# Безопасность оператора связи

## Взгляд из 2005-го года

Алексей Лукацкий
Бизнес-консультант по кибербезопасности
22 ноября 2018

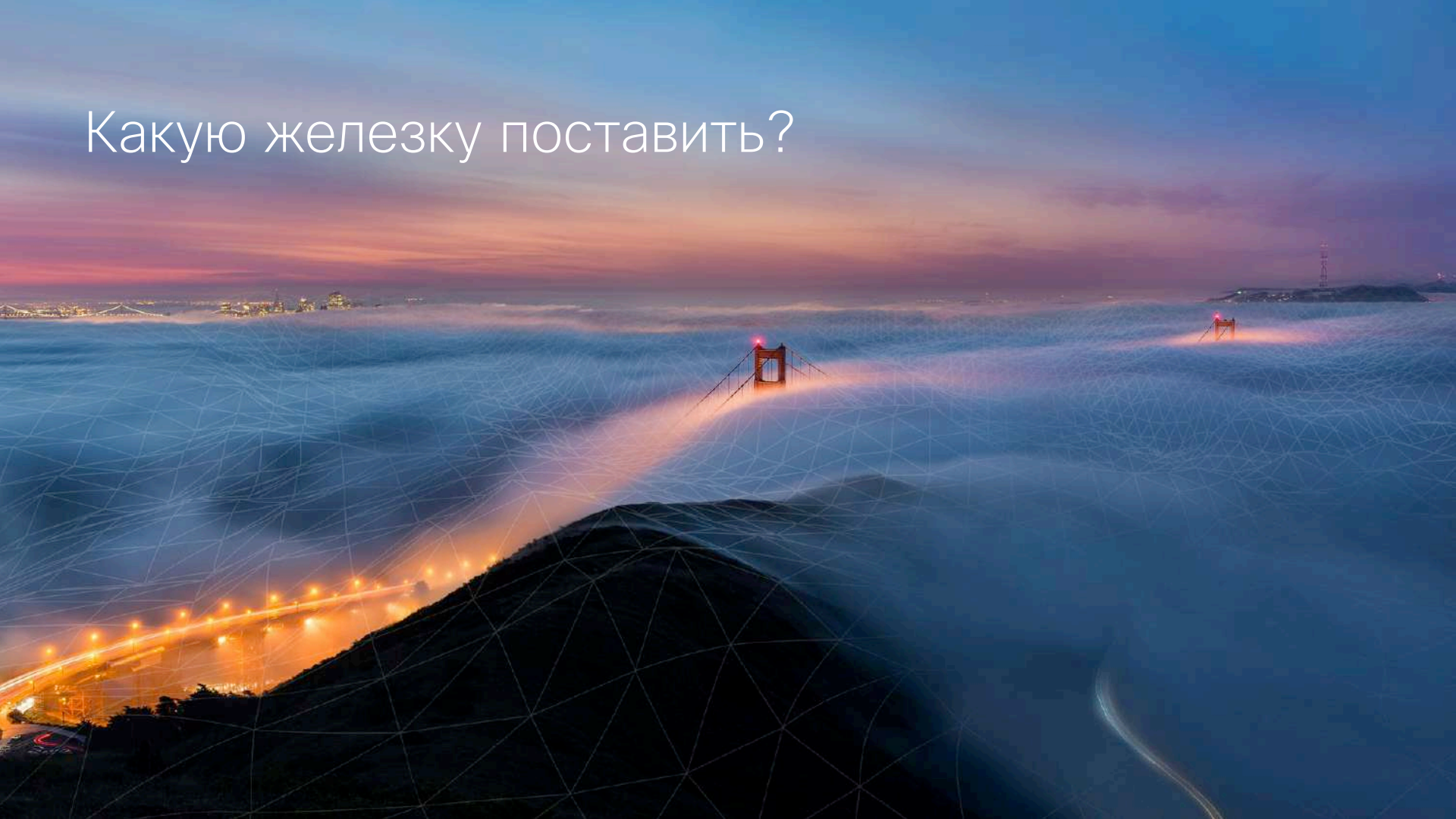
# Кибербезопасность у оператора связи


Защита внутренней ИТ-инфраструктуры оператора связи (офисные системы и т.п.)

