Cisco Expo 2011

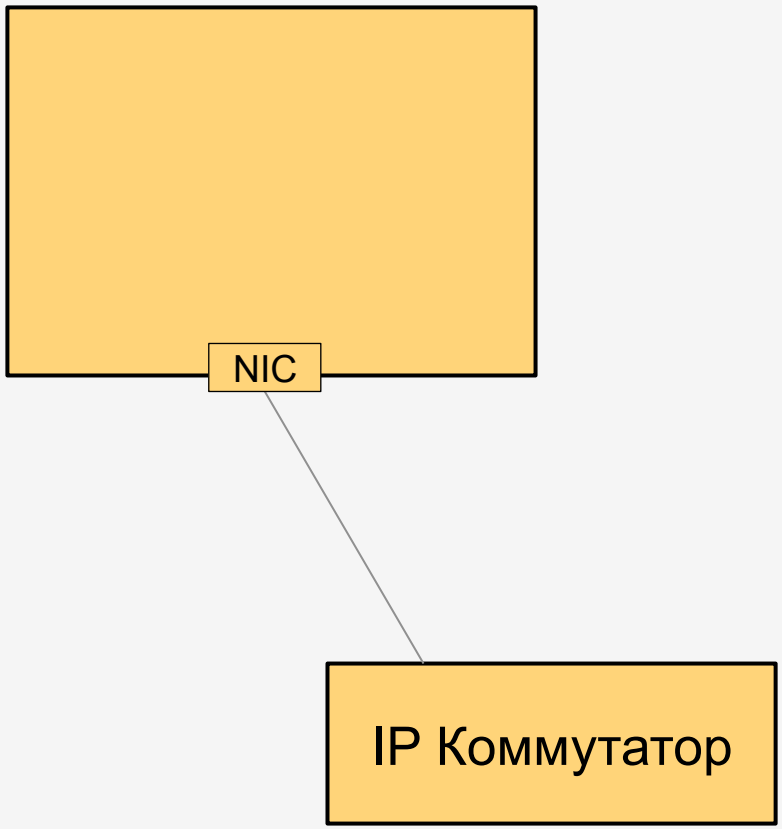
# Виртуализация ввода-вывода в конвергентной среде:

