ЦЕНТР
ПРИКЛАДНЫХ
ИССЛЕДОВАНИЙ
КОМПЬЮТЕРНЫХ
СЕТЕЙ

# Применение технологий SDN/NFV в сетях современного предприятия

С.Монин

06/10/15

# План

1. Предпосылки применения SDN/NFV в сетях предприятия

    1.1 Недостатки традиционных сетей

    1.2 Преимущества SDN

    1.3 Преимущества NFV

    1.4 Синергия SDN и NFV

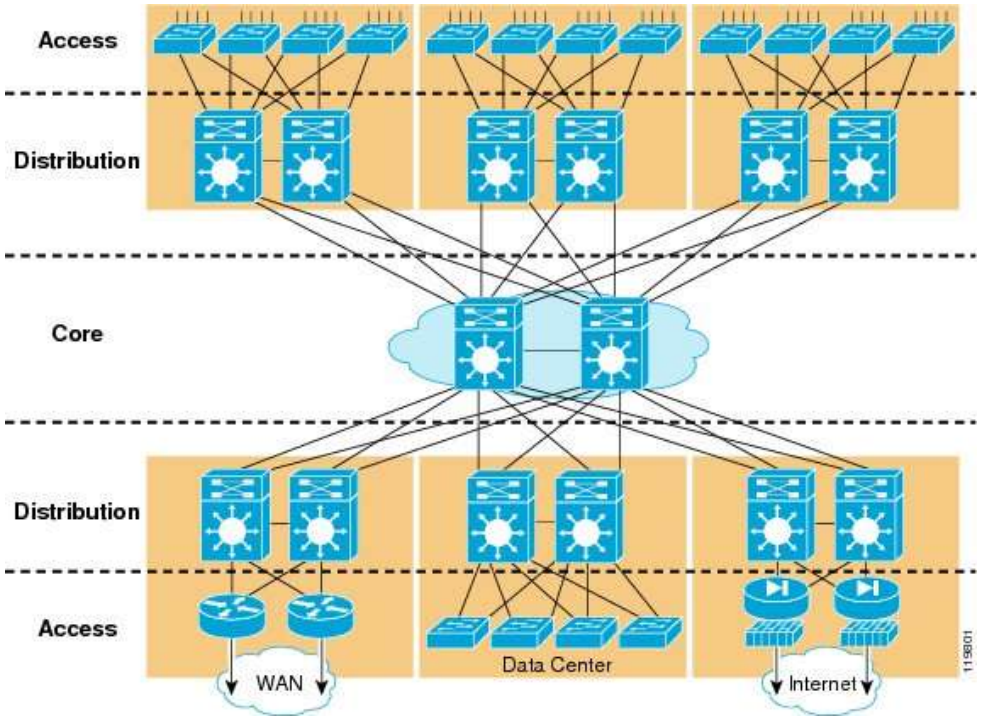
2. Особенности новых технологий

3. Выводы

ПКС сети

# Предпосылки применения SDN/NFV в сетях предприятия

## Чем плохи/хороши традиционные сети предприятия ?




### Минусы:

- Количество протоколов, требующих настройки - несколько десятков !
- Поддержка протоколов разными вендороми – сильно отличается.
- Vendor Lock – большие расходы CapEX.
- Требуются отдельные устройства для обеспечения сетевых функций (FW, NAT..)
- Проблема наличия квалифицированного персонала, проблема OpEX.
- Сложно внедрить новые решения без одобрения вендора.
- Централизованное управление не оперативно.
- Так или иначе – настраивать нужно все.
- Кто определяет политику движения трафика?