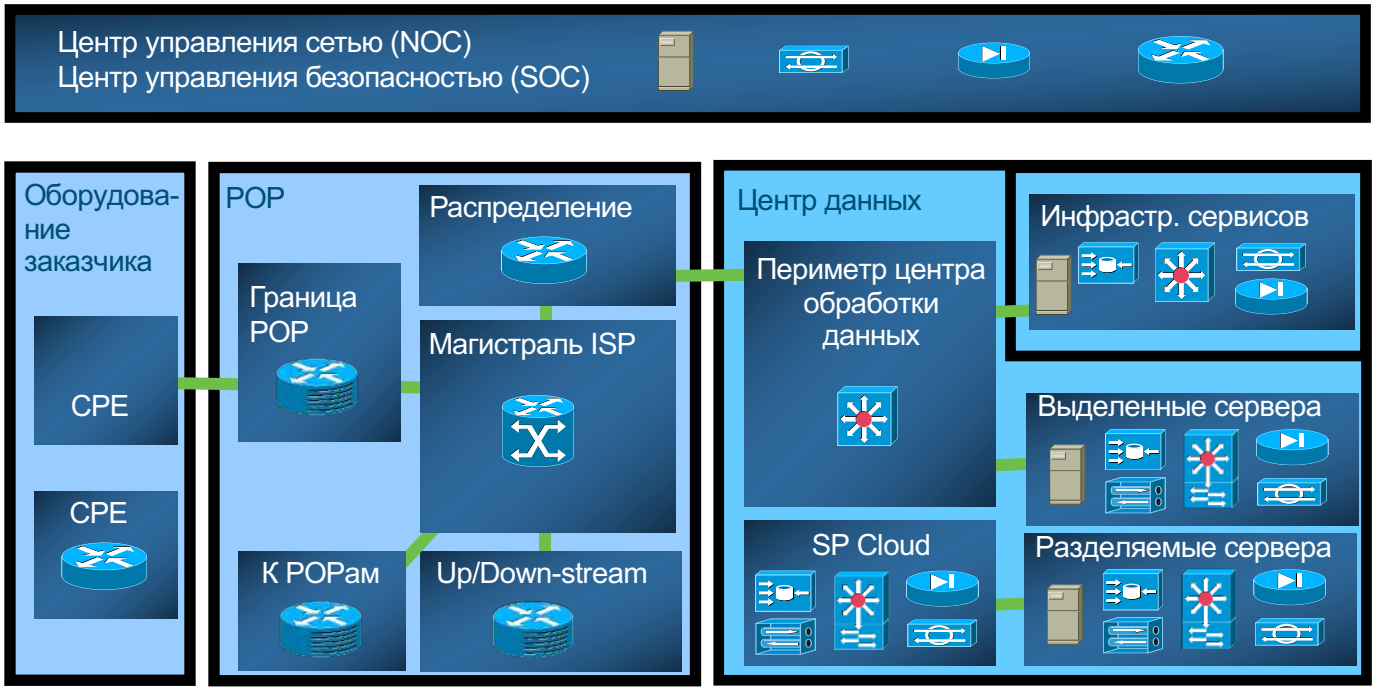

Защита инфраструктуры оператора связи, предоставляющей сервисы клиентов


Предоставление безопасности как сервиса для клиентов

# Какую железку поставить?



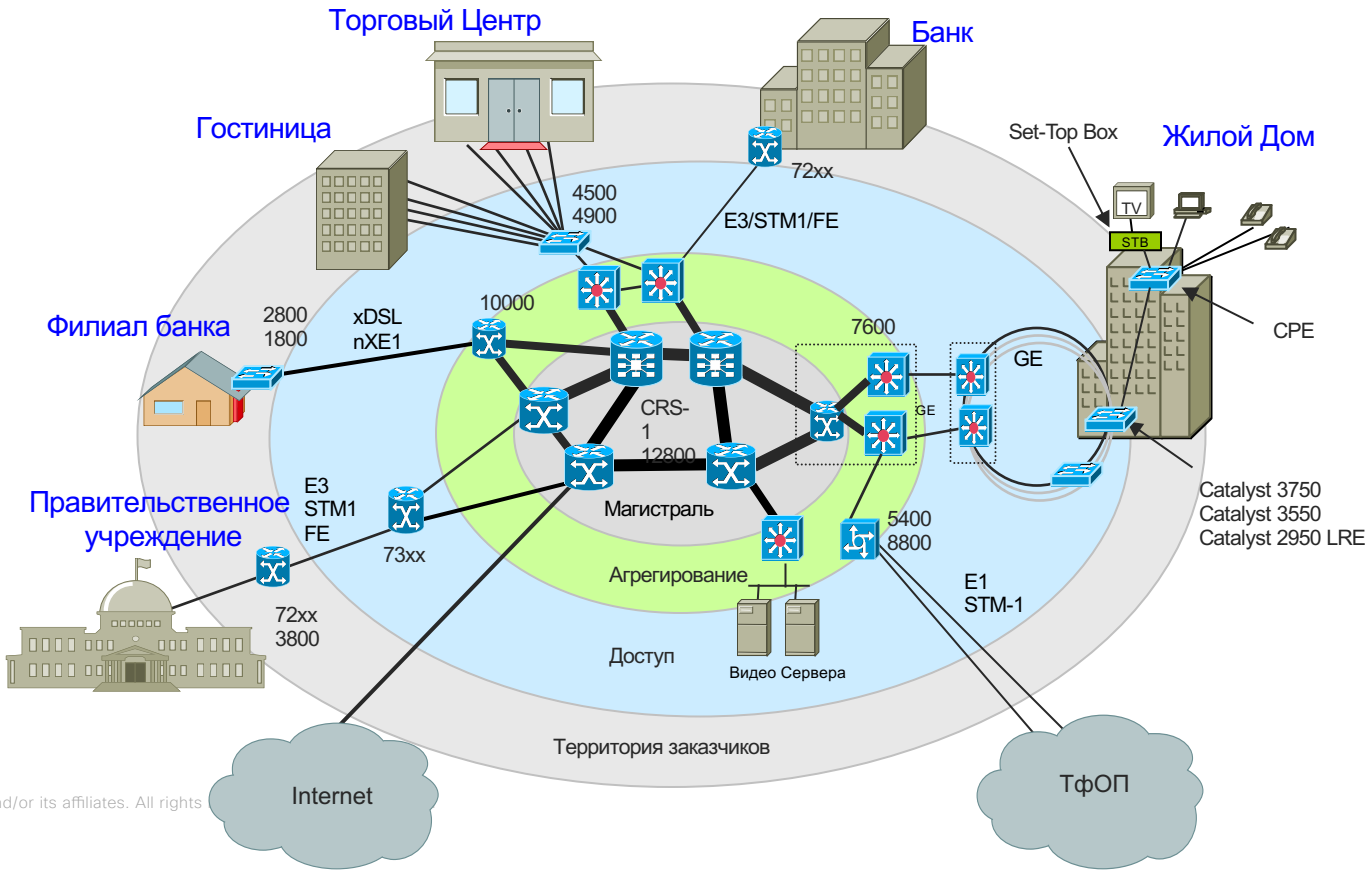
# Функциональные блоки оператора связи



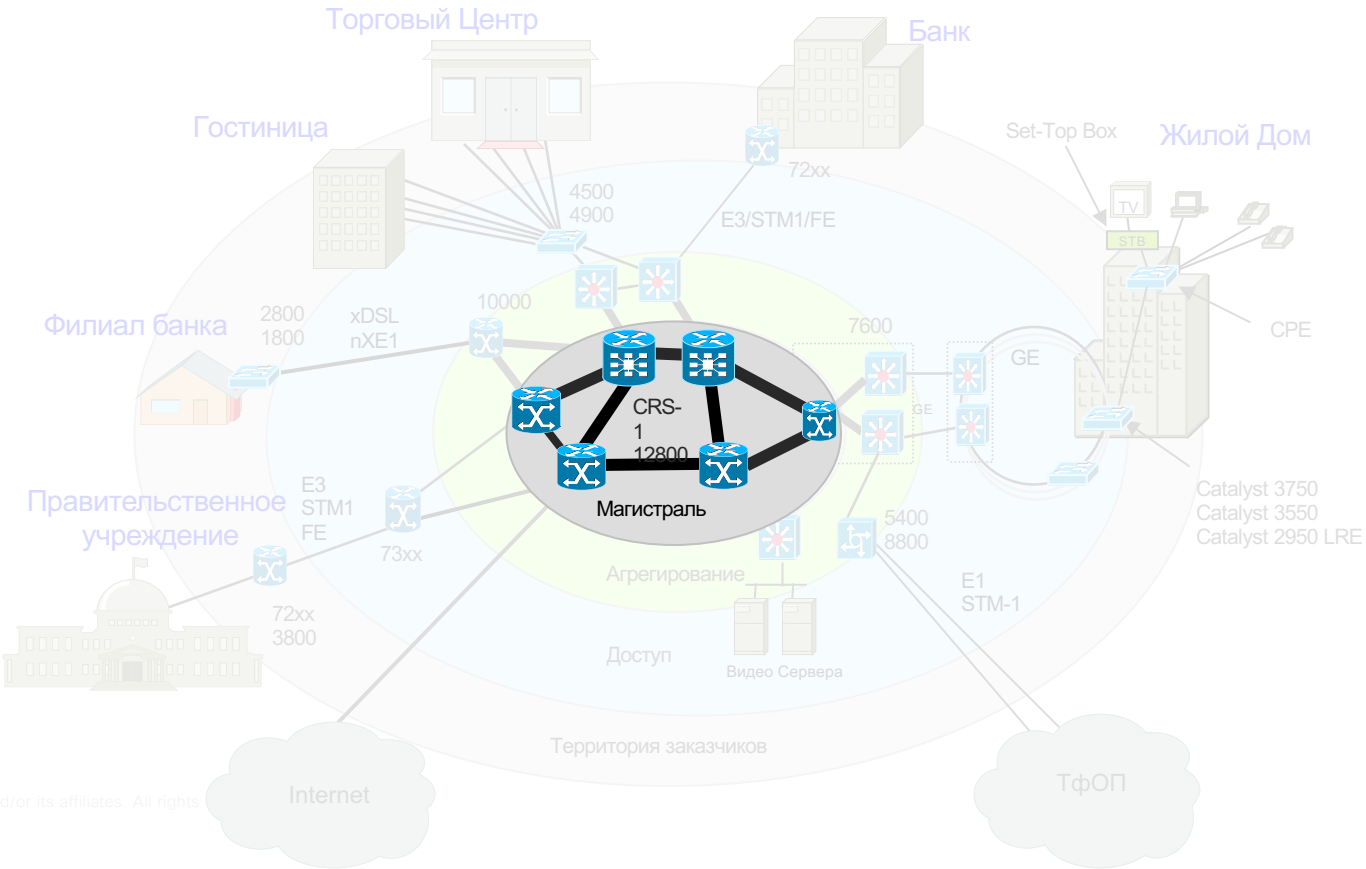
# Начинать надо не с железок

- Системный подход, в котором безопасность внедрена через всю сеть и не ограничена точечными продуктами
- Принцип эшелонированной обороны
