нагрузки	Есть режимы выравнивания нагрузки на базе потоков для приложений, где необходимо сохранять в целостности диалоги, а для трафика не IP подойдет циклическое (round-robin) распределение пакетов	Разделяя трафик на несколько «рукавов» с сохранением целостности потоков пакетов, функция динамического выравнивания нагрузки позволяет анализировать этот трафик с помощью соответствующего числа (от 2 до 16) одновременно работающих устройств мониторинга
Глубокий анализ пакетов	Анализ заголовков L5–L7 и полезной нагрузки пакета на совпадение с заданными образцами. Можно использовать 16 наборов образцов, каждый из которых представляет собой одну или две строки длиной до 64 символов	Позволяет находить вложенные метки MPLS, номера телефонов и кредитных карт, а также ключевые слова или фразы типа «Конфиденциально» и «Не распространять»
Соединение портов	Порты 1–8 являются портами ProPort, которые поддерживают фильтрацию, DPI и динамическое выравнивание нагрузки. Порты 9–24 являются обычными портами, которые обеспечивают коммутацию, агрегацию и регенерацию, а также они могут быть выходами для фильтров, DPI и выравнивания нагрузки	Трафик сетевых каналов и Span-портов может быть агрегирован, регенерирован и направлен в выходные порты почти в любой комбинации
Фильтрация на входе/выходе	Будучи связанными с портами, фильтры являются входными на сетевых портах и выходными на портах мониторинга	Трафик с выхода входного фильтра может быть направлен в любой из 24-х портов, а на вход выходного фильтра трафик может поступать с любого из 24-х портов
Захват пакетов	В любой момент времени вы можете захватить 8-секундную последовательность пакетов на выходе любого фильтра L2–L4 или DPI	Это позволяет легко проверять фильтры и обнаруживать редкие события. Пакеты хранятся в файлах pcap, которые могут быть легко экспортированы в анализатор протоколов типа Wireshark
100%-ная видимость трафика	Коммутатор пропускает все пакеты длиной от 64 до 9600 байт, если у них корректные контрольные суммы CRC	Посылает на устройство мониторинга весь трафик (без потерь пакетов) даже при 100%-ной загрузке порта

Сравнение функциональности

Продукт	Фильтрация	Выравнивание нагрузки	Временные метки	Захват пакетов	Микро-всплески	Соединение портов	Скорость	Число портов
Director xStream Pro	L2/4, DPI	Статическое, динамич.	NTP, RTP, GPS	8-с Snapshot	Есть	Агрегация, реген., коммутация	10G 1G	24
Director xStream	L2/4	Статическое	Нет	Нет	Нет	Агрегация, реген., коммутация	10G 1G	24
Director Pro	L2/4, DPI	Статическое, динамич.	Нет	Нет	Нет	Агрегация, реген., коммутация	10G 1G	3 24
Director	L2/4	Статическое	Нет	Нет	Нет	Агрегация, реген., коммутация	10G 1G	4 24
iLink Agg xStream	Нет	Нет	Нет	Нет	Нет	Агрегация, реген., коммутация	10G 1G	24
iLink Agg	Нет	Нет	Нет	Нет	Нет	Агрегация, реген., коммутация	1G	24

BALANCER™

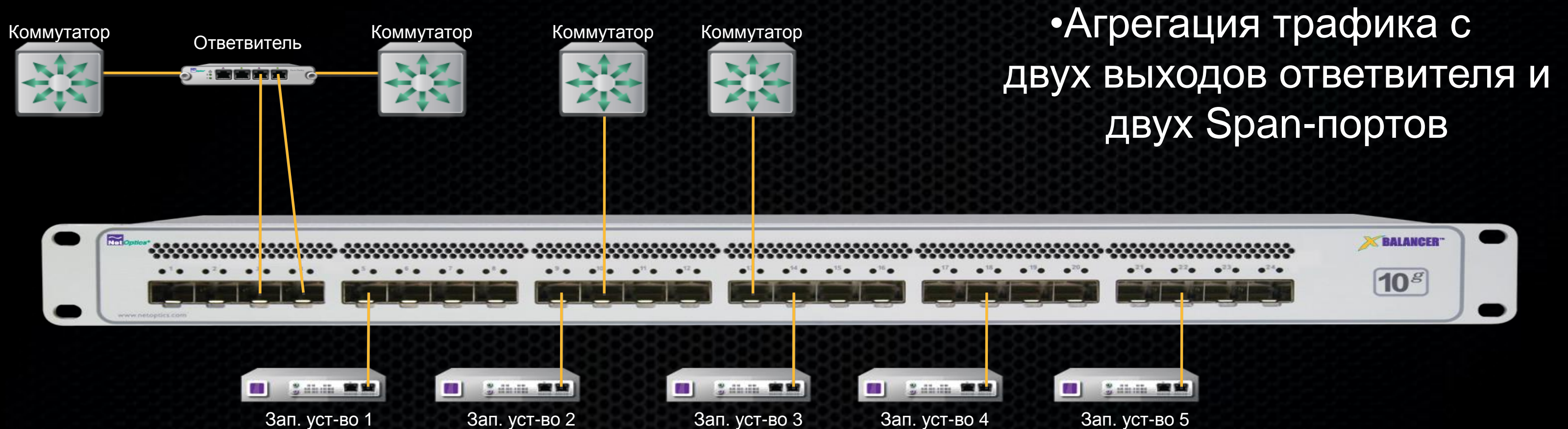


- С увеличением скорости передачи данных по сетевым каналам до 10 Гбит/с мониторинг функционирования и безопасности сетей стал более важен, чем когда-либо раньше.
 - Но средства мониторинга не справляются со столь интенсивным трафиком!
- Решение проблемы – распределение трафика по нескольким одновременно работающим средствам мониторинга.



- Первое и единственное устройство для подключения средств мониторинга к сети, специально предназначенное для выравнивания нагрузки на эти средства.
- Выравнивание нагрузки на базе потоков (иногда говорят «на базе сеансов»). Потоки могут определяться по 5 полям – IP-адреса отправителя и получателя, номера портов отправителя и получателя и тип протокола – или по любой комбинации этих полей.
- До 4 независимых групп портов с выравниванием нагрузки.
- До 16 выходных портов в группе.
- Варианты организации мониторинга out-of-band и inline.
- Разделение ресурсов средств мониторинга – равномерное распределение трафика нескольких независимых каналов по набору средств мониторинга.
- Скорости 10G и 1G; автоматическое преобразование скоростей.
- 24 порта SFP+ с поддержкой преобразования среды передачи.

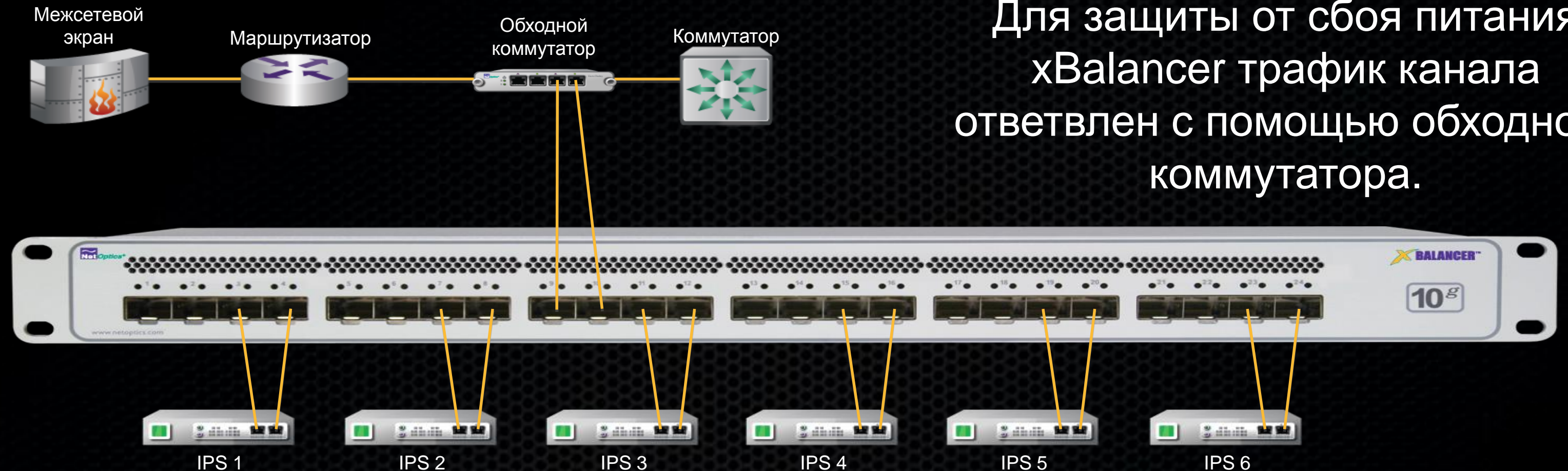
Пример подключения out-of-band



- Распределение агрегированного трафика по пяти сетевым записывающим устройствам для расследования сетевых инцидентов.
- Любой порт может быть задействован в качестве входного, выходного или в том и другом качестве одновременно.