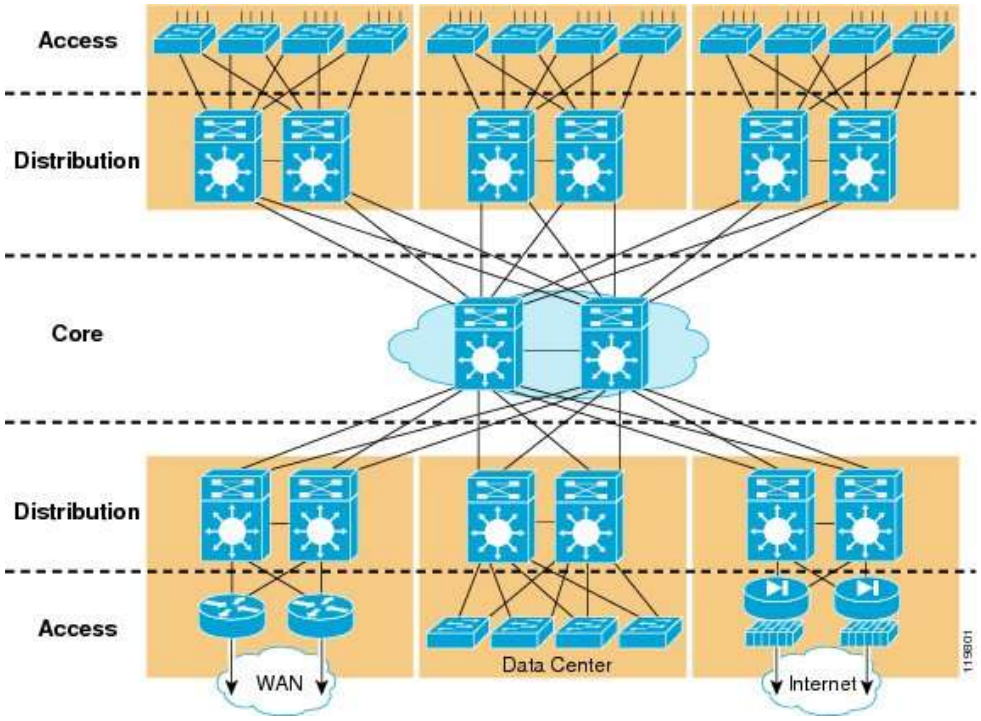
### Плюсы:

- Они уже есть и работают сейчас

Почему для ЦОД, SP уже все есть…

# Предпосылки применения SDN/NFV в сетях предприятия

Чем плохи/хороши традиционные сети предприятия ?




Перечисленные проблемы ранее пытались решить

- SNMP
- CAPWAP
- NetConf
- Telnet, SSH
- и др.

Нерешаемая проблема:
Распределенный Control Plane с разными возможностями.

# Организация сети крупной компании с территориально распределенной структурой на основе SDN решений от ЦПИКС

**ЗАДАЧА:**

Модернизируемый сегмент охватывает один крупный региональный офис (300 сетевых портов) и четыре филиала (по 50 портов) в каждом.
Проложенная СКС обеспечивает скорость каналов 1 Гбит/с для подключения рабочих мест (90% подключений) и 10 Гбит/с (10% подключений) для подключения серверов и передачи данных в ядре ЛВС.
Связь между удаленными офисами осуществляется через Интернет по VPN, канал подключения каждого офиса к Интернету – 1 Гбит/с.

**Контроллер SDN.** Контроллер должен представлять собой отказоустойчивую систему, желательно с территориальным разделением резервирующих устройств.
**Коммутаторы**. Заказчик просит Поставщика рассмотреть возможность использования в проекте коммутаторов без предустановленной ОС .
**Функционал.** Заказчик рассчитывает, что решения SDN позволят ему автоматизировать следующие процедуры:

- Управление списками контроля доступа на сетевых устройствах
- Блокировка определенных приложений, пользователей и их групп в соответствии с установленными политиками безопасности
- Настройка алгоритмов приоритизации и обеспечения качества обслуживания (QoS)
- Настройку новых сетевых устройств

# Преимущества SDN

Из коммутаторов/маршрутизаторов весь интеллект перемещается в контроллер.