- В первую очередь позволяет фокусироваться на критичных областях
- Облегчает реализацию политики безопасности
- Предотвращает атаки
- Более гибок и адаптивен к постоянно меняющимся угрозам

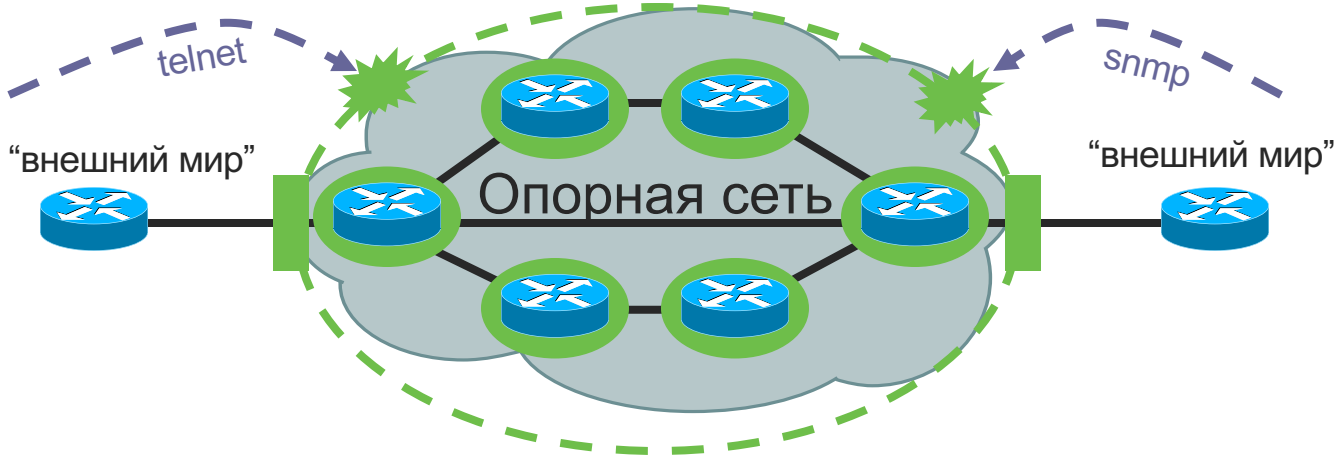
# Пакетная магистраль оператора связи



# Здесь никто не ставит железки по ИБ



# Защита хаоса приводит все равно к хаосу




- Основные маршрутизаторы защищены индивидуально “с плюсом”
- Инфраструктурная защита
- Маршрутизаторы обычно НЕ доступны извне