# Nexus 1000V
# Virtual services
# Cisco Virtualization Adapter

Виктор Подкорытов
инженер-консультант Cisco
vpodkory@cisco.com
+380 44 3913600

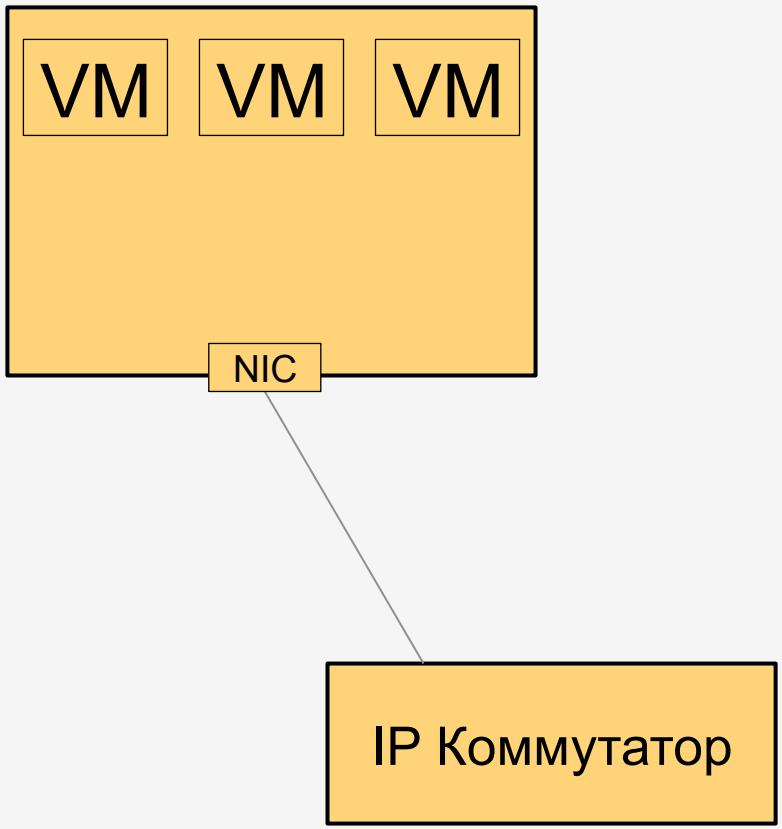
innovate together

# Де-эволюция подключения сервера




Полная
Видимость
Сервера

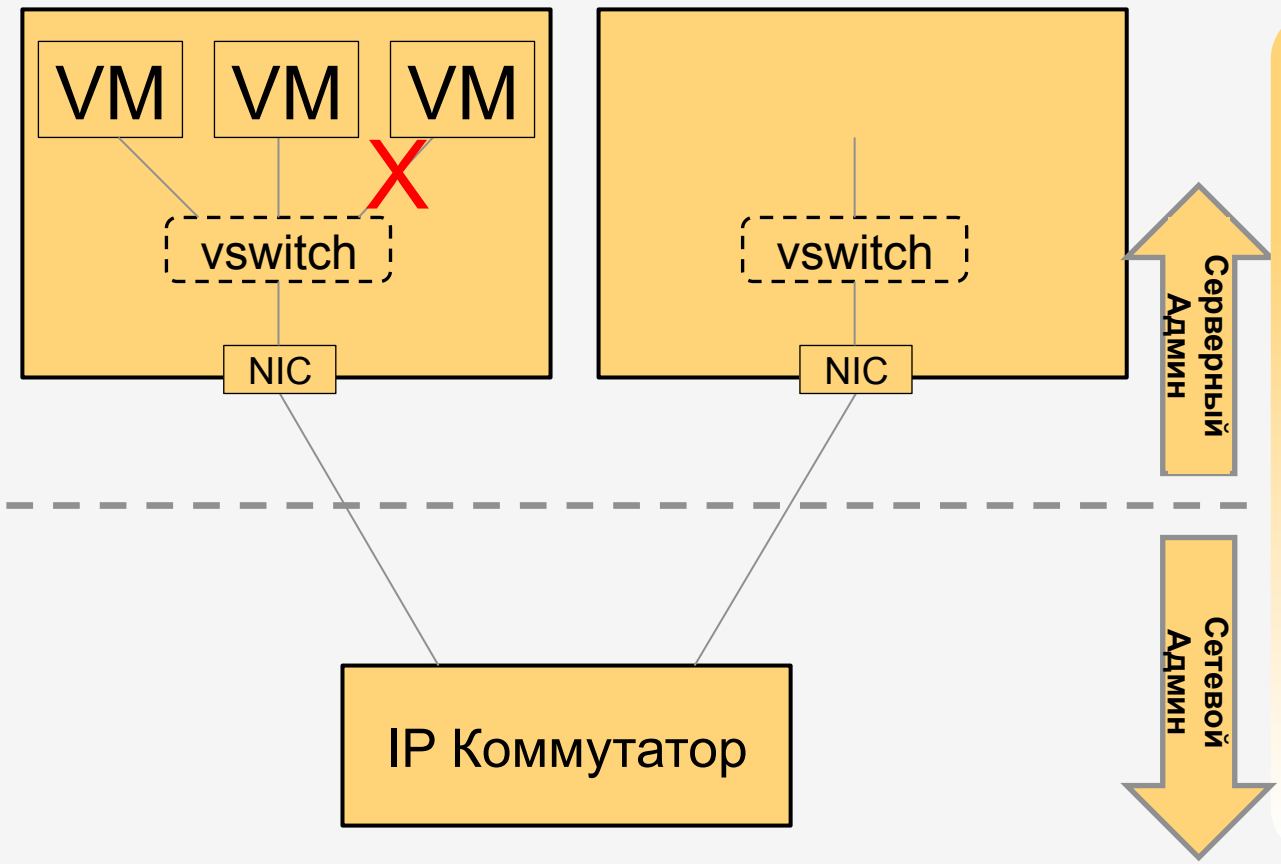
# Виртуализованный Сервер




**Виртуализованный Сервер**

- Подключается транком
- Нет видимости трафика индивидуальных VM
- Не возможно обнаружить и устранить проблемы
- Применить политики безопасности