1. Теперь сетевое устройство может стать проще/дешевле.
Функции ПКС коммутатора сводятся к следующему:

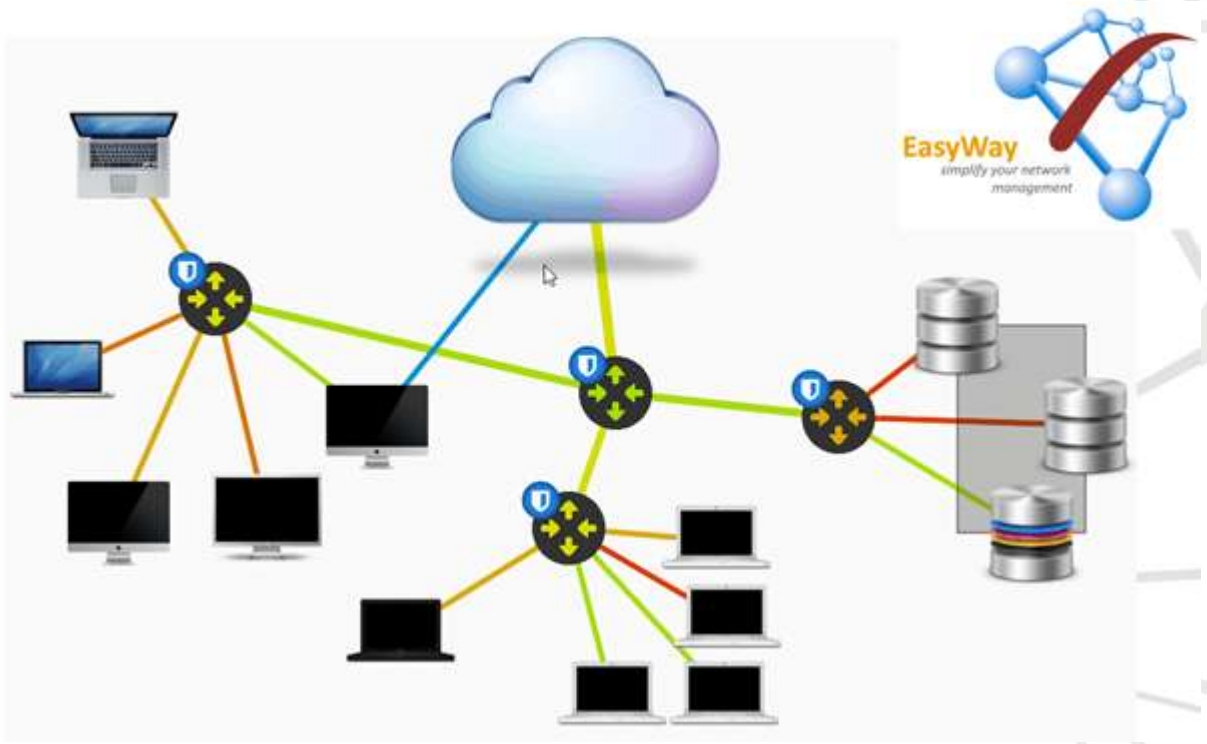
- Хранить таблицу правил, присланных контроллером
- Проверять входящий трафик и коммутировать его в соответствии с таблицей
- Собирать статистику
- Взаимодействовать с контроллером (PacketIn, PacketOut, ModFlow…),
  то есть обеспечивать поддержку **одного** протокола OpenFlow.

2. Теперь Control Plane сосредоточен в одном месте, значит можно реализовать почти все, причем динамически. (возможны «переходные» варианты Legacy+SDN)

3. Не нужны умные админы, достаточно секретаря и программиста.

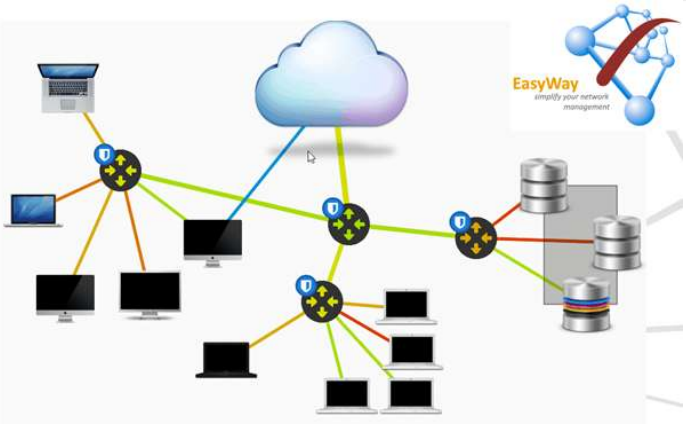
# Преимущества SDN+NFV

Сначала простой вариант: сетевые функции берет на себя приличный контроллер.




Для среднего предприятия этого может быть достаточно.