Пример подключения inline

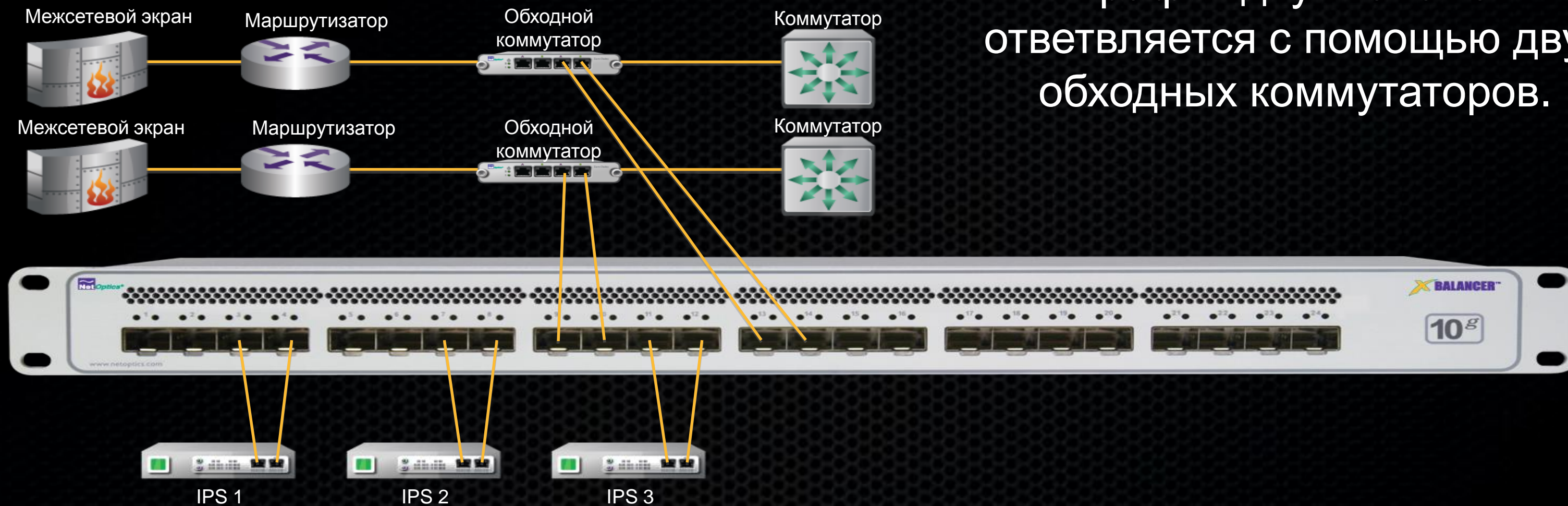
Для защиты от сбоя питания xBalancer трафик канала ответвлен с помощью обходного коммутатора.



- Двухнаправленный inline-трафик распределяется по шести системам IPS.
- Любые порты могут быть использованы в качестве входных, выходных или в обоих качествах.
- xBalancer контролирует состояние систем IPS с использованием статусных (heartbeat) пакетов.

Пример разделения ресурсов средств МОНИТОРИНГА

Трафик двух каналов
ответвляется с помощью двух
обходных коммутаторов.



- Трафик обоих каналов равномерно распределяется по трем системам IPS, но трафик каждого канала остается обособленным!
- Любые порты могут быть использованы в качестве входных, выходных или в обоих качествах.