# Виртуальный Коммутатор




## Виртуальная Коммутация

### Нет политик

• Функциональность QoS, Security, и управление политиками не доступны в стандартном vswitch

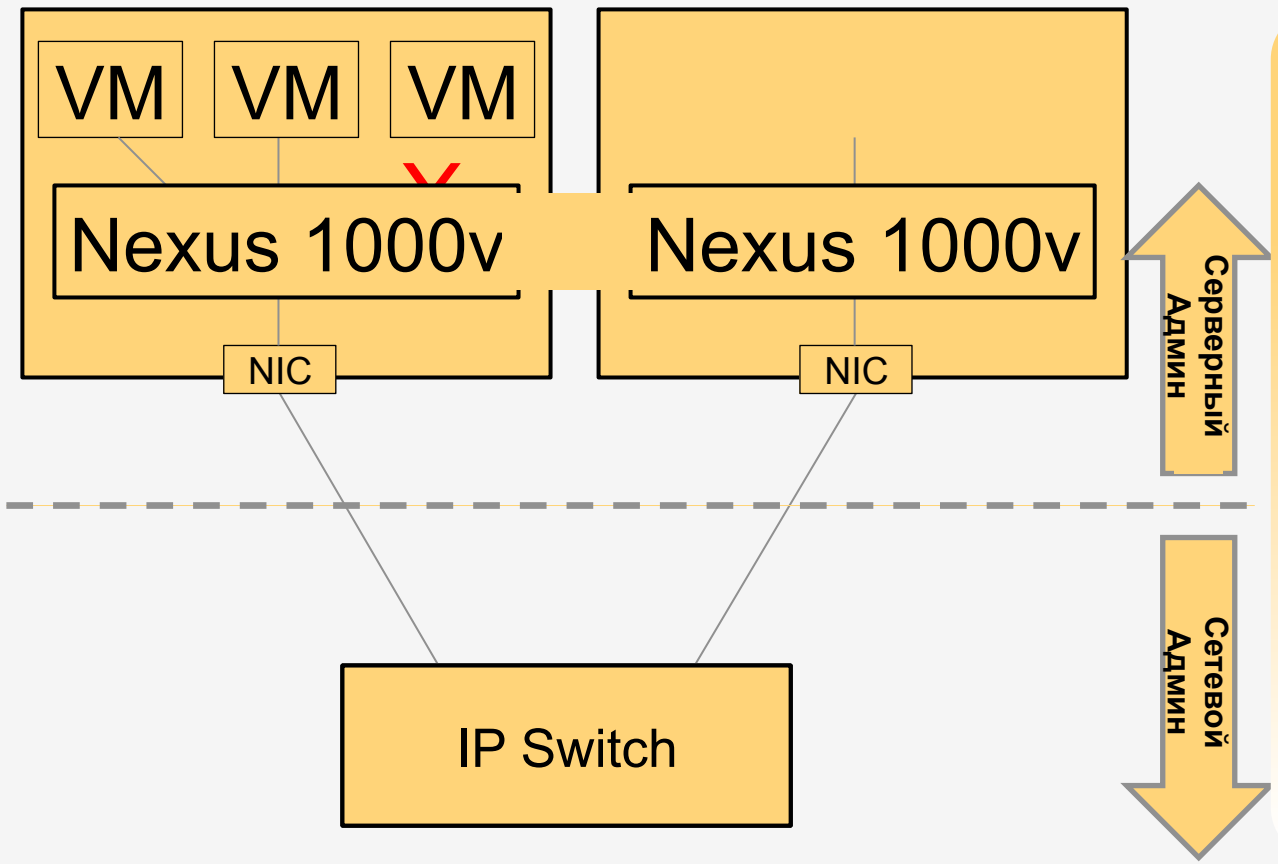
### Мобильность VM

• Политики не следуют за VM при ее миграции(vMotion) **(доступно с DVS)**

### Операционная целостность

• Конфигурация vswitch должна быть выполнена на vCenter (как правило доступна Серверными администраторами)