# Преимущества SDN+NFV




GUI+Средство визуализации = EasyWay

Перечень приложений для контроллера, работающего в сети предприятия:

- Приложение для сегментации сети и ограничения трафика + Поддержка QoS
- Приложение “Edge”: VPN + функции Firewall+NAT и маршрутизация с филиалами, провайдерами и партнерами, туннелирование трафика.
- Приложение AAA- работа с пользователями
- Приложение Mirror для зеркалирования трафика
- Приложение IPS для санации трафика на предмет зловредностей
- Приложение AntiDDoS для динамической блокировки бот-сетей
- Модуль интеграции с WiFi контроллерами

# Преимущества SDN+NFV

Что делать, если у вас трафик 10Gb/s требует шифрации и NAT, имеются 18 FullView BGP соседей, требуется DPI гигабитного трафика на предмет  200 сигнатур последнего вируса и при этом вы испытываете DDoS атаку ?

Тут два пути: первый - купить самые мощные middlebox вашего вендора и приготовится делать это раз в два года…

второй – купить обычный сервер…

# Преимущества SDN+NFV

Когда давно Sun Microsystems заявила: «Сеть – это компьютер»
Сегодня это действительно так!

Вопрос: Что не давало нам долгое время использовать обычные сервера с ПО, которое реализует сетевые функции  например FireWall ?

Ответ: «Медленный» сетевой стек Linux и слабые возможности недорогих, обычных процессоров в области обработки трафика.

Теперь – можно делать сетевые устройства даже операторского класса, можно сделать сетевые функции облачными, работающими по принципу гармошки…

DPDK NetMap OpenStack QEMU

# Синергия SDN и NFV

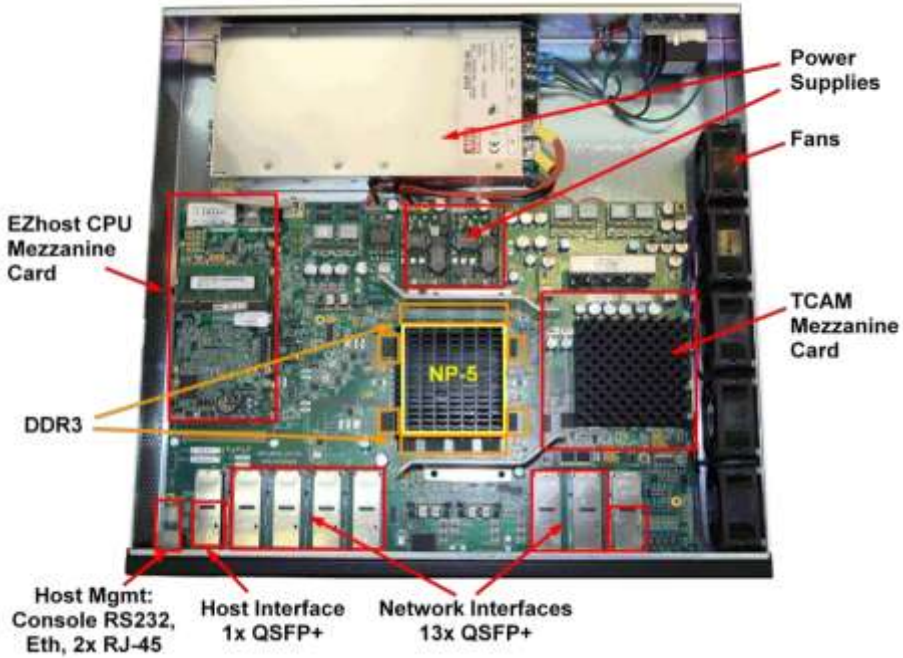
Мы встраиваем мощный сервер NFV  в инфраструктуру сети, управляемой SDN контроллером. Это позволяет управлять цепочками сервисов не только про-активно, но и реактивно, динамически.

Пример: Про-активное правило «весь трафик следующий на адреса партнера X.X.X.X должен сначала пройти шифрацию на NFV сервере».