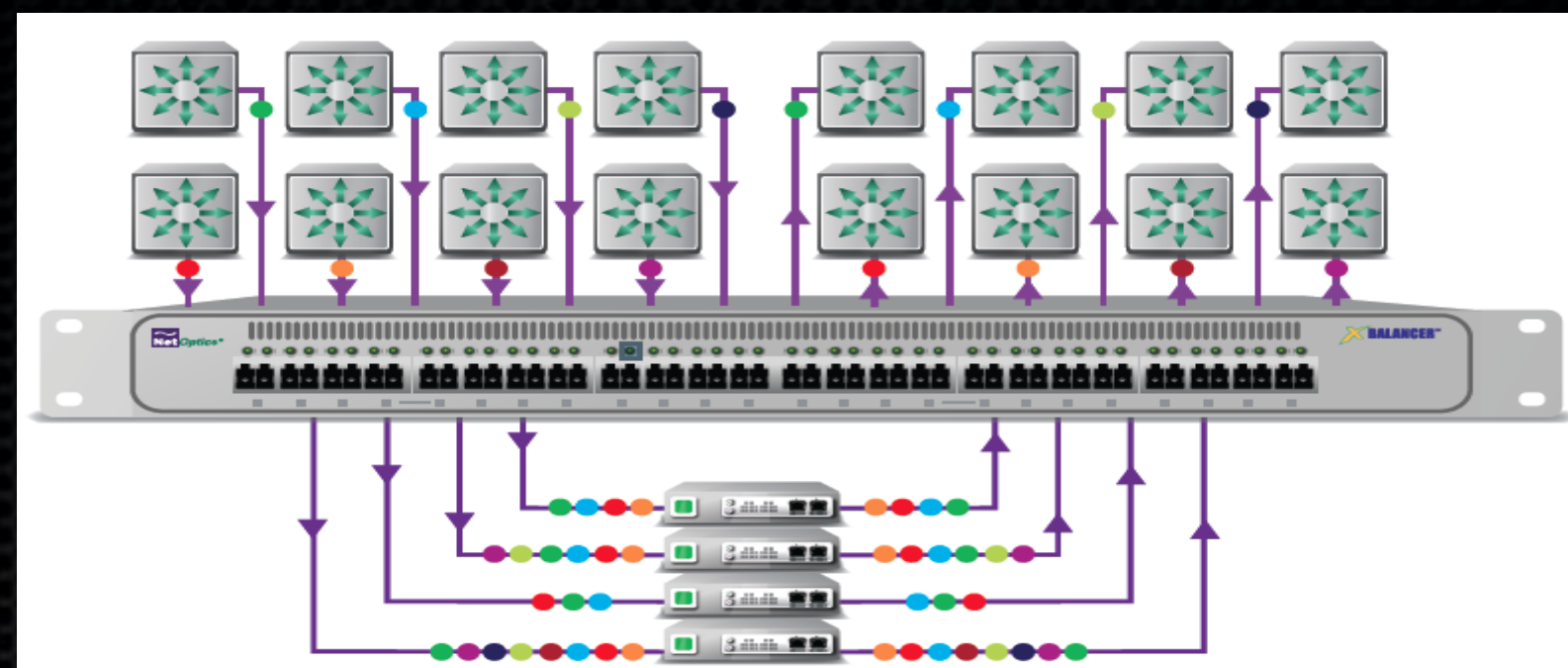
Загруженные конфигурации

- 1 группа

Inline, разделение ресурсов

- 8 независимых каналов

- 4 системы IPS

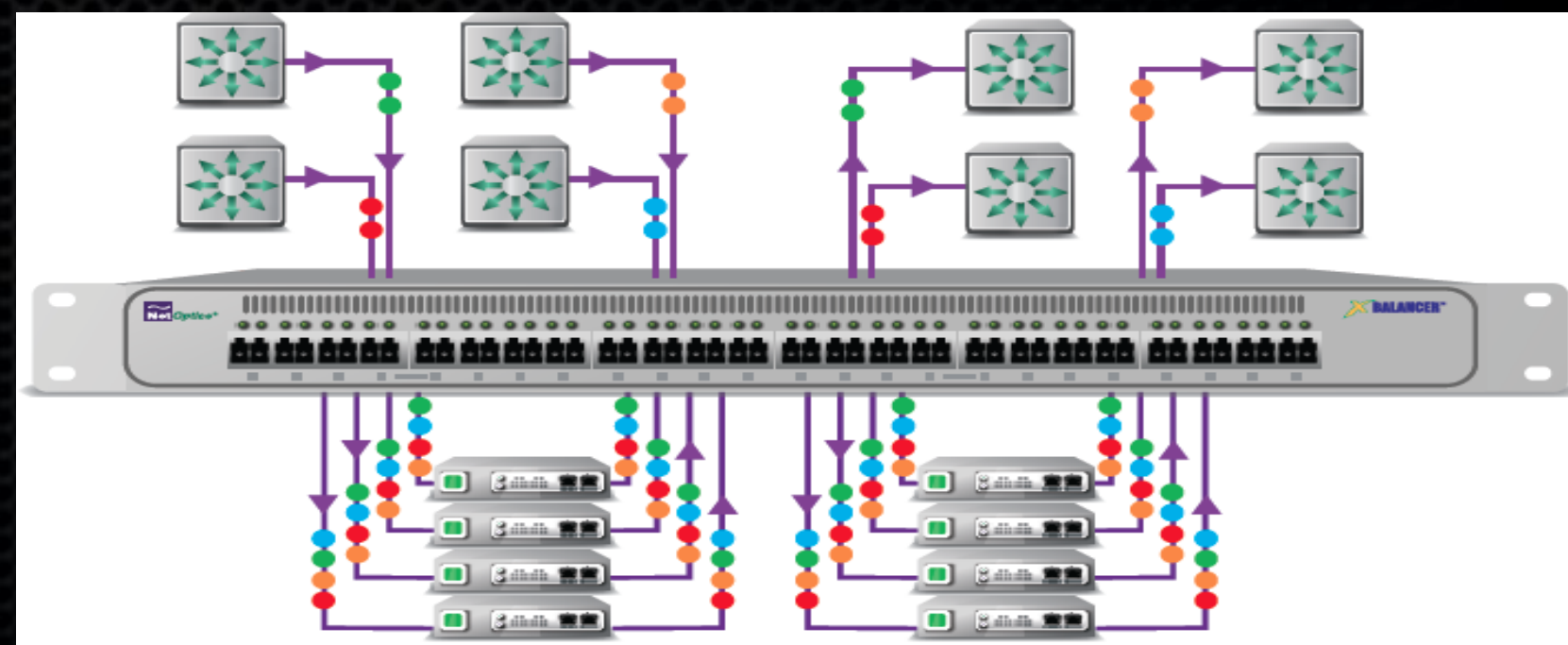


- 1 группа

Inline, разделение ресурсов

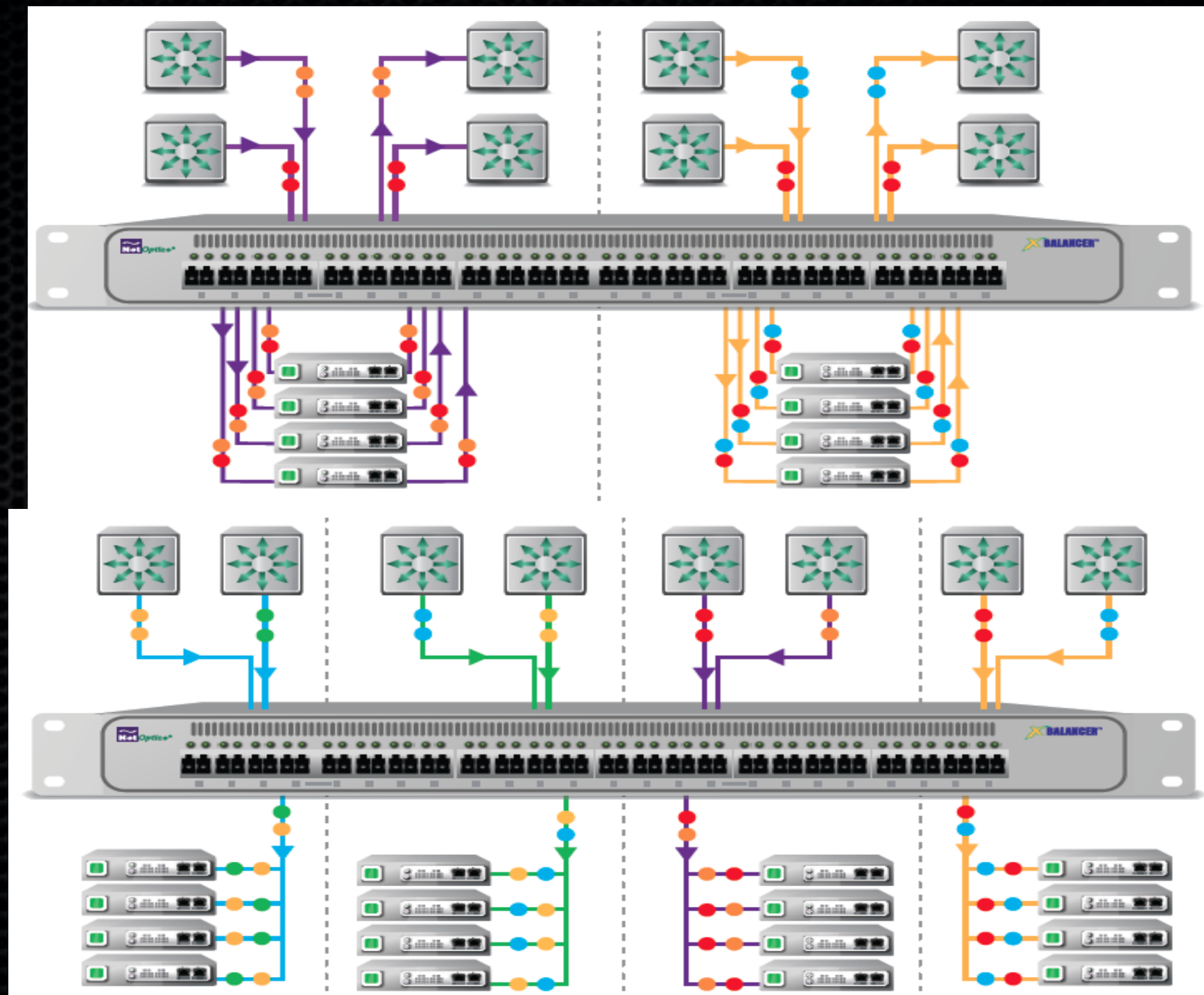
- 4 независимых канала

- 8 систем IPS



Загруженные конфигурации (продолжение)

- 2 группы. Каждая:
- Inline, разделение ресурсов
- 2 независимых канала
- 4 системы IPS
- 4 группы. Каждая:
- Out-of-band, агрегирование
- 2 входных порта
- 4 средства out-of-band



- ✓ 24 входных + 24 выходных порта (симплексные кабели).
- ✓ Контроль состояния inline-средств мониторинга с помощью пакетов heartbeat.
- ✓ Гибкая конфигурация (функциональность Director xStream).
- ✓ Блокировка консоли.
- ✓ TACACS+, RADIUS.
- ✓ SNMP (скоро будет).
- ✓ Графический веб-интерфейс (скоро будет).

Платформа управления Indigo Pro

indigo **PRO**™

 NetOptics®

Краткая характеристика Indigo Pro

Indigo Pro – передовое управляющее решение, обеспечивающее управление устройствами Net Optics, интерфейс типа «инструментальная панель» (dashboard), графическое представление информации, а также сбор и визуализацию статистических данных о трафике, передаваемых устройствами Net Optics по сети.

Indigo Pro используется вместе с другими системами сетевого управления с целью сделать сеть более «интеллектуальной» и значительно повысить эффективность работы ИТ-персонала.

Целевые потребители

Существующие клиенты,
которые имеют большое число устройств Director, Director Pro, iTap и др.
которым нужна централизованная простая в использовании платформа
управления с передовыми функциями, включая визуализацию трафика.

Новые заказчики, которые хотят:

- упростить управление многочисленными средствами доступа к данным;

- сократить эксплуатационные расходы;

- использовать имеющиеся в устройствах Net Optics возможности сбора статистических данных о трафике.

- которые имеют новые крупномасштабные инсталляции продуктов Director.

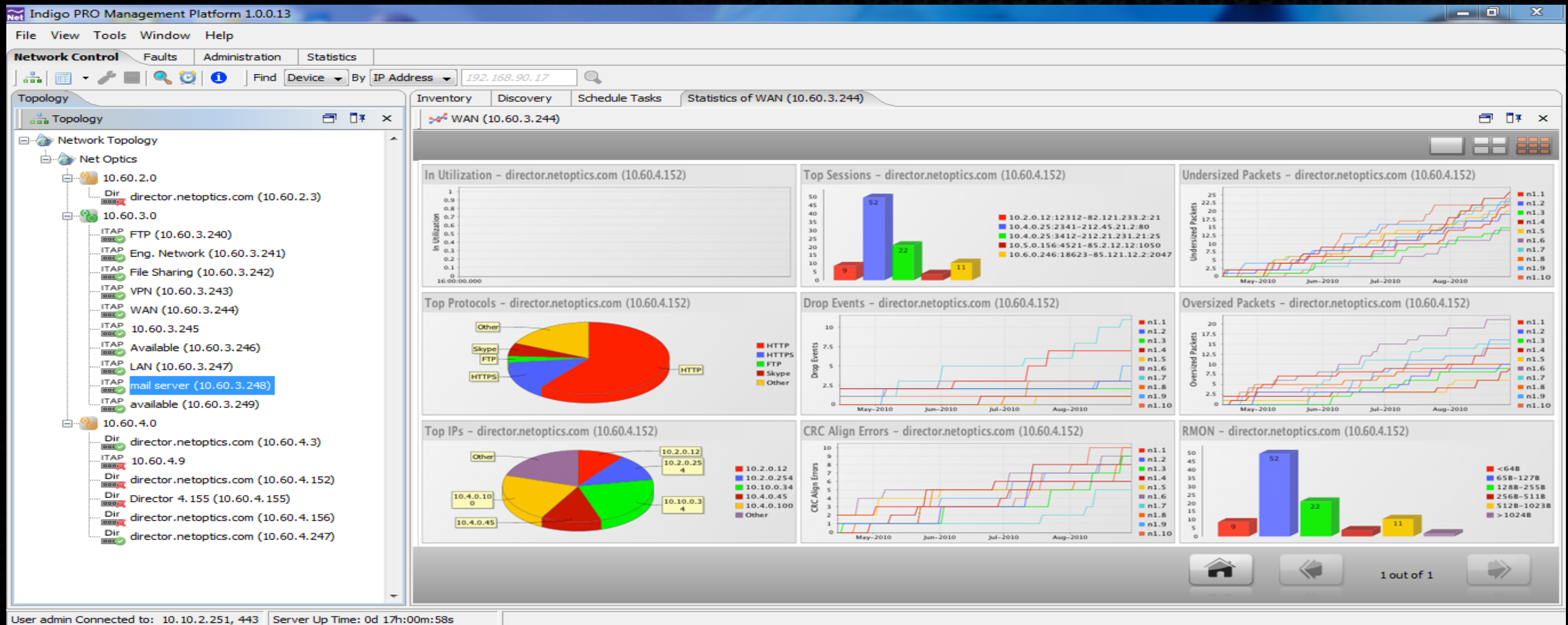
Платформа управления Indigo Pro

Новые решения для управления крупномасштабными инсталляциями продуктов Net Optics.

- Конфигурирование и мониторинг устройств Net Optics (Director, Director Pro, iTap и др.).
- Сбор статистики с использованием технологий ProPush™ и SNMP.
- Мониторинг состояния каналов и трафика.
- Выдача отчетов.
- Интегрированные решения в виде аппаратных устройств:
 - Indigo Collector Pro – собирает и отображает статистику по трафику.
 - Indigo Manager Pro – помимо этого обеспечивает управление устройствами Net Optics.
- Лицензируются по числу узлов (управляемых устройств).