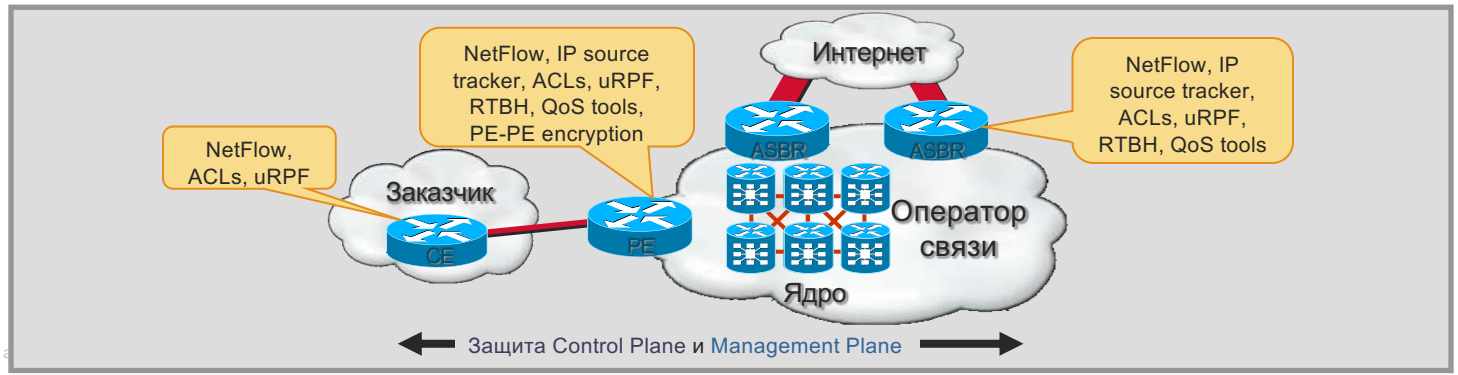
# Три золотых правила ядра оператора

- Стабильность на 100%
  - Достигается за счет резервирования элементов и связей
- «Невидимость» для атак
  - Правильный дизайн сети
- Выдерживание DoS-атак
  - Защитные механизмы операционной системы сетевого устройства
  - Специализированные решения в случае необходимости

# Network Foundation Protection

Защита инфраструктуры

| | |
|---|---|
| Data Plane | • **Обнаружение аномалий и реагирование в реальном времени**<br>• **Технологии: NetFlow, IP source tracker, ACLs, uRPF, RTBH, QoS tools** |
| Control Plane | • **Эшелонированная защита для протоколов маршрутизации**<br>• **Технологии: Receive ACLs, control plane policing, routing protection** |
| Management Plane | • **Защита и защищенное управление сетевой ОС**<br>• **Технологии: CPU and memory thresholding, dual export syslog, encrypted access, SNMPv3, security audit** |



# Списки контроля доступа


- На периметре: “deny ip any <адреса ядра>”
  - За исключением, например, протоколов маршрутизации
- Идея: Нет трафика в ядро → нет атак
- Предотвращение атак на 100%
- DoS: Очень сложно реализовать, только с транзитным трафиком

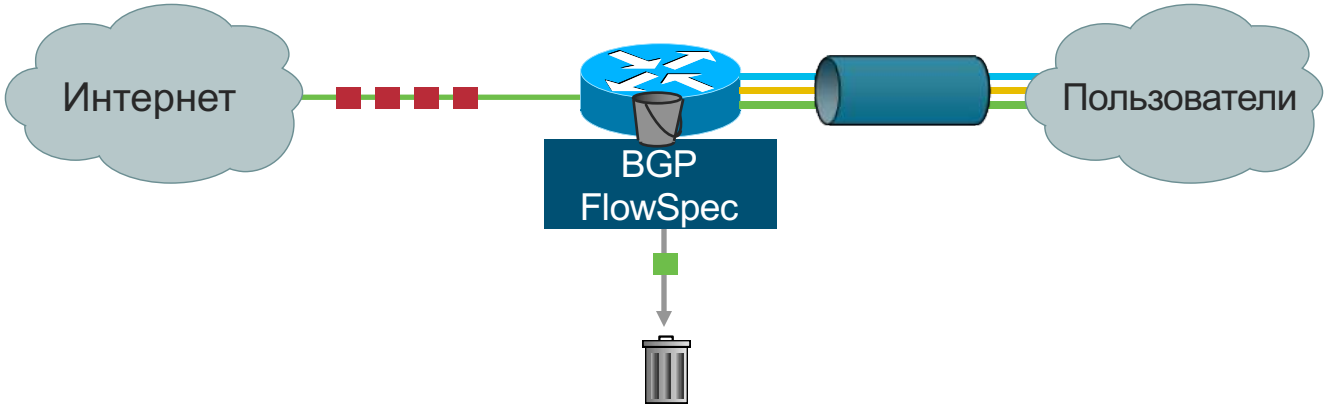
# Инфраструктурные ACL

- Инфраструктурные ACL разрешают работу только необходимых протоколов и запрещают ВСЕ остальные в рамках пространства инфраструктуры
- ACL также должны осуществлять фильтрацию несуществующих адресов
  - Фильтрация пакетов Вашего пространства от внешних источников (соседей и клиентов)
  - Фильтрация пакетов согласно RFC 1918
  - Фильтрация пакетов из групповых источников (224/4)
  - RFC3330 определяет специально используемые адреса IPv4

# Однонаправленная проверка передачи по обратному маршруту (uRPF)

- Unicast Reverse Path Forwarding
- Проверяется источник входящих IP пакетов для того, чтобы быть уверенным в том, что маршрут обратно к источнику является “действующим”
- Позволяет «отсечь» подмену адресов как из внешних сетей, так и во внутренних сетях
- 95% всех DoS-атак использует подмену адресов

# Отражение атак с помощью BGP FlowSpec

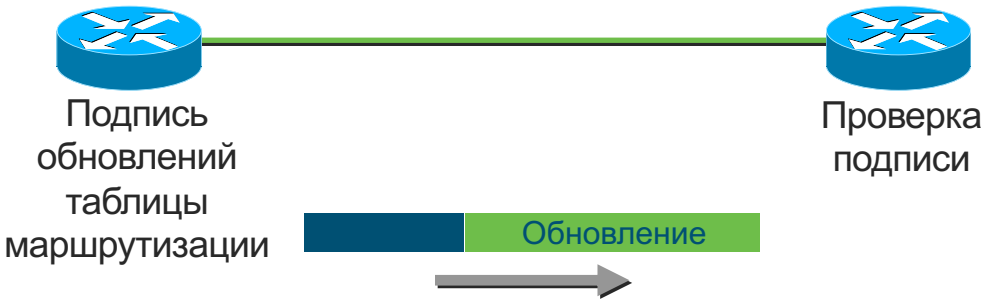



- Ограничение полосы пропускания и (или) сброс трафика;
- Перенаправление на заданный адрес следующего перехода IPv4/IPv6 или на другой VRF
- Очень полезно для защиты от DDoS-атак:  BGP FS может быть включено или выключено на каждом интерфейсе отдельно