Реактивное правило «В случае если приложение IDS на контроллере подозревает аномалию в трафике пользователя Y весь его трафик перенаправить на систему IPS NFV»

# Синергия SDN и NFV

Еще один вариант: можно использовать SDN коммутаторы с продвинутыми сетевыми процессорами. Тогда можно часть сетевых функций (Шифрация, DPI, Туннелирование, NAT…) реализовать прямо на интерфейсах, смотрящих на провайдера.

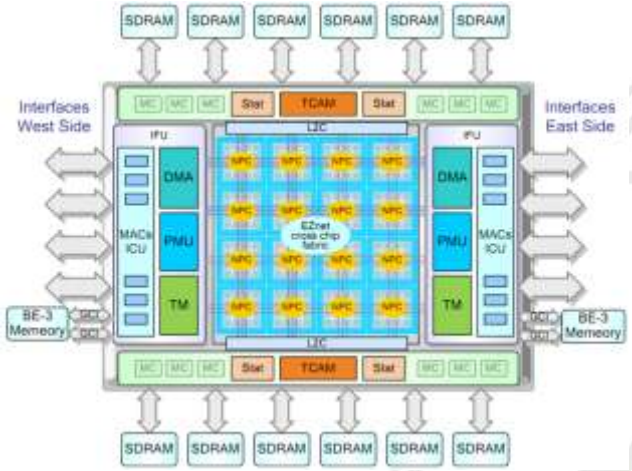




- Сетевой процессор  производительностью до 480 Гб/с, 500 миллионов пакетов в секунду
- 5-уровневая иерархическая система очередизации. Поддержка WFQ с приоритетной очередью.
- Поддержка WRED, Shaping (CIR, PIR), Per flow metering, marking, policing для миллионов потоков.
- L2-4 switching/routing. Сбор статистики по потокам, программируемые пороги. 512M счетчиков.

# Синергия SDN и NFV

Новые сетевые процессоры:




NPS-400

- Поддержка IPsec на скорости до 200 Gbps (server offload)
- DPI на скорости до 800 Gbps (application recognition)
- 200 Gbps (pattern match) с распознаванием более 1500 сигнатур. Собственные сигнатуры
- TCAM с алгоритмом расширения объема памяти за счет DRAM.
- Высокоскоростной алгоритм поиска по большому количеству записей в таблицах:
- Поддержка в Smart NFV appliance до 24GB памяти DDR4 (до 96 GB max)
- Frame size from 1B to 12KB
- Up to 64GB frame memory (for 96GB DRAM); up to 256M frames
- Shaping, WRED, per flow metering, marking, policing для миллионов потоков
- OAM processing, keepalive, watchdog,  802.1ag/CFM, state tracking, reporting.
- До 512 миллионов разнообразных счетчиков.
- До 6.4 миллиардов операций в секунду по сбору статистики.

# Синергия SDN и NFV

Апофеоз виртуализации сетевой функции: использование вместо коммутатора обычного сервера с большим количеством сетевых интерфейсов ( например 24 * 1Gb/s портов и 2 * 10Gb/s порта) и модулем для поддержки OpenFlow 1.3.x от разработчиков ЦПИКС.

Что это может дать? Всего одно устройство на филиал :)

К нему подключены компьютеры 22 сотрудников  и ТД,
Один 10Gb/s интерфейс подключен к провайдеру «А» второй- к провайдеру «В».
Все необходимые сервисы (Почта, IP-Телефония и.т.п.) работают на этом же сервере вместе с
SDN контроллером RUNOS и набором приложений.

## Продукты ЦПИКС

Runos — SDN/OpenFlow контроллер. Runos контроллер является первой отечественной сетевой операционной системой для программируемых сетей SDN. Отличительными особенностями контроллера является высокая производительность и удобство разработки .
Проект Runos находится в открытом доступе на http://arccn.github.io/runos/ под лицензией Apache 2.0. В коммерческой версии Runos контроллер обладает механизмами резервирования, масштабируемости и распределенного управления.
Active/Standby резервирование с поддержкой горячего резервирования.
Active/Active резервирование с возможностью балансировки нагрузки.
Распределенная версия контроллера для управления большими сегментами сетей.

Runos обладает следующими характеристиками производительности:

Пропускная способность: 8 000 000 событий в секунду.

Задержка на обработку одного запроса: 30мкс.

…подробности в отдельном докладе.