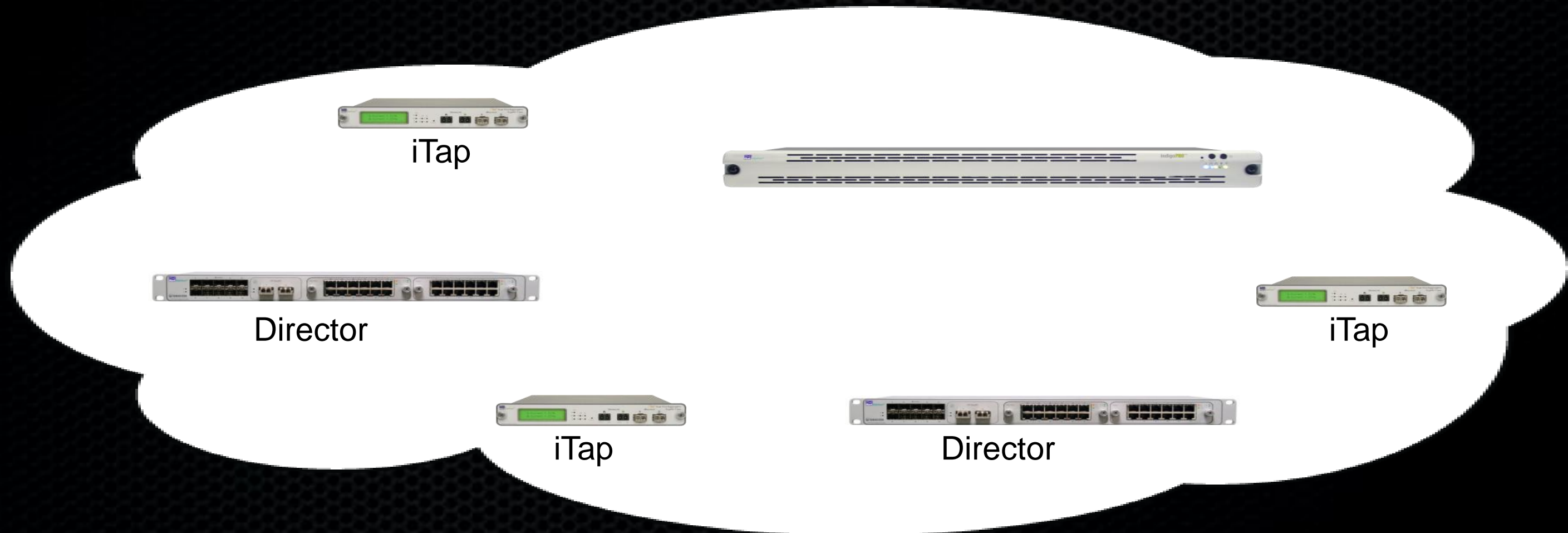
Визуализация трафика. Dashboard



Визуализация трафика. Технология ProPush™

Традиционный NetFlow- или SNMP-опрос: каждые 5–30 минут.

- ProPush: устройства посылают данные в Indigo Pro каждые 1–10 секунд.
- ProPush выявляет микровсплески трафика, которые другие системы не обнаруживают.
- Безопасность: системе управления не нужны IP-адреса устройств.

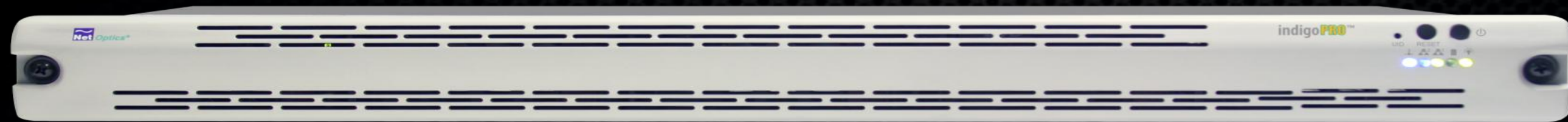


Функциональность и полезность Indigo Pro

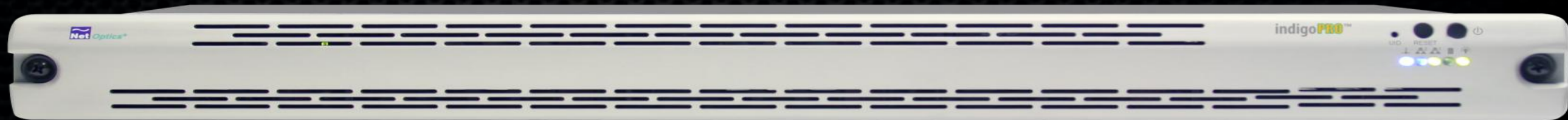
Функция	Описание	Полезность для заказчика
Быстрое обнаружение устройств	Быстрое автоматическое обнаружение устройств Net Optics и других сетевых элементов; создание их иерархии; отображение топологии сети	Быстрые идентификация, локализация и управление всеми сетевыми устройствами с единой консоли
Сбор и хранение статистики по трафику	Сбор статистической информации о трафике с использованием технологии ProPush и SNMP-опроса; статистика хранится в базе данных	Наличие централизованного репозитория статистики по сетевому трафику; обнаружение микровсплесков трафика
Представление статистики по трафику	Многофункциональный презентационный уровень, обеспечивающий вывод различных графиков с размещением их на инструментальной панели	Наглядное представление статистики по трафику, включая вывод информации в реальном масштабе времени и за определенные периоды в прошлом
Конфигурирование устройств и управление ими	Управление сотнями устройств	Единый интерфейс для управления большими инсталляциями устройств различных типов
Изображение устройств	Фотореалистичное представление устройств, включая модули, порты и светодиодные индикаторы	Наглядное изображение устройств, упрощающее управление ими
Массовое обновление программного обеспечения	Обновление ПО и конфигураций многочисленных устройств в рамках одной операции	Простота обновления ПО и конфигураций устройств из центрального узла с протоколированием и изменением управляющей информации
Обработка отказов	События характеризуются цветами сетевых элементов; регистрация принятых и сгенерированных событий	Простота прогнозирования и идентификации проблем с передачей трафика и сбоев в работе устройств

Collector и Manager

- Indigo **Collector Pro** – центральный узел, который собирает и визуализирует статистическую информацию о трафике, предоставляемую устройствами Net Optics.



- Indigo **Manager Pro** обеспечивает все функции Collector Pro плюс возможность управления устройствами Net Optics.



Indigo Collector Pro и Indigo Manager Pro

Характеристика	Indigo Collector Pro	Indigo Manager Pro
Единая аппаратная платформа	+	+
Быстрое обнаружение устройств	+	+
Обработка событий и отказов		+
Массовое обновление ПО		+
Планировщик		+
Конфигурирование устройств и управление ими		+
Изображение устройств		+
Сбор и хранение статистики по трафику	+	+
Инструментальная панель и графики	+	+
Анализ данных	+	+
Пользовательский веб-интерфейс	+	+
Управление учетными записями пользователей	+	+

Обнаружение устройств

The screenshot displays the Indigo PRO Management Platform 1.0.0.13 interface. The main window is titled "Network Control" and includes a menu bar (File, View, Tools, Window, Help) and a toolbar with icons for various functions. The "Discovery" tab is active, showing a "Periodic Discovery" configuration. The "Next Start At" is set to "4/14/10 10:21:56 AM" and "Run Every [hours]" is set to "8". A search bar at the top right shows "192.168.90.17".

On the left, the "Topology" pane shows a hierarchical view of the network. Under "Net Optics", there are two main IP ranges: 10.60.2.0 and 10.60.3.0. The 10.60.3.0 range includes several subnets: FTP (10.60.3.240), Eng. Network (10.60.3.241), File Sharing (10.60.3.242), VPN (10.60.3.243), WAN (10.60.3.244), 10.60.3.245, Available (10.60.3.246), LAN (10.60.3.247), mail server (10.60.3.248), and available (10.60.3.249). The 10.60.4.0 range includes: director.netoptics.com (10.60.4.3), 10.60.4.9, director.netoptics.com (10.60.4.152), Director 4.155 (10.60.4.155), director.netoptics.com (10.60.4.156), and director.netoptics.com (10.60.4.247).

The "Discovery" pane shows a table of discovery ranges:

From IP	To IP	Mask
10.60.2.0		255.255.255.0
10.60.4.1	10.60.4.254	
10.60.3.0		255.255.255.0

An "Add Discovery Range" dialog box is open, showing the configuration for a new range. The "Discovery Range" section has "IP range" selected. The "From IP" and "To IP" fields are empty. The "Subnet" option is unselected. The "IP" field is empty and the "Mask" is set to "255 . 255 . 255 . 0". The "SNMPv2c Settings" section has a table with columns "Read", "Write", "Port", and "SNM", and buttons "Add", "Edit", and "Delete". The "Device Defaults" section has "Subnet Name" (empty) and "Group Name" (set to "Net Optics"). The "Run Immediately" checkbox is checked. "OK" and "Cancel" buttons are at the bottom.

At the bottom of the main window, a status bar shows "User admin Connected to: 10.10.2.251, 443" and "Server Up Time: 0d 17h:07m:57s".

Инвентаризация устройств

The screenshot displays the Indigo PRO Management Platform 1.0.0.13 interface. The left pane shows a network topology tree with nodes for Net Optics, 10.60.2.0, 10.60.3.0, and 10.60.4.0. The right pane shows an inventory table for devices.