# Защита протоколов маршрутизации

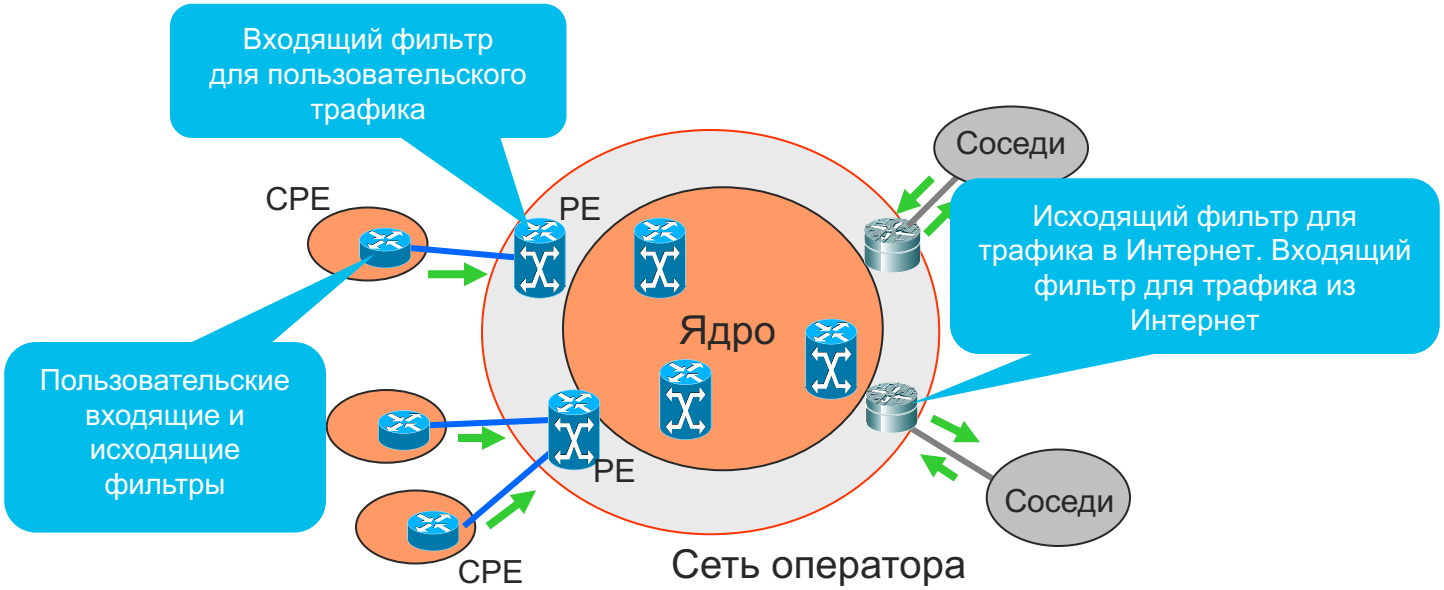
- Динамическая маршрутизация может быть нарушена
  - Отказ в обслуживании (Denial of service)
  - Фальшивые маршруты
  - Смена маршрута
  - И т.д....

# Защищенная маршрутизация




Проверяет аутентичность соседа и целостность обновления таблицы маршрутизации

# Контроль обновлений маршрутов




Фильтры трафика заказчиков и фильтры трафика соседям и от них для защиты маршрутизации

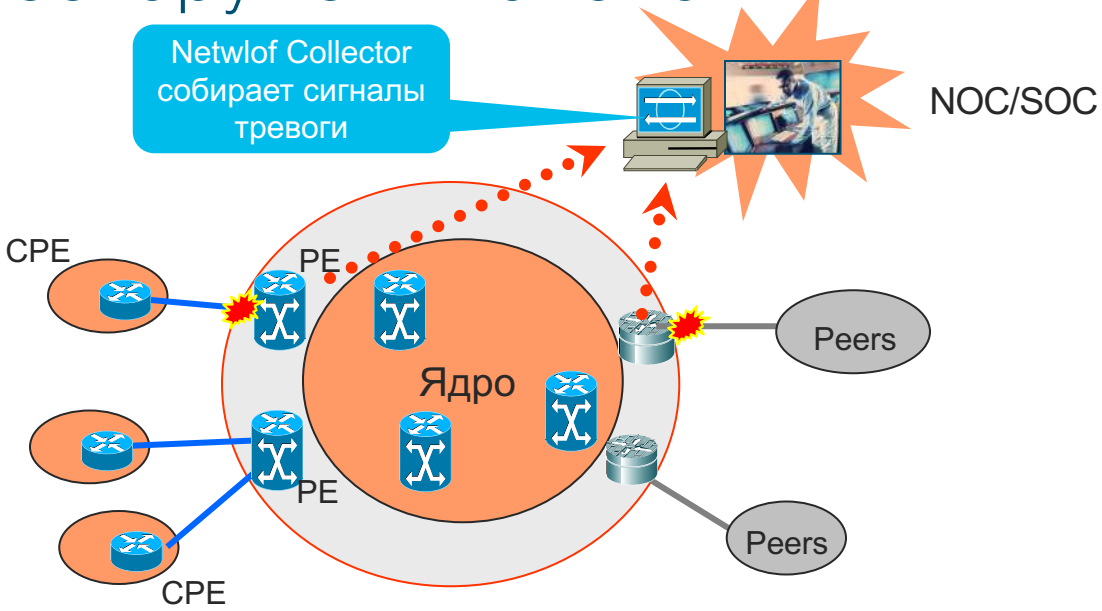
# Фильтрация в «черную дыру»

- Blackhole Filtering либо Blackhole Routing (фильтрация либо маршрутизация в «черную дыру») направляет пакет в т.н. bit bucket («корзину») маршрутизатора
  - Другое название “route to Null0” (маршрут «в никуда»)
- Работает по адресу назначения, так как представляет собой часть логики передачи
- Микросхемы пересылки предназначены для работы с маршрутами к Null0 – сброс пакета происходит с минимальным (либо полностью отсутствующим) эффектом
- Давно используется как средство уничтожения нежелательных пакетов

# Использование удаленно включаемых «черных дыр»

- Remote Triggered Black Hole
- Используется ли это сейчас?
  - Да!  Многие операторы сязи и большое количество предприятий все чаще используют эту технологию
- Часто является единственным действенным средством противостояния массированным атакам DoS
  - Высокая эффективность гарантирована
- Внешние, по отношению к автономной системе, «сигнальные» маршрутизаторы не применяются
  - Зависит от обмена информацией
- Услуга: включение пользователем
  - Конечные пользователи имеют возможность проводить процедуру сами, не привлекая SP