# Виртуальный Коммутатор



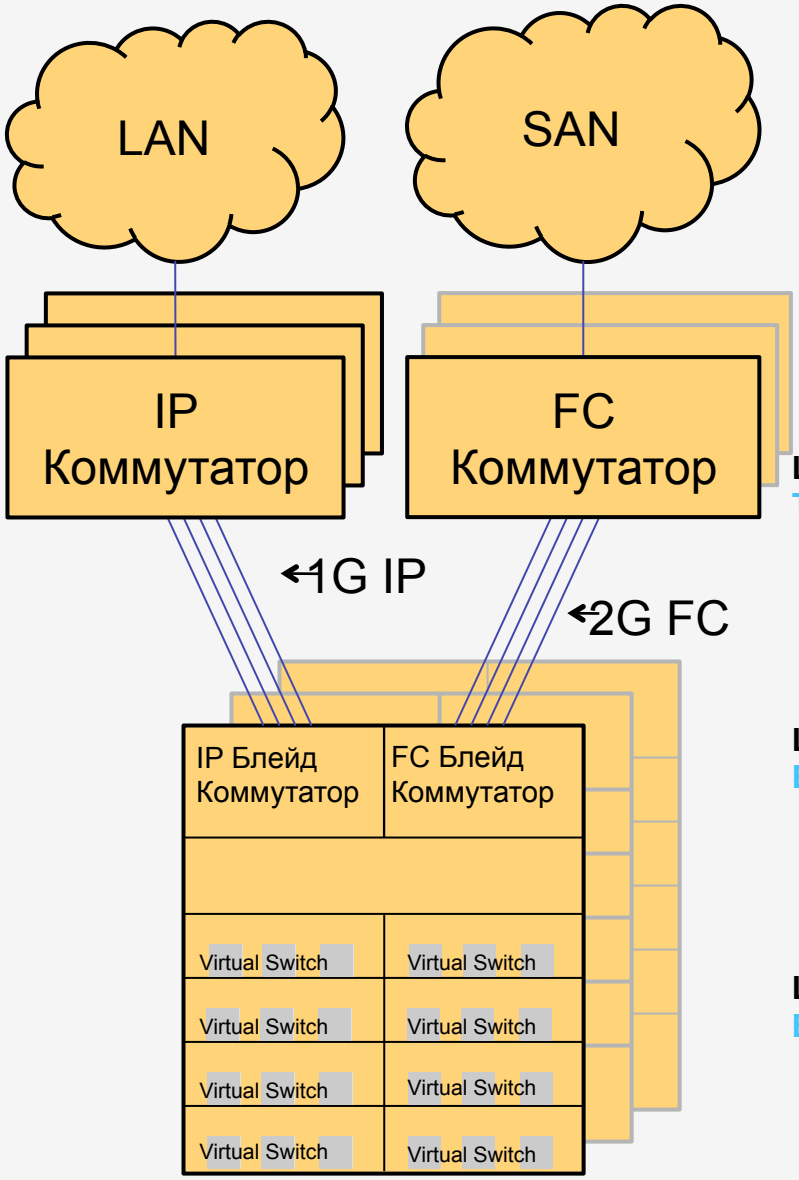

**Выгоды Nexus 1000v**

**Полнофункциональный Cisco коммутатор с NX-OS с QoS, Security, и управлением политиками**

**Мобильность VM**
**Сетевые Настройки следуют за VM при миграции(vmotion)**

**Операционная целостность**
**Сетевой Администратор настраивает сетевые подключения, которые становятся доступны в vCenter для серверных администраторов**