## Продукты ЦПИКС

Приложение SDEnterprise для Runos контроллера по управлению распределенной корпоративной сетью.

VPN — взаимодействие с VPN сервисом: потоки с заданными характеристиками перенаправляются до VPN сервиса и от VPN сервиса в сторону получателя, взаимодействие с VPN сервисом через Rest интерфейс (настройка, сбор статистики).

ACL — управление списками контроля доступа, какие группы и пользователя куда имеют доступ, высокоуровневые политики переводятся в правила на сетевых устройствах по всей сети.

Firewall — взаимодействие с Firewall/DPI сервисами: перенаправление подозрительных потоков на систему безопасности, получение информации о наличии вредоносной активности, блокирование потока на граничном порту, взаимодействие с системой безопасности происходит по Rest интерфейсу.

Edge-service — взаимодействие с Интернет провайдером (BGP, MPLS).

AAA — локальная (в пределах порта) аутентификации пользователя с установкой на всю сеть правил, согласно политики для этого пользователя.

## Продукты ЦПИКС

OpenFlow коммутаторы ЦПИКС.
ЦПИКС предлагает несколько линеек коммутаторов на базе доступного аппаратного обеспечения. Разработанное для них ПО можно получить отдельно и установить на устройства самостоятельно.

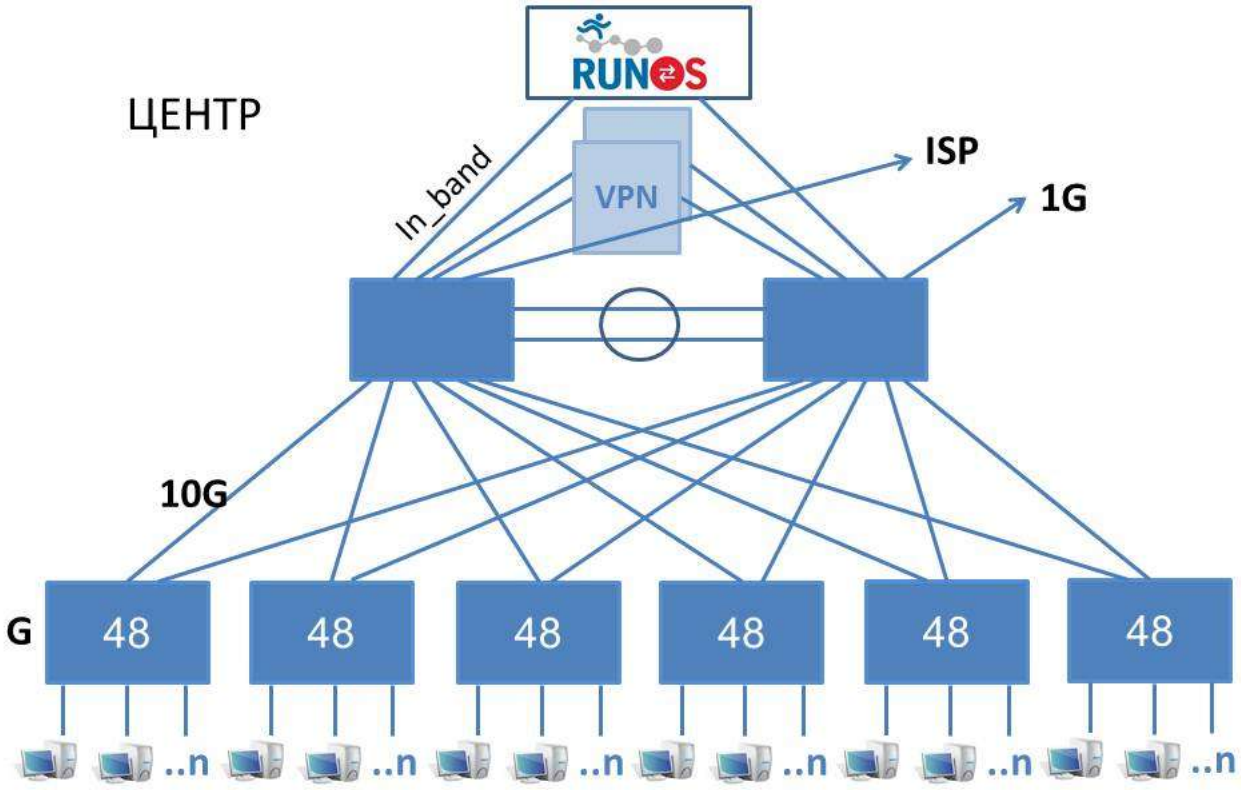
- На основе white box коммутаторов.