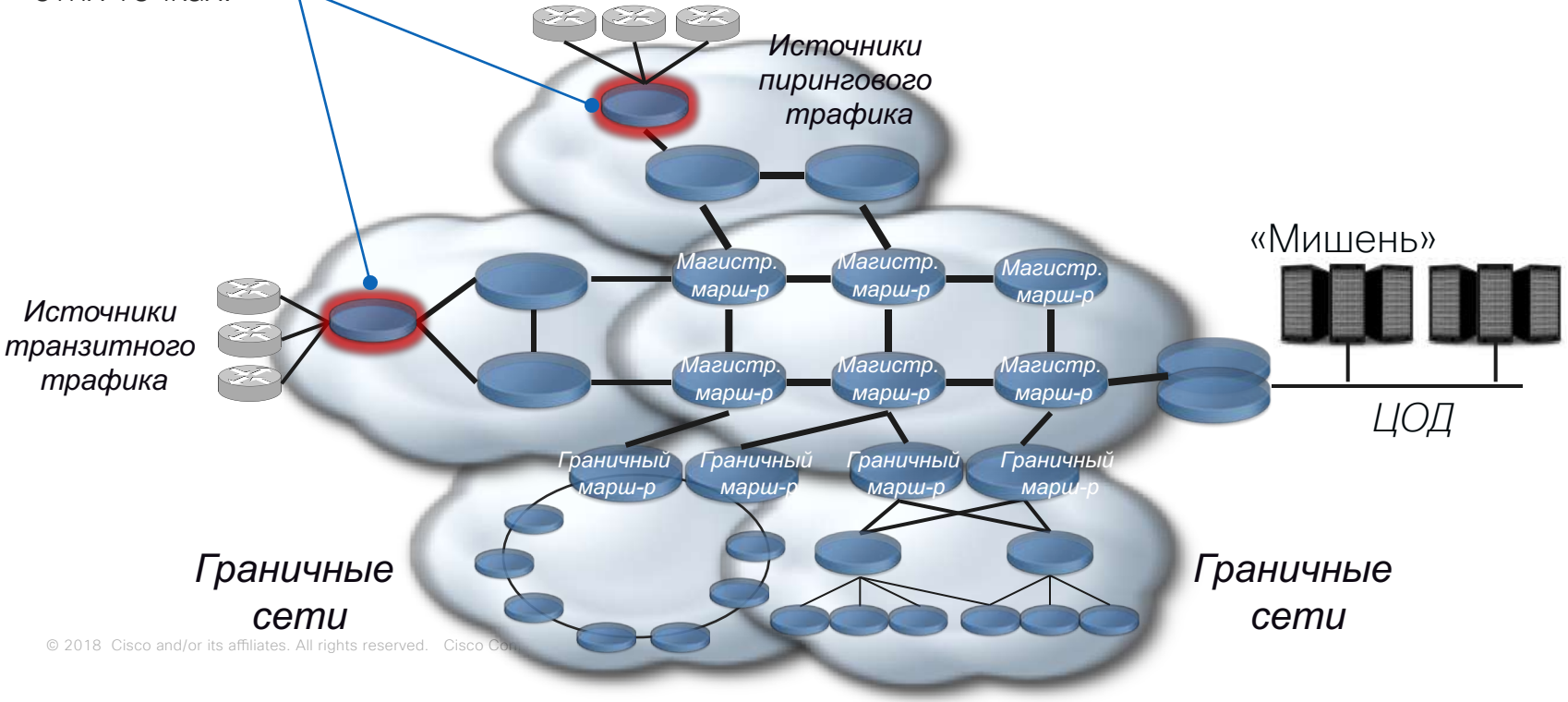
# Netflow для обнаружения аномалий




Системы обнаружения атак на базе Netflow (например, Cisco Stealthwatch) ищут следы несанкционированной активности в сети на базе уже существующей инфраструктуры

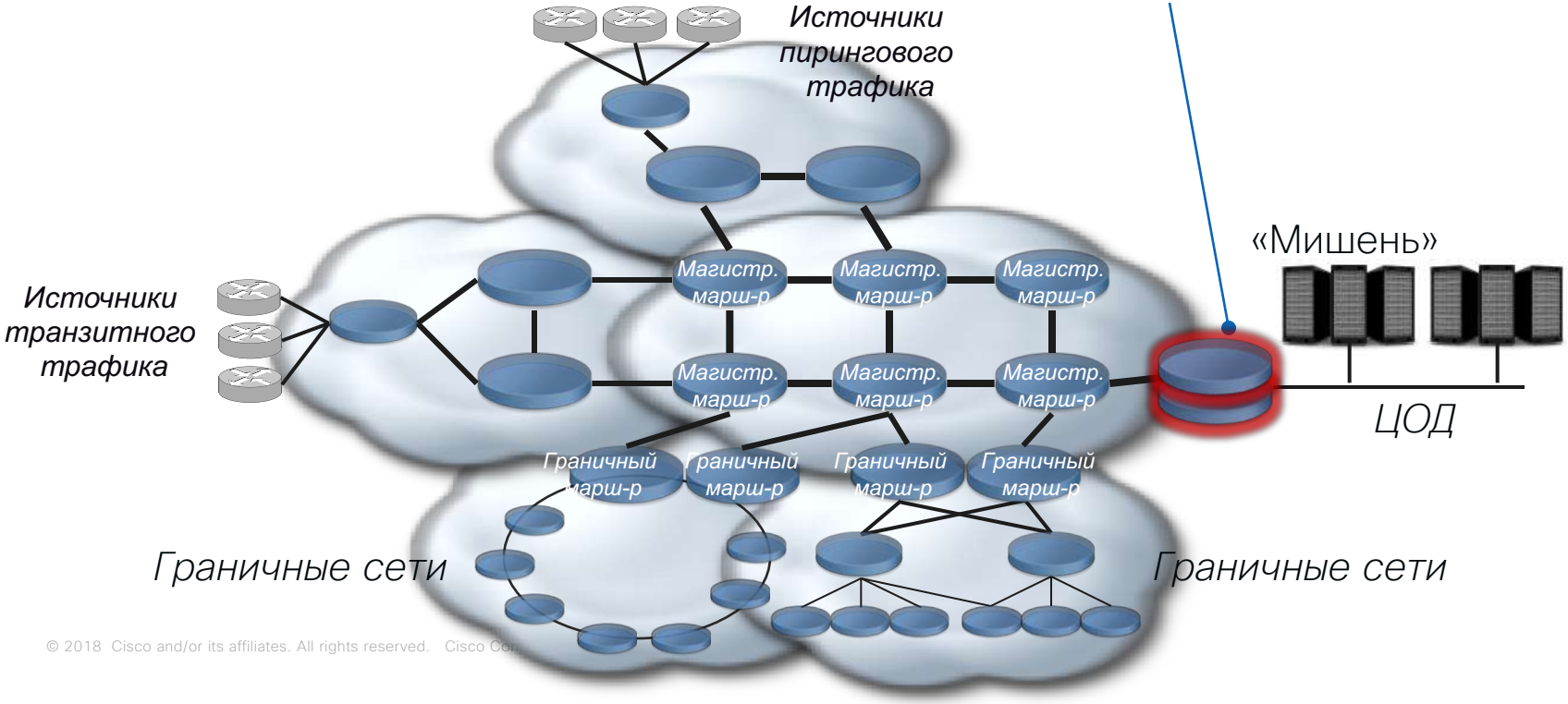
# Где использовать Netflow?