# Де-эволюция подключения серверов



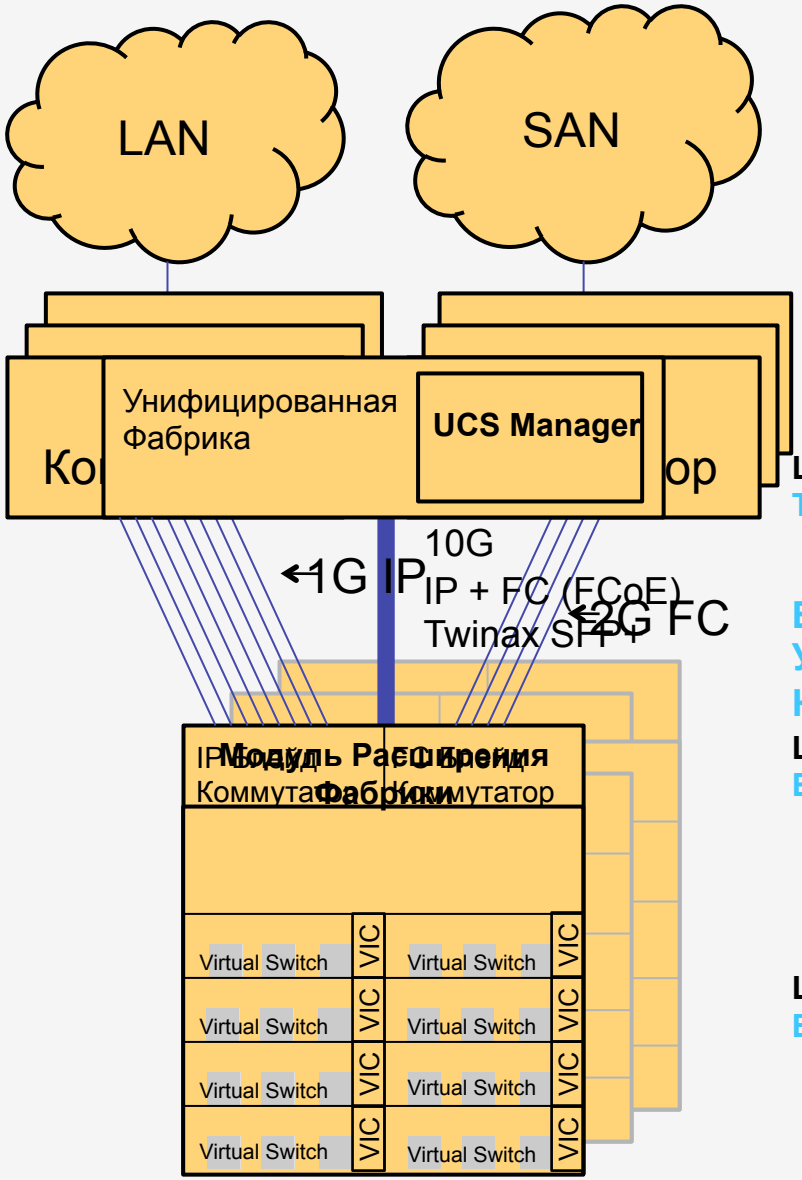

**Layer 3:** X 2
TOR коммутатор

**Layer 2:** X 2
Блейд коммутатор

**Layer 1:**
Вирт. Коммутатор

**Блейд Система/Стойка**
- 3 Уровня коммутации
- Увеличенный диаметр STP
- Отдельные системы управления
- Увеличение сложности при масштабировании