Device	Product	Power Supply 1	Power Supply 2	SW Version
FTP (10.60.3.240)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
10.60.3.245	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
VPN (10.60.3.243)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
available (10.60.3.249)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
LAN (10.60.3.247)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
WAN (10.60.3.244)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
mail server (10.60.3.248)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
Eng. Network (10.60.3.241)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
Available (10.60.3.246)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
File Sharing (10.60.3.242)	1G Copper 10/100/1000 Inline Port Aggregator	ON	ON	
director.netoptics.com (10.60.4.247)	Director :DIR740000093V005	Not Present	Not Present	dir_030002_030810
Director 4.155 (10.60.4.155)	Director :DIR74000001652955	N/A	N/A	
director.netoptics.com (10.60.4.152)	Director :DIR7400000165298	Not Present	Not Present	dir_030002_032210
director.netoptics.com (10.60.4.156)	Director :DIR7400000165296	Not Present	Not Present	dir_030002_030510
director.netoptics.com (10.60.4.3)	Director :000000-0000-0000000	Not Present	Not Present	dir_030100_041410
10.60.4.9				
director.netoptics.com (10.60.2.3)	Director :DIR74000008CF004	N/A	N/A	

Net Optics Devices (17) Other Devices (0)

User admin Connected to: 10.10.2.251, 443 Server Up Time: 0d 17h:05m:57s

Планировщик заданий

The screenshot displays the Indigo PRO Management Platform 1.0.0.13 interface. The main window is titled 'Indigo PRO Management Platform 1.0.0.13' and has a menu bar with 'File', 'View', 'Tools', 'Window', and 'Help'. Below the menu bar are tabs for 'Network Control', 'Faults', 'Administration', and 'Statistics'. A search bar is present with 'Find Device' and 'By IP Address' set to '192.168.90.17'. The main area is divided into several panes:

- Topology:** A tree view showing a network structure under 'Net Optics'. It includes sub-nodes like '10.60.2.0', '10.60.3.0', and '10.60.4.0', each with associated services like 'FTP', 'Eng. Network', 'File Sharing', 'VPN', 'WAN', 'mail server', and 'available'.
- Schedule Tasks:** A pane with tabs for 'Inventory', 'Discovery', 'Schedule Tasks', and 'Statistics of WAN (10.60.3.244)'. It shows 'Task Configuration' with 'Max Concurrent Devices' set to 10. Below is a 'Task List' table with one entry: 'SW Upgrade'. At the bottom, there are 'Add Task', 'Edit', and 'Remove' buttons.
- Selected Task Status:** A table listing the status of selected tasks, including device names and their IP addresses.

A 'Schedule Task' dialog box is open in the foreground, titled 'Task Targets'. It prompts the user to 'Please Select the effected devices of this task:'. It features two lists:

- Available Devices:** Lists 'All Devices', 'director.netoptics.com (10.60.4.156)', and 'Director 4.155 (10.60.4.155)'. A right-pointing arrow button is next to this list.
- Selected Devices:** Lists 'director.netoptics.com (10.60.2.3)', 'director.netoptics.com (10.60.4.152)', 'director.netoptics.com (10.60.4.247)', and 'director.netoptics.com (10.60.4.3)'. A left-pointing arrow button is next to this list.

Navigation buttons at the bottom of the dialog include 'Back', 'Next', 'Finish', and 'Cancel'. The status bar at the bottom of the application shows 'User admin Connected to: 10.10.2.251, 443' and 'Server Up Time: 0d 17h:09m:58s'.

Панель событий

Indigo PRO Management Platform 1.0.1.3

File View Tools Window Help

Network Control | Faults | Administration | Dashboard

Find Device By IP Address 192.168.90.17

Topology

Network...

- London
 - Net Optics
 - 10.60.2.0
 - Dir (10.60.2.3)
 - 10.60.3.0
 - ITAP FTP (10.60.3.240)
 - ITAP Eng. Network (10.60.3.241)
 - ITAP File Sharing (10.60.3.242)
 - ITAP VPN (10.60.3.243)
 - ITAP WAN (10.60.3.244)
 - ITAP 10.60.3.245
 - ITAP Available (10.60.3.246)
 - ITAP LAN (10.60.3.247)
 - ITAP mail server (10.60.3.248)
 - ITAP available (10.60.3.249)
 - 10.60.4.0
 - Dir director1 (10.60.4.3)
 - 10.60.4.9
 - Pro director2 (10.60.4.152)
 - Dir director3 (10.60.4.155)
 - Dir director4 (10.60.4.156)
 - Dir director5 (10.60.4.247)
 - New York
 - Stock Exchange

Inventory | Device View | Discovery | Schedule Tasks | Statistics of director2 (10.60.4.152)

director2 (10.60.4.152)

The dashboard displays several charts for director2 (10.60.4.152):

- Top Protocols**: Pie chart showing HTTP as the dominant protocol.
- Undersized Packets**: Line chart showing packet counts over time for various ports (n1.1 to n1.10).
- In Utilization**: Line chart showing network utilization percentage over time.
- Top IPs**: Pie chart showing traffic distribution by IP address.
- Oversized Packets**: Line chart showing oversized packet counts over time.
- Drop Events**: Line chart showing the number of dropped packets over time.
- Top Sessions**: Bar chart showing the number of sessions for different IP ranges.
- RMON**: Bar chart showing RMON statistics for different packet size ranges.
- CRC Align Errors**: Line chart showing the number of CRC alignment errors over time.

Events - director2 (10.60.4.152)

Time & Date	Severity	Ack.	Description	Source	Type
4/16/10 4:11:...	Major		Connection to device lost	director2 (10.60.4.152)	Device Disconnected
4/16/10 4:10:...	Info		Connection to device restored	director2 (10.60.4.152)	Device Connected
4/14/10 4:18:...	Major		Connection to device lost	director2 (10.60.4.152)	Device Disconnected
4/14/10 1:30:...	Info		Connection to device restored	director2 (10.60.4.152)	Device Connected
4/14/10 1:30:...	Major		Connection to device lost	director2 (10.60.4.152)	Device Disconnected
4/13/10 11:12:...	Info		Connection to device restored	director2 (10.60.4.152)	Device Connected
4/13/10 11:12:...	Major		Connection to device lost	director2 (10.60.4.152)	Device Disconnected
4/13/10 10:42:...	Info		Connection to device restored	director2 (10.60.4.152)	Device Connected
4/13/10 10:42:...	Major		Connection to device lost	director2 (10.60.4.152)	Device Disconnected
4/13/10 6:04:...	Info		Connection to device restored	director2 (10.60.4.152)	Device Connected

User admin Connected to: 10.10.2.251, 443 Server Up Time: 0d 06h:22m:14s

Мастер диаграмм

Report Type ▼

Network Topology

- Subnet Group 1
 - Subnet Group 1
 - 192.168.200.103(Paris-BS-01)
 - 192.168.200.103(Paris-BS-01)
 - Subnet 2
 - 192.168.200.103(Paris-BS-01)
- Group

Protocols between 192.168.10.1 and 80.187.90.22

Protocol	Percentage
HTTPS	30%
FTP	30%
ICQ	40%

Snapshot

From ▼ ▼

▼ Back

Apply

Изображение устройства

The screenshot displays the Net Optics Collector 1.0.0.3 software interface. The main window is divided into several sections:

- Topology:** A tree view on the left showing a network topology. Under "Subnet Group 1", there are three ITAP devices with IP addresses 10.50.0.15, 10.50.0.16, and 10.50.0.17. Below that, under "Net Optics", there are five Director devices with IP addresses 10.60.4.4, 10.60.4.151, 10.60.4.152, 10.60.4.155, and 10.60.4.157, all associated with the domain director.netoptics.com.
- Panel View:** The main area on the right shows a detailed view of the selected device, 10.60.4.152 (director.netoptics.com). It features a high-resolution image of the physical device, which is a rack-mountable network switch with various ports and a "Net Optics" logo.
- Events - Subnet Group 1:** A table at the bottom right displays recent events. The table has columns for Time & Date, Severity, Ack., Description, Source, and Type.

At the bottom of the window, a status bar shows: "User admin Connected to: localhost, 443" and "Server Up Time: 0d 00h:34m:46s".

Time & Date	Severity	Ack.	Description	Source	Type
03:13:27 08/04/10	Info		Connection to device restored	10.60.4.152 (director.netoptics.com)	Device Connected
03:13:16 08/04/10	Major		Connection to device lost	10.60.4.152 (director.netoptics.com)	Device Disconnected
01:23:28 08/04/10	Major		Connection to device lost	10.60.4.4 (director.netoptics.com)	Device Disconnected

Задание прав пользователей

The screenshot displays the NetOptics NMS 1.0.0.0 Administration interface. The main window is titled "Administration" and contains a left-hand navigation tree with categories like Access Control, Server Settings, Database Settings, Northbound Interface, Events Configuration, and Third Party Settings. The "Users" tab is active, showing a list of profiles: Admin, Tech, and Viewer. The "Admin" profile is selected, and its configuration is shown in the main area. The configuration includes a "Profile Name" field set to "Admin", an "Admin Operations" section with checkboxes for System Administration, Users Management, Profiles Management, and Views Management, and an "Application Operations" section with checkboxes for View Events, Acknowledge Events, Topology Change, Topology View, Tasks Configuration, Tasks View, Device Configuration, Advanced Device Configuration, Discovery View, Discovery Configuration, and Performance View. At the bottom of the configuration area are buttons for "New Profile", "Delete", and "Apply". The status bar at the bottom indicates "User admin Connected to: localhost, 443", "Server Up Time: 0d 00h: 11m: 16s", and a red warning: "The NMS license will expire in 28 days."

NetOptics NMS 1.0.0.0

File View Tools Window Help

Network Control Faults Administration Statistics

Administration

- Access Control
- Server Settings
- Database Settings
- Northbound Interface
- Events Configuration
- Third Party Settings

Users Profiles Views

- Admin
- Tech
- Viewer

Details

Profile Name: Admin

Admin Operations

- System Administration
- Users Management
- Profiles Management
- Views Management

Application Operations

- View Events
- Acknowledge Events
- Topology Change
- Topology View
- Tasks Configuration
- Tasks View
- Device Configuration
- Advanced Device Configuration
- Discovery View
- Discovery Configuration
- Performance View

New Profile Delete Apply

System Settings Audit Trail

User admin Connected to: localhost, 443 | Server Up Time: 0d 00h: 11m: 16s | The NMS license will expire in 28 days.