Подавляющее большинство DDoS-атак из интернета осуществляются через источники транзитного и пирингового трафиков. В первую очередь выборка пакетов должна проводиться в этих точках.



# Где использовать Netflow?

Чтобы обнаружить внутренние атаки из граничных сетей, нельзя включать NFv9 на всех граничных маршрутизаторах; и лучше осуществлять мониторинг устройств ближе к сервисной инфраструктуре (ЦОД).

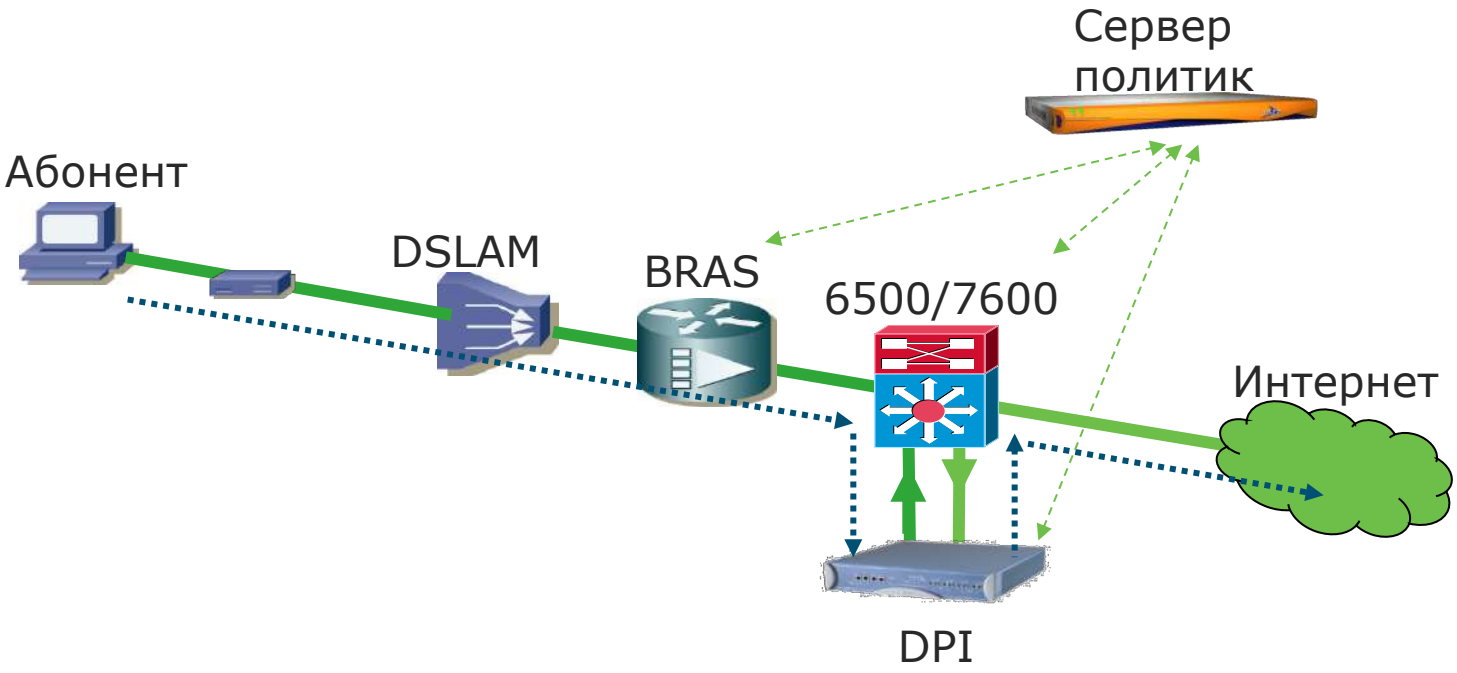


# Где использовать Netflow?

Если в сети слишком много источников и маршрутизаторов пирингового или транзитного трафика, то можно сократить область проверки и осуществлять мониторинг только магистральных маршрутизаторов.