# Революция подключения серверов




**Layer 3:** X 2
TOR коммутатор

ЕДИНЫЙ Уровень Коммутации

**Layer 2:** X 2
Блейд коммутатор

**Layer 1:**
Вирт. Коммутатор

**Фабрика ЦОД:**
- **UCS 62xx**
- **Nexus 55xx**

Cisco коммутатор с NX-OS с QoS, Security, и управлением политиками

**В шасси/стойке:**
- **Nexus 2000**
- **UCS 2200**
- **HP B22HP**

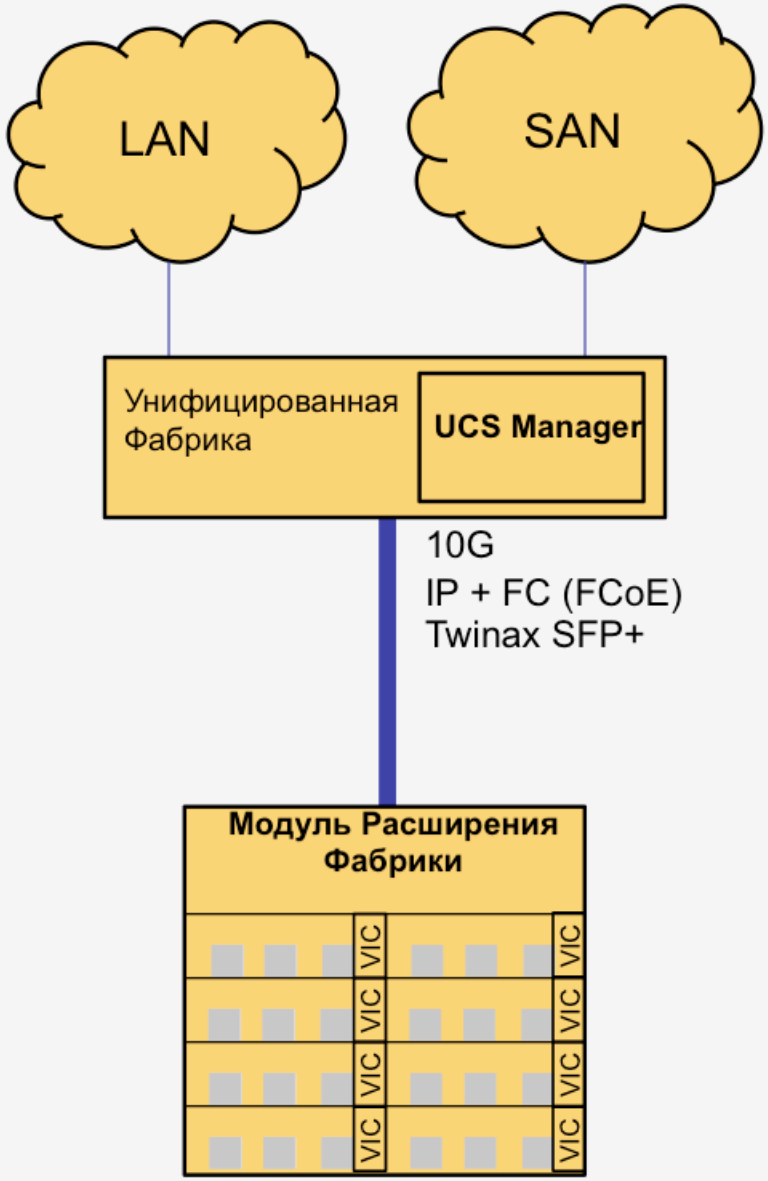
Интерфейсный модуль от Фабрики
- **IBM Nexus4k**