Контрольный журнал

NetOptics NMS 1.0.0.0

File View Tools Window Help

Network Control Faults **Administration** Statistics

Administration

Seq No.	Time & Date	Username	Operation	IP Address	Status
173	15:56:10 22/03/10	admin	Get View	127.0.0.1	Allowed
172	15:56:07 22/03/10	admin	system_administration	127.0.0.1	Allowed
171	15:56:07 22/03/10	admin	system_administration	127.0.0.1	Allowed
170	15:56:04 22/03/10	admin	Login	127.0.0.1	Allowed
169	15:53:51 22/03/10	admin	Logout	127.0.0.1	Allowed
168	15:53:46 22/03/10	admin	Get Tasks	127.0.0.1	Allowed
167	15:53:46 22/03/10	admin	Get Tasks	127.0.0.1	Allowed
166	15:53:43 22/03/10	admin	System Administration	127.0.0.1	Allowed
165	15:53:43 22/03/10	admin	System Administration	127.0.0.1	Allowed
164	15:53:43 22/03/10	admin	System Administration	127.0.0.1	Allowed
163	15:53:43 22/03/10	admin	System Administration	127.0.0.1	Allowed
162	15:53:43 22/03/10	admin	Get Element	127.0.0.1	Allowed
161	15:53:42 22/03/10	admin	Get View	127.0.0.1	Allowed
160	15:53:40 22/03/10	admin	system_administration	127.0.0.1	Allowed
159	15:53:40 22/03/10	admin	system_administration	127.0.0.1	Allowed
158	15:53:37 22/03/10	admin	Login	127.0.0.1	Allowed
157	15:53:05 22/03/10	admin	Logout	127.0.0.1	Allowed
156	15:47:48 22/03/10	admin	Get Performance	127.0.0.1	Allowed
155	15:47:48 22/03/10	admin	Get Performance	127.0.0.1	Allowed
154	15:47:14 22/03/10	admin	Get Tasks	127.0.0.1	Allowed
153	15:47:13 22/03/10	admin	Get Tasks	127.0.0.1	Allowed
152	15:47:10 22/03/10	admin	System Administration	127.0.0.1	Allowed
151	15:47:10 22/03/10	admin	System Administration	127.0.0.1	Allowed
150	15:47:10 22/03/10	admin	System Administration	127.0.0.1	Allowed
149	15:47:10 22/03/10	admin	System Administration	127.0.0.1	Allowed
148	15:47:10 22/03/10	admin	Get Element	127.0.0.1	Allowed
147	15:47:09 22/03/10	admin	Get View	127.0.0.1	Allowed
146	15:47:06 22/03/10				
145	15:47:06 22/03/10				
144	15:47:03 22/03/10				
143	15:45:59 22/03/10				
142	15:43:23 22/03/10				
141	15:43:23 22/03/10				
140	15:43:17 22/03/10				
139	15:43:17 22/03/10				
138	15:43:14 22/03/10				
137	15:43:14 22/03/10				
136	15:43:13 22/03/10				
135	15:43:13 22/03/10				
134	15:43:13 22/03/10				
133	15:43:13 22/03/10				
132	15:43:10 22/03/10	admin	system_administration	127.0.0.1	Allowed
131	15:43:10 22/03/10	admin	system_administration	127.0.0.1	Allowed
130	15:43:06 22/03/10	admin	Login	127.0.0.1	Allowed
129	15:41:55 22/03/10	admin	Get Performance	127.0.0.1	Allowed
128	15:41:45 22/03/10	admin	Get Tasks	127.0.0.1	Allowed
127	15:41:45 22/03/10	admin	Get Tasks	127.0.0.1	Allowed

<< Refresh Filter Export to CSV print >>

System Settings Audit Trail

User admin Connected to: localhost, 443 | Server Up Time: 0d 00h:12m:16s | **The NMS license will expire in 28 days.**

Audit Filter Dialog

Operation Time From: 15:59:38 21/03/10 To: 15:59:38 22/03/10

Operation Name Contains

Operation Status Status Allowed

Action Username Username admin

User Address Contains

Select All

OK Cancel

Обработка отказов

The screenshot displays the NetOptics NMS 1.0.0.0 interface. The main window shows a table of events with columns for Time & Date, Severity, Ack., Description, Source, and Type. An 'Events Filter' dialog box is open, allowing users to filter events based on various criteria.

Time & Date	Severity	Ack.	Description	Source	Type
12:29:48 22/03/10	Info		deviceConnectedDescription	192.168.10.135 ()	Device Connected
12:15:16 22/03/10	Major		deviceDisconnectedDescription	192.168.10.135 ()	Device Disconnected
18:12:45 21/03/10	Major		deviceDisconnectedDescription	192.168.10.134 (Director 1)	Device Disconnected
18:12:16 21/03/10	Info		deviceConnectedDescription	192.168.10.134 (Director 1)	Device Connected
18:07:25 21/03/10	Major		deviceDisconnectedDescription	192.168.10.134 (Director 1)	Device Disconnected
17:51:36 21/03/10	Info		deviceConnectedDescription	192.168.10.134 (Director 1)	Device Connected
17:25:36 21/03/10	Major		deviceDisconnectedDescription	192.168.10.134 (Director 1)	Device Disconnected
17:15:26 21/03/10	Info		deviceConnectedDescription	192.168.10.134 (Director 1)	Device Connected
17:10:16 21/03/10	Major		deviceDisconnectedDescription	192.168.10.134 (Director 1)	Device Disconnected
12:50:52 21/03/10	Info		deviceConnectedDescription	192.168.10.134 (Director 1)	Device Connected
12:50:52 21/03/10	Info		deviceConnectedDescription	192.168.10.135 ()	Device Connected
12:50:39 21/03/10	Major		deviceDisconnectedDescription	192.168.10.135 ()	Device Disconnected
12:50:39 21/03/10	Major		deviceDisconnectedDescription	192.168.10.134 (Director 1)	Device Disconnected

Events Filter

- Seq No. Equals or Lower
- Severity Equals Minor
- Ack Status Ack. Unack.
- Event Type Director Status
 - ITap Link Status
 - ITap System
 - Director Configuration
 - ITap Utilization
 - Device Connected
 - ITap Power Supply
 - Device Disconnected
- Select/Deselect All
- Event Time From: 16:01:08 22/03/10 To: 16:01:08 22/03/10
- Source Path Contains

OK Cancel

User admin Connected to: localhost, 443 | Server Up Time: 0d 00h:14m:16s | The NMS license will expire in 28 days.

Конфигурирование устройства

The screenshot displays the Net Optics Collector 1.0.0.3 interface. The main window is titled "Device View" and shows configuration for the device "10.60.4.151 (director.netoptics.com)".

System Information:

- Name: director.netoptics.com
- Contact: xin@
- Location: Unknown
- Date & Time: 04/07/10 18:40:53

IP Settings:

- IP Address: 10 . 60 . 4 . 151
- Subnet Mask: 255 . 0 . 0 . 0
- Default Gateway: 10 . 0 . 0 . 1
- SNMP Manager Address: 0 . 0 . 0 . 0

Users Configuration:

Index	User Name	User Password	Privilege
-------	-----------	---------------	-----------

Events - Subnet Group 1:

Time & Date	Severity	Ack.	Description	Source	Type
03:13:27 08/04/10	Info		Connection to device restored	10.60.4.152 (director.netoptics.com)	Device Connected
03:13:16 08/04/10	Major		Connection to device lost	10.60.4.152 (director.netoptics.com)	Device Disconnected
01:23:28 08/04/10	Major		Connection to device lost	10.60.4.4 (director.netoptics.com)	Device Disconnected

At the bottom of the interface, a status bar shows: "User admin Connected to: localhost, 443" and "Server Up Time: 0d 00h:31m:45s".

Управляющие решения Indigo

	CLI	Веб-менеджер	SNMP	Indigo System Manager	Indigo Pro
Предоставление	1	1	1	Windows-приложение	Устройство высотой 1U
Число узлов	1	1	1	1–10	1–1000 (зависит от лицензии)
Функции	<ul style="list-style-type: none"> • Конфиг. • Фильтры/ правила • Последоват. включение • SSH 	<ul style="list-style-type: none"> • Конфиг. • Фильтры/ правила • Последоват. включение • HTTPS 	<ul style="list-style-type: none"> • Управление • Оповещение • MIB 	<ul style="list-style-type: none"> • Управление • Последоват. включение • CLI & веб-менеджер 	<ul style="list-style-type: none"> • Управление устройствами Net Optics • Сбор и визуализация статистики по трафику • Предоставление CLI & веб-интерфейса • Обновление ПО • Управление разнообразными продуктами
Лицензия / цены	Включена в продукт	Включена в продукт	Включена в продукт	Бесплатная, требуется EULA	Платная
Продукты, поддерживаемые на момент анонса	Все	iTap iBypass Director	iTap iBypass Director iLink Agg	iTap iBypass Director	iTap Director Director Pro
Продукты, которые будут поддерживаться	Все	Все	Все	Новые продукты не будут поддерживаться	Все