# А что еще нужно оператору связи?

# DPI, COPM и другие регуляторные хотелки



# А нужен ли МСЭ?

# Безопасность может быть встроенной или наложенной

## Use Case

Пакетное ядро

Mobile Access Edge

Partner Edge

Internet Edge

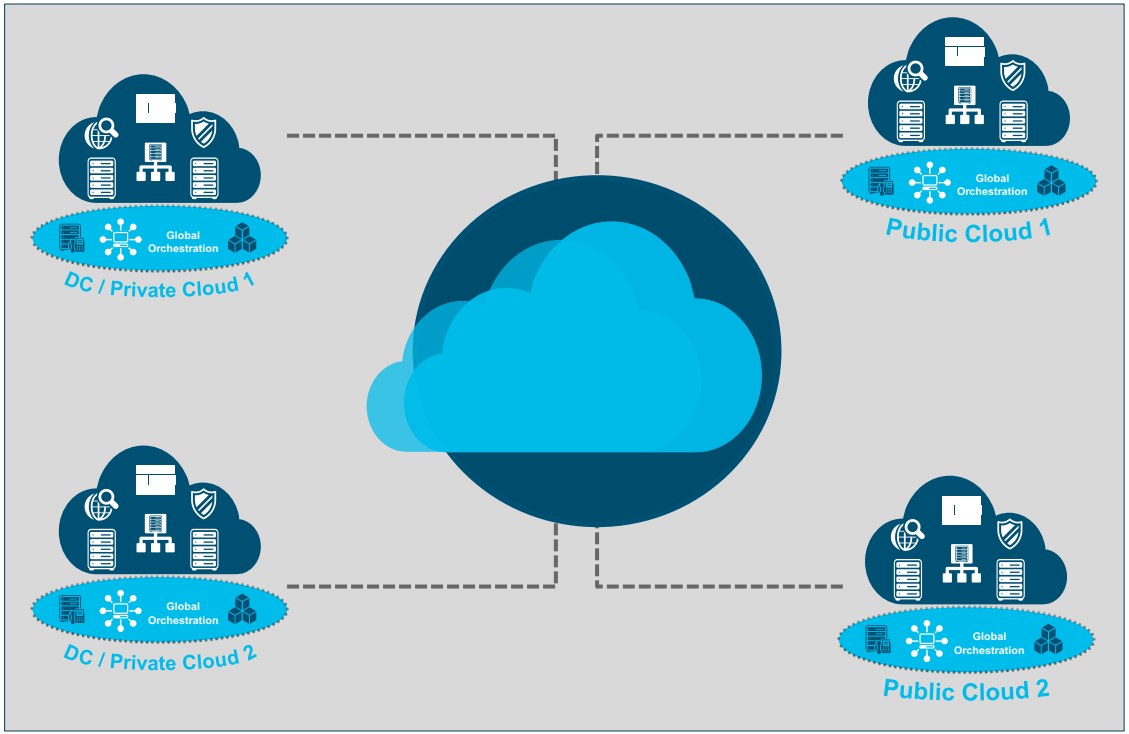

## Требования к железу

- Высокопроизводительный FW
- Высокая плотность портов, 100Gbps
- Энергоэффективность

## Требования к ПО

- Mobile Access: строгая аутентификация, авторизация (IKE v1/V2 & PKI protocols); конфиденциальность с IPSec ESP; LTE S1 FW (GTP, S1-SP FW)
- Partner Edge: GTP, NAT
- Internet Edge: FW, NAT, IPS, фильтрация контента

# ЦОДы




## Требования

- Масштибируемость: производительность
- Мультиконтекстность
- Сегментация: Internal/External
- Трафик Север-Юг, Запад-Восток
- Многовендорная оркестрация

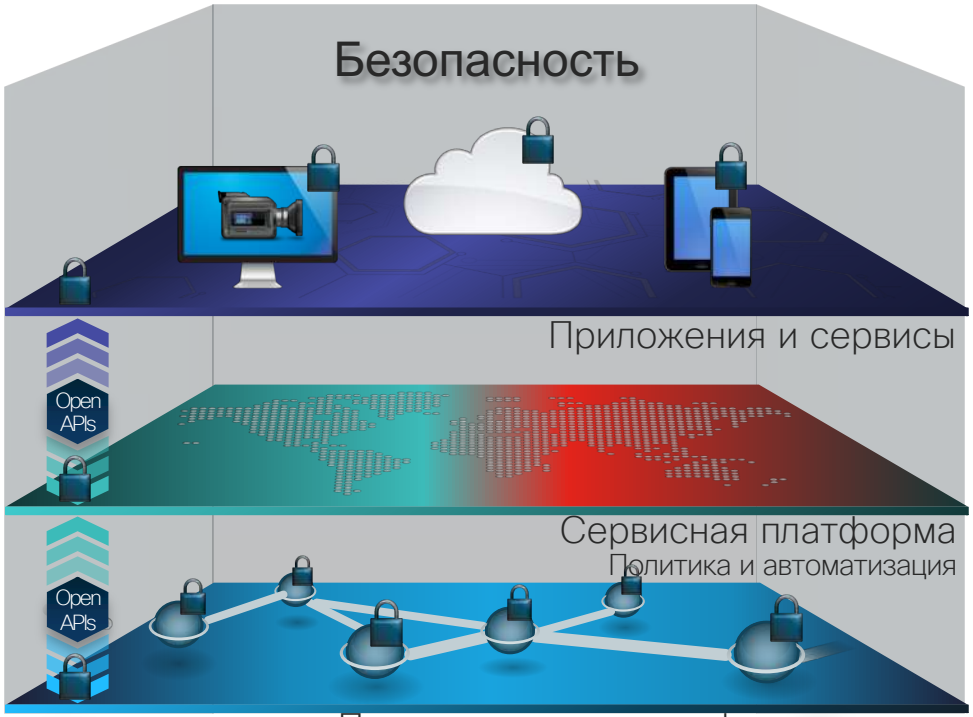
## Преимущества

- Высокая производительность
- Интеграция с сетью: Маршрутизация, коммутация
- Высокая плотность: 40G/100G
- Кластеризация: Intra-chassis, Inter-chassis, Inter-site
- Разгрузка потоков
- Управление на базе политик

# Могут понадобиться платформы ИБ нового поколения

| | | | |
|---|---|---|---|
| Модульные вычисления | Аппаратные компоненты системы могут легко модернизироваться | Динамическое предоставление сервисов | Динамическое управление цепочкой сервисов и добавление новых по мере необходимости |
| Архитектурное масштабирование | Базируется на множестве передовых технологий (x86 и ARM, шифрование и сетевые процессоры, спец. микросхемы, кластеризация) | Управление сервисами «на лету» | Сервисы могут быть добавлены, удалены, или изменены без нарушения обслуживания существующих потоков данных |
| Отсутствие единой точки отказа | Специальное программное и аппаратное обеспечение. Сервисы работают в независимых контейнерах, и не затрагивают другие сервисы | Интеграция решений 3-их компаний | Архитектура позволяет быстро добавлять новые сервисы, необходимые заказчикам |
| Независимость от вариантов внедрения | Одинаковый набор возможностей как в физической, так и в виртуальной среде, включая поддержка SDN. | Унифицированное управление политиками и лицензиями | Использует унифицированные прикладные интерфейсы и интерфейсы управления для всех сервисов, включая политики и лицензирование |

# Операторы предъявляют новые требования к ИБ-решениям не в области ИБ




- Пользовательские и системные приложения
- Доставка новых сервисов (B2B/B2C)

- Открытые, основанные на страндартах
- Автоматизация и оркестрация
- Интеграция с вендорами VNF

- Вычисления, хранения, сеть
- Сетевое ядро, облака и мобильный доступ