**В сервере:**
- **Adapter-FEX**
- **VM-FEX**

Виртуальная Интерфейсная Карта – модуль от Фабрики

**Сетевое подключение следует за VM при миграции**

# Революция подключения серверов




ЕДИНЫЙ Уровень Коммутации

**Фабрика ЦОД:**
- **•UCS 62xx**
- **•Nexus 55xx**

Cisco коммутатор с NX-OS с QoS, Security, и управлением политиками

**В шасси/стойке:**
- **•Nexus 2000**
- **•UCS 2200**
- **•HP B22HP**

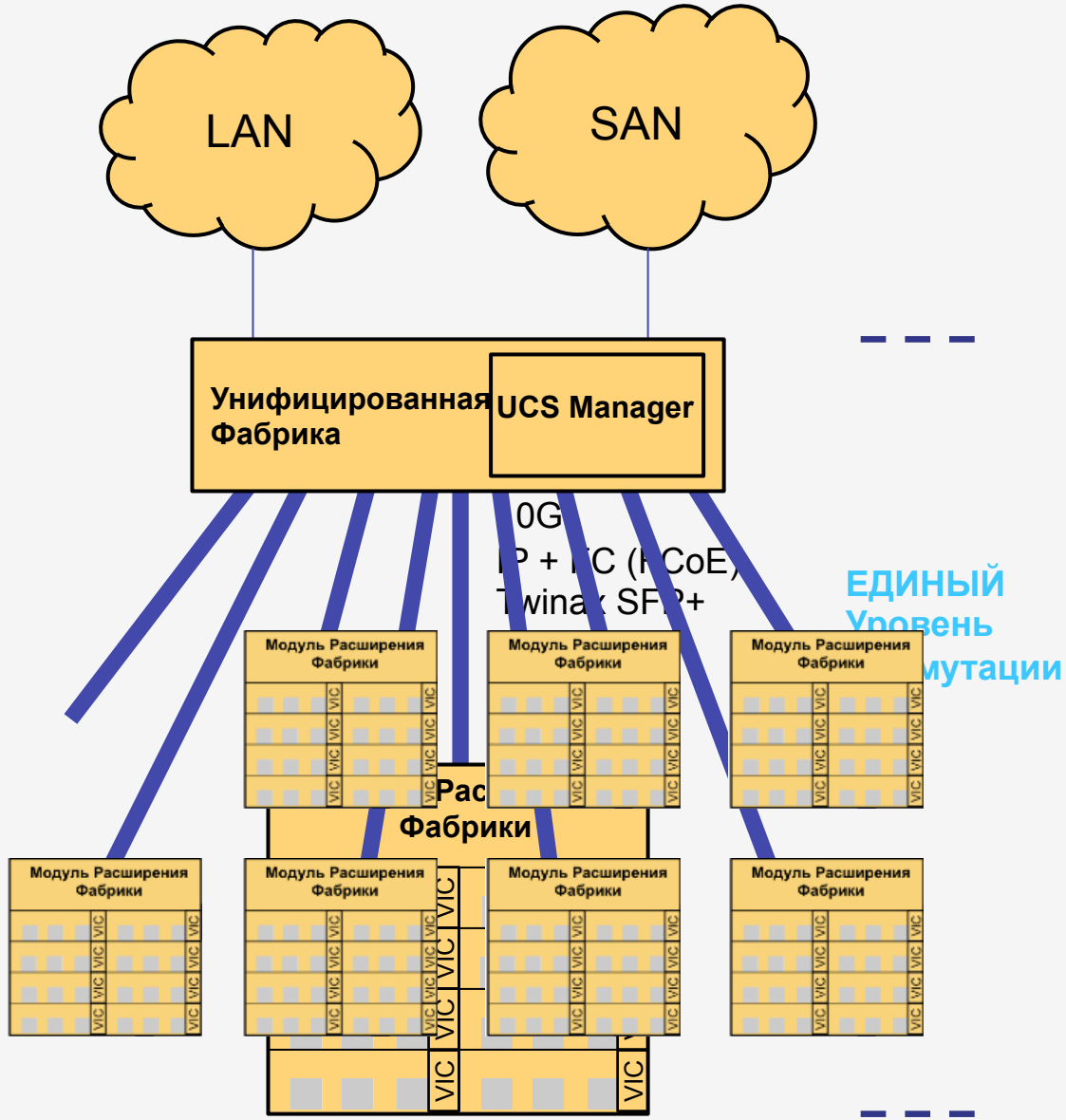
Интерфейсный модуль от Фабрики
- **•IBM Nexus4k**