Реальная безопасность

Реальное соответствие

Реальный мониторинг

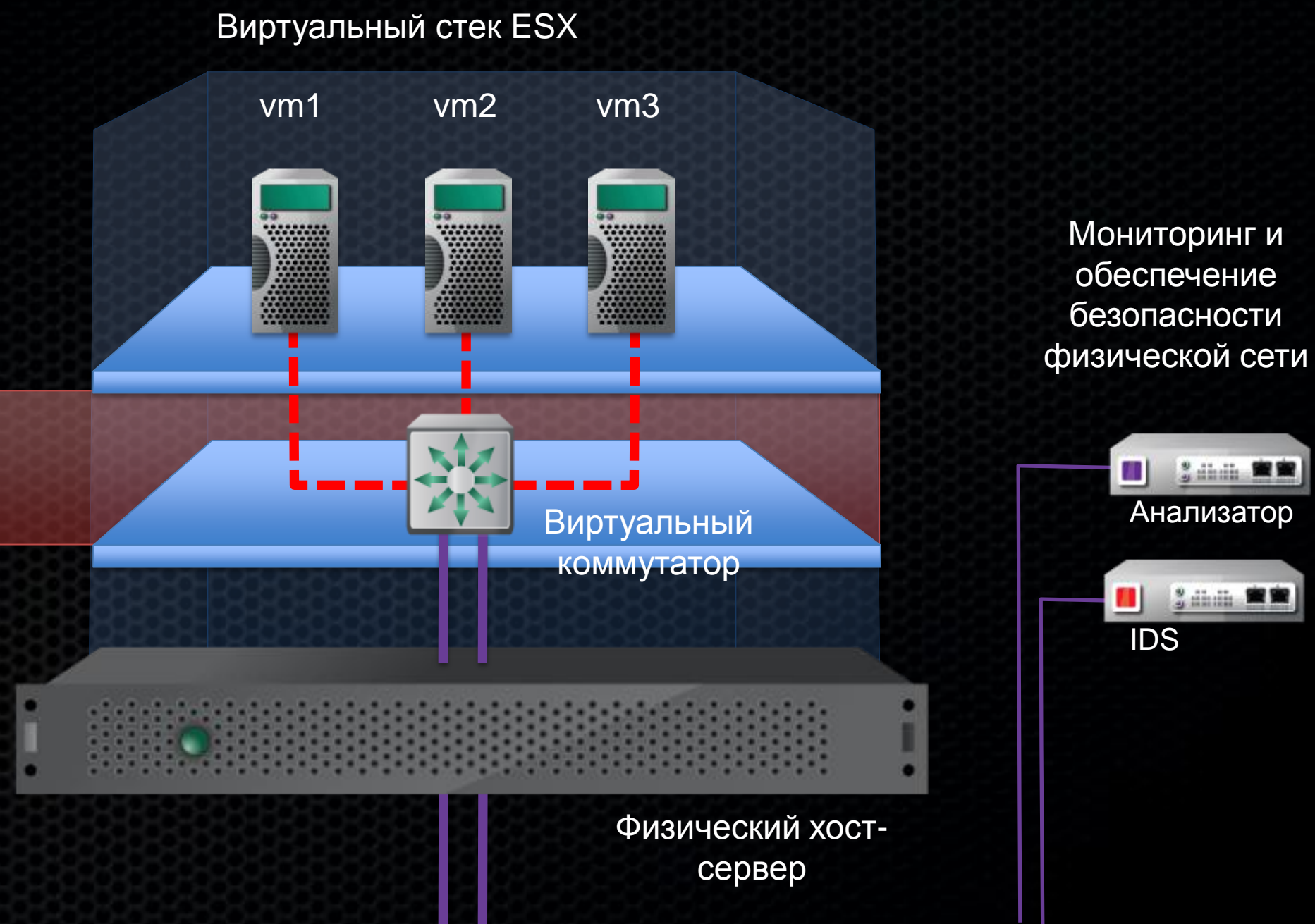
В виртуализированном ЦОДе.

Не обеспечиваются безопасность, мониторинг и контроль соответствия нормативным требованиям



Полное отсутствие контроля трафика между VM

- Нет видимости трафика, уязвимостей и угроз.
- Данные, передаваемые между серверами, не захватываются для аудита.
- Контроль использования ресурсов может выявить источник проблем.