На коммутаторы установливается Open Networking Linux  с разработанным в ЦПИКС OpenFlow 1.3 агентом. Поддерживается до 48 1GE (+4x10Ge) портов.

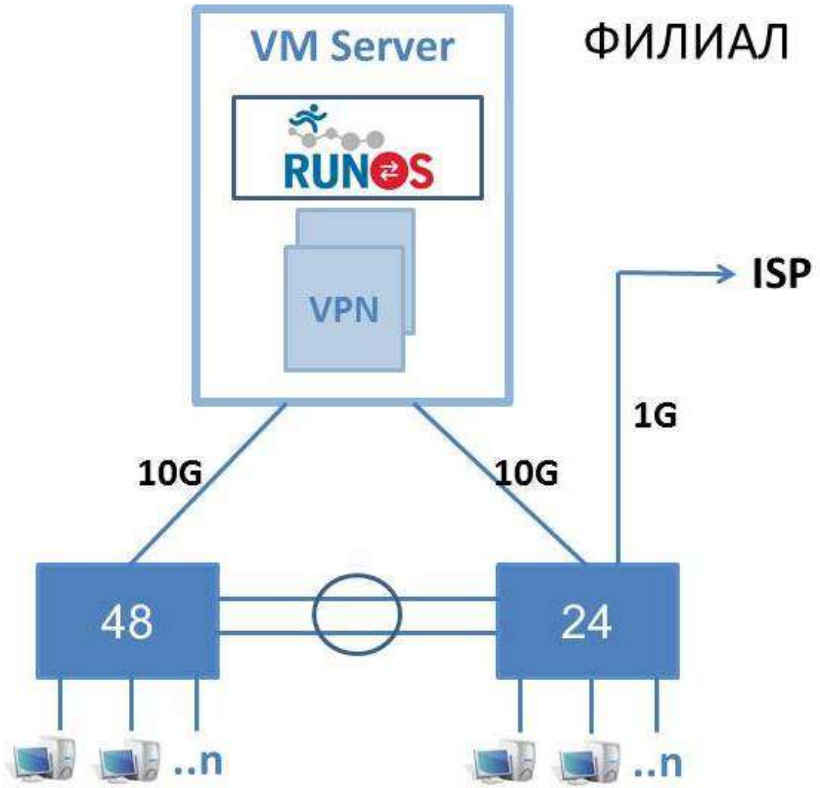
- На основе x86 серверов. Поддерживается до 24x 1GE, до 12x 10Gbps портов с суммарной гарантированной пропускной способностью на устройство в 60Gbps.Важным отличием коммутатров на x86 серверах от white box коммутаторов является полная поддержка возможностей протокола OpenFlow 1.3. (перезапись IP заголовков)

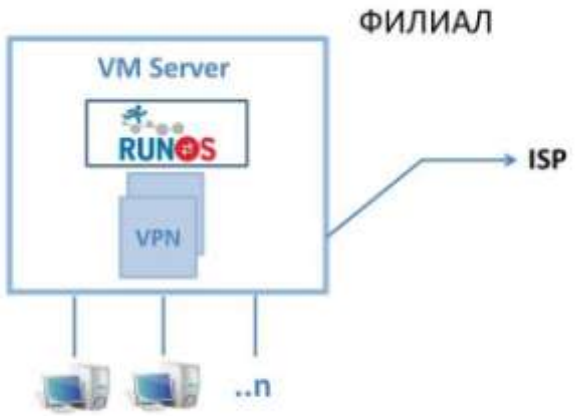
- Собственная разработка на основе NP-5

# Организация сети крупной компании с территориально распределенной структурой на основе SDN решений от ЦПИКС



# Организация сети крупной компании с территориально распределенной структурой на основе SDN решений от ЦПИКС



# Вопросы ?