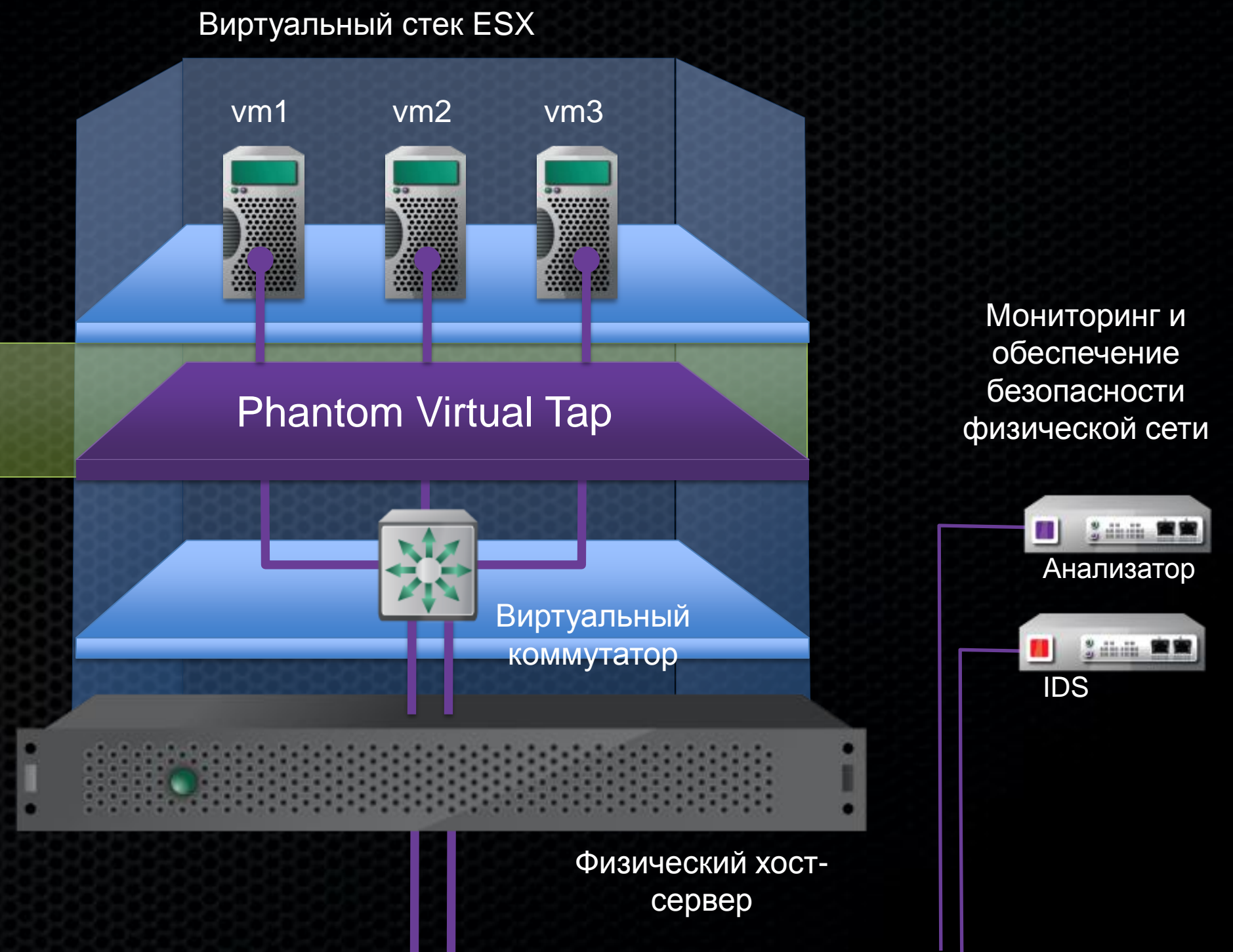


Решение Phantom Virtual Tap

**Обеспечивает
безопасность, мониторинг
работы и контроль
соответствия нормативным
требованиям**

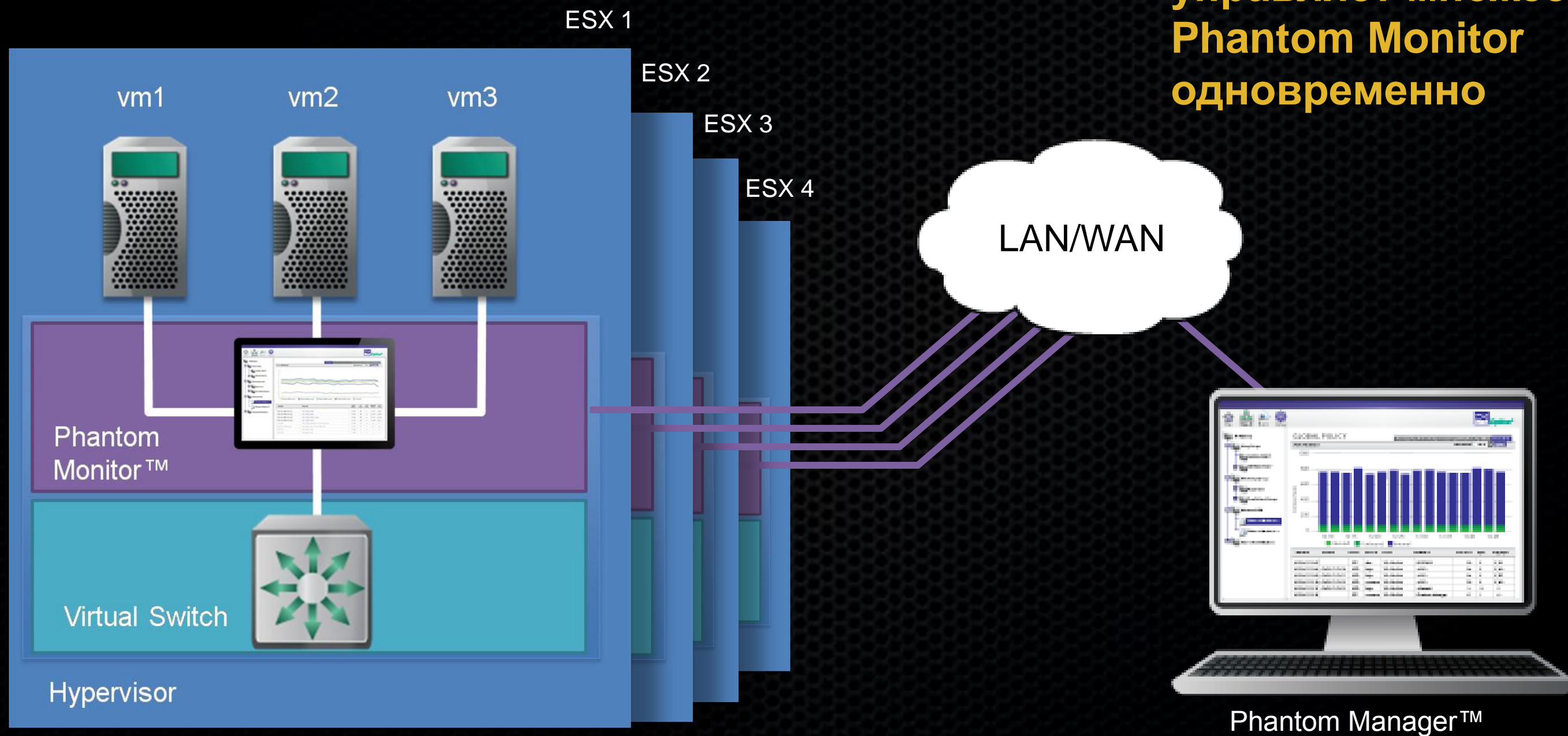
✓ 100%-ная видимость
трафика между VM

- Передает виртуальный трафик физическим средствам мониторинга.
- Устраняет барьеры на пути к виртуализации.
- Способствует достижению надлежащего уровня безопасности и соответствия нормативным требованиям в виртуализированной среде.



Решение на базе гипервизора

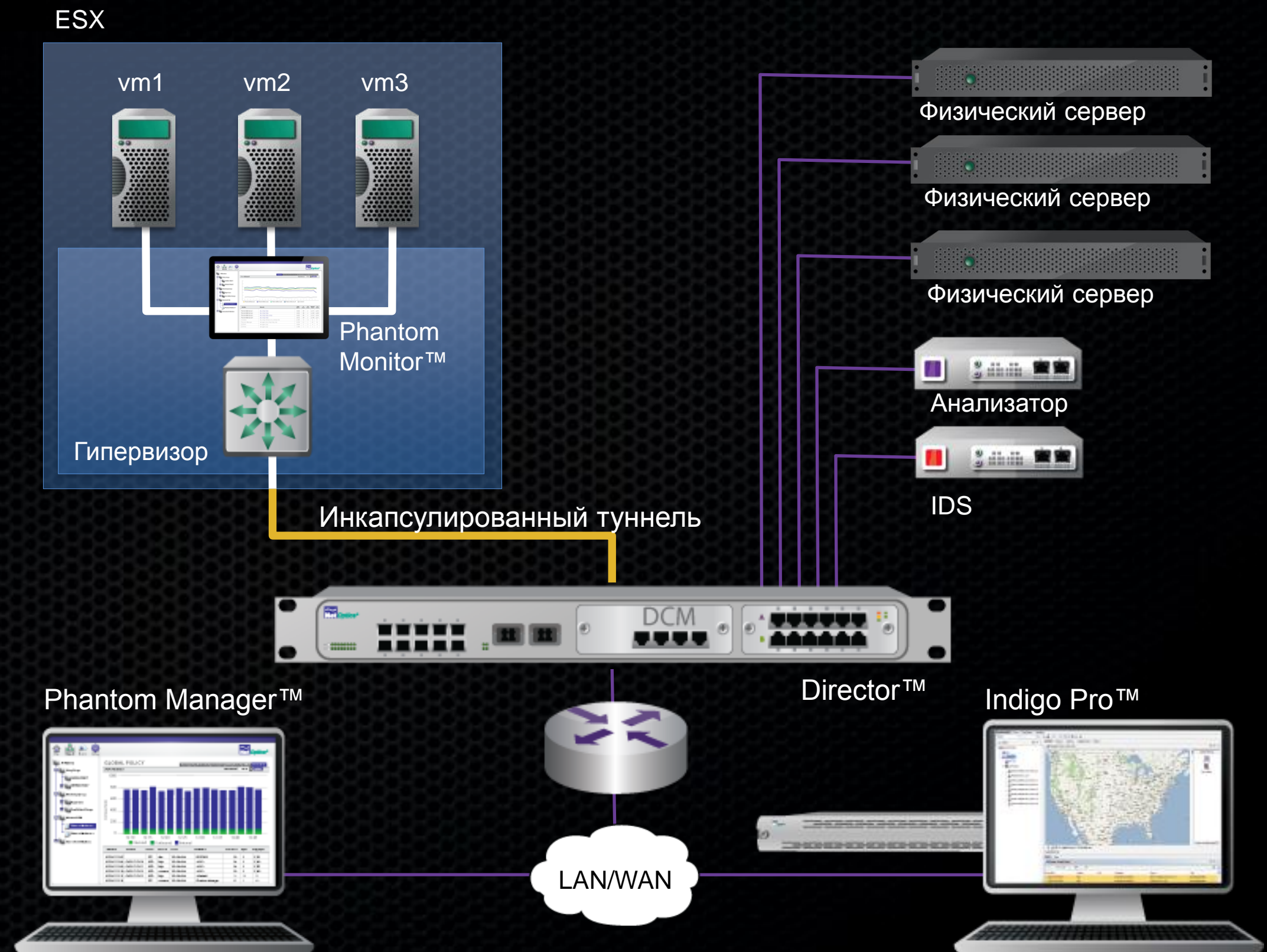
Phantom Manager
управляет множеством
Phantom Monitor
одновременно



Конвергированное решение Net Optics

Конвергенция средств мониторинга физических и виртуальных сетей

- Специальный гипервизорный ответвитель.
 - VMware VMsafe Certified.
 - Полная видимость трафика между VM.
- Ориентация на виртуализацию.
 - Мониторинг при живой миграции (VMotion).
 - Ответвитель для каждой VM (по VM ID).
- Тесная интеграция с VMware vCenter.
- Отказоустойчивая не нарушающая работу сети архитектура.





- Обеспечивает полный контроль трафика в виртуальной среде
- Позволяет осуществлять контроль безопасности, соответствия нормативным требованиям и производительности сетей
- Помогает реализовать весь потенциал вашего виртуального ЦОДа

Получите 30-дневную пробную копию!

appTap-Устройство мониторинга



The image displays the NetOptics appTap device and its corresponding web-based monitoring interface. The device is a rack-mountable unit with a small LCD screen, network ports labeled 'Network A/B' and 'Monitor A/B', and a 'Capture' port. The interface is divided into several sections:

- Navigation:** Log Off, Configure, Packet Capture, Capacity Planner, Availability, Events.
- Time Selection:** Last Hour, Last 8 Hours, Last Day, Last 2 Days, Last Week, Custom.
- Top 30 Clients and Servers:** Subnet: Default (0.0.0.0/0), 10 Mbps, All Applications. Time range: 1/3/2011, 00:00 to 18/3/2011, 17:30. A bar chart shows traffic volume in GBytes, with 'Octets To' in blue and 'Octets From' in green.
- Application Distribution:** A pie chart showing traffic by application. The largest slice is HTTP at 77.28%.
- Reports:** A list of report types including Vol History, Vol Summary, App Distrib, App History, Top Talkers, Conn Summ, VoIP Calls, ToS Report, and Flow Map.
- Historical Data:** A bar chart showing traffic volume over time from 2011-03-03 to 2011-03-16.

Application	Percentage
HTTP	77.28%
Port 6001	0.26%
imap	0.57%
smtp	1.10%
imaps	1.11%
domain	1.29%
POP3	2.19%
POP3S	4.67%
HTTPS	5.57%
Port 61	5.65%

- первое в отрасли интегрированное решение, в котором функционал ответвителя сетевого трафика сочетается с возможностями анализа работы сети и приложений.
- удовлетворяет потребность предприятий в недорогом мониторинге сетей их удаленных филиалов с каналами доступа в Интернет на скоростях до 100 Мбит/с.
- устройство типа plug-and-play
- В зависимости от потребностей своего бизнеса заказчик может выбрать одну из трех версий (или конфигураций) appTap

- Мониторинг сети, приложений, веб-доступа, средств IM и VoIP.
- Непрерывный и эпизодический захват пакетов. Захват заголовков и контента с использованием различных фильтров.
- Выдача информации об использовании сети
- Отображение корреляции VoIP SIP/RTP и предоставление детальной информации об отдельных VoIP-вызовах.
- Одновременный мониторинг многочисленных сетей, подсетей и виртуальных ЛВС с единой консоли.
- Генерирование и экспорт записей NetFlow.
- Отображение динамики параметров сети во времени.
- Снижение потребности в высококвалифицированных инженерах.
- Возможность подключения продуктов (например, систем IDS) других фирм через порты мониторинга.

Приложения appTap

Функции	Network Monitoring	Application Monitoring	Session Monitoring
Выдача статистической информации о работе сети	+	+	+
Захват пакетов	+	+	+
Экспорт записей NetFlow	+	+	+
Выдача лестничных диаграмм потоков	+	+	+
Доступ к сохраненным данным		+	+
Поддержка многочисленных пользователей		+	+
Поддержка многочисленных сетей		+	+
Мониторинг приложений		+	+
Анализ потоков		+	+
Выдача детальной информации о VoIP- вызовах			+
Мониторинг веб-доступа			+
Мониторинг IM			+

Вопросы?