**В сервере:**
- **• Adapter-FEX**
- **• VM-FEX**

Виртуальная Интерфейсная Карта – модуль от Фабрики

**Сетевое подключение следует за VM при миграции**

# Революция подключения серверов




**Фабрика ЦОД (UCS/Nexus)**

**Масштабирование без увеличения сложности:**

- **сотни серверов**
- **тысячи VM**

**Мобильность VM по всей фабрике**

**Операционная целостность:**

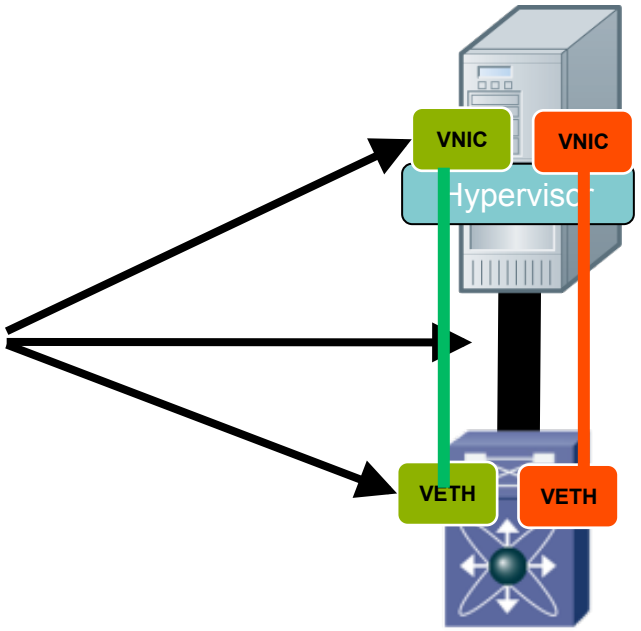
- **vCenter**
- **VMM**

# Cisco видение Сети для Виртуализации

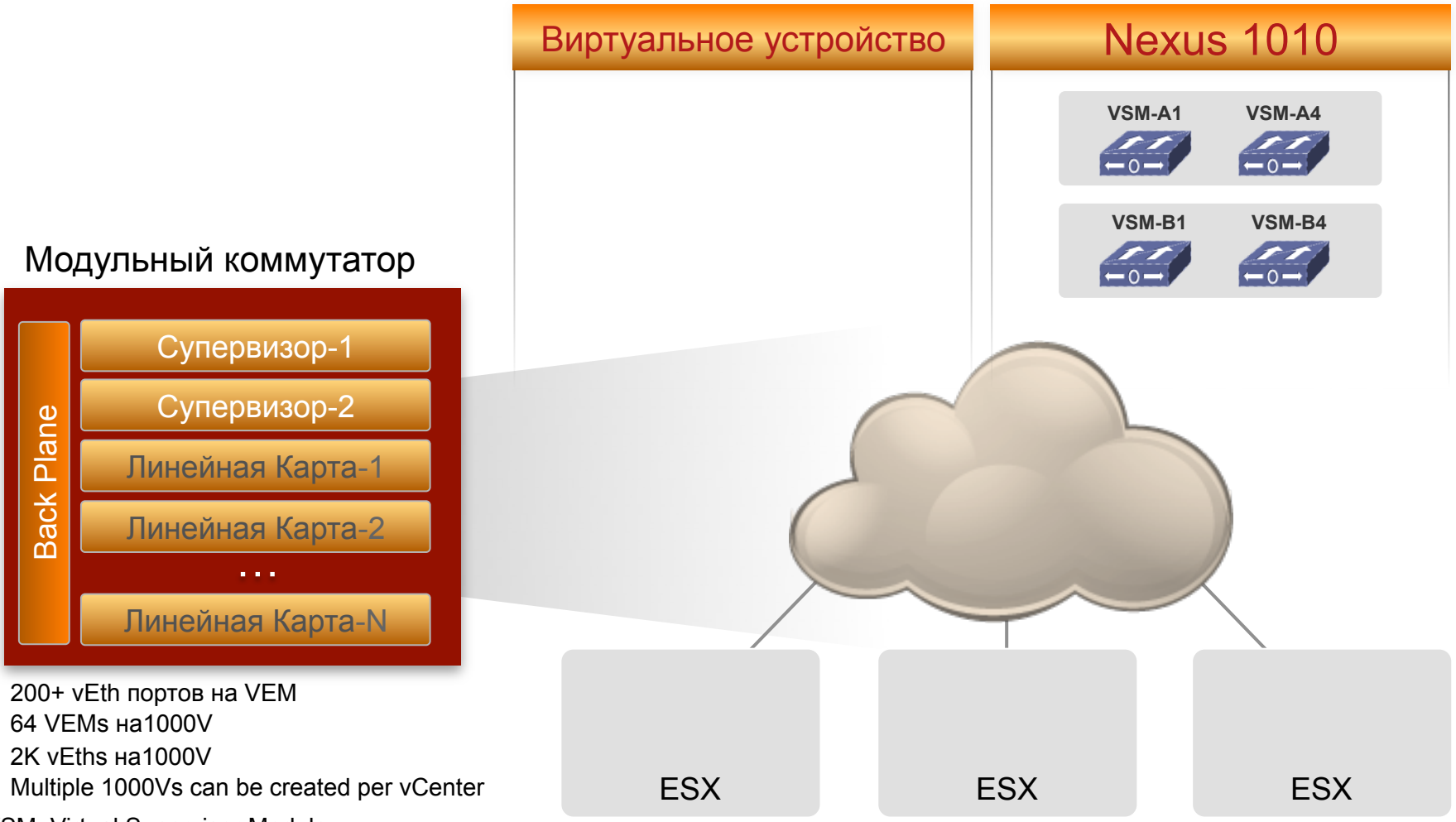
# Cisco Nexus 1000V

# Cisco технология VN-Link

- Логический Эквивалент комбинации сетевой карты NIC, порта коммутатора Cisco и патчкорда RJ-45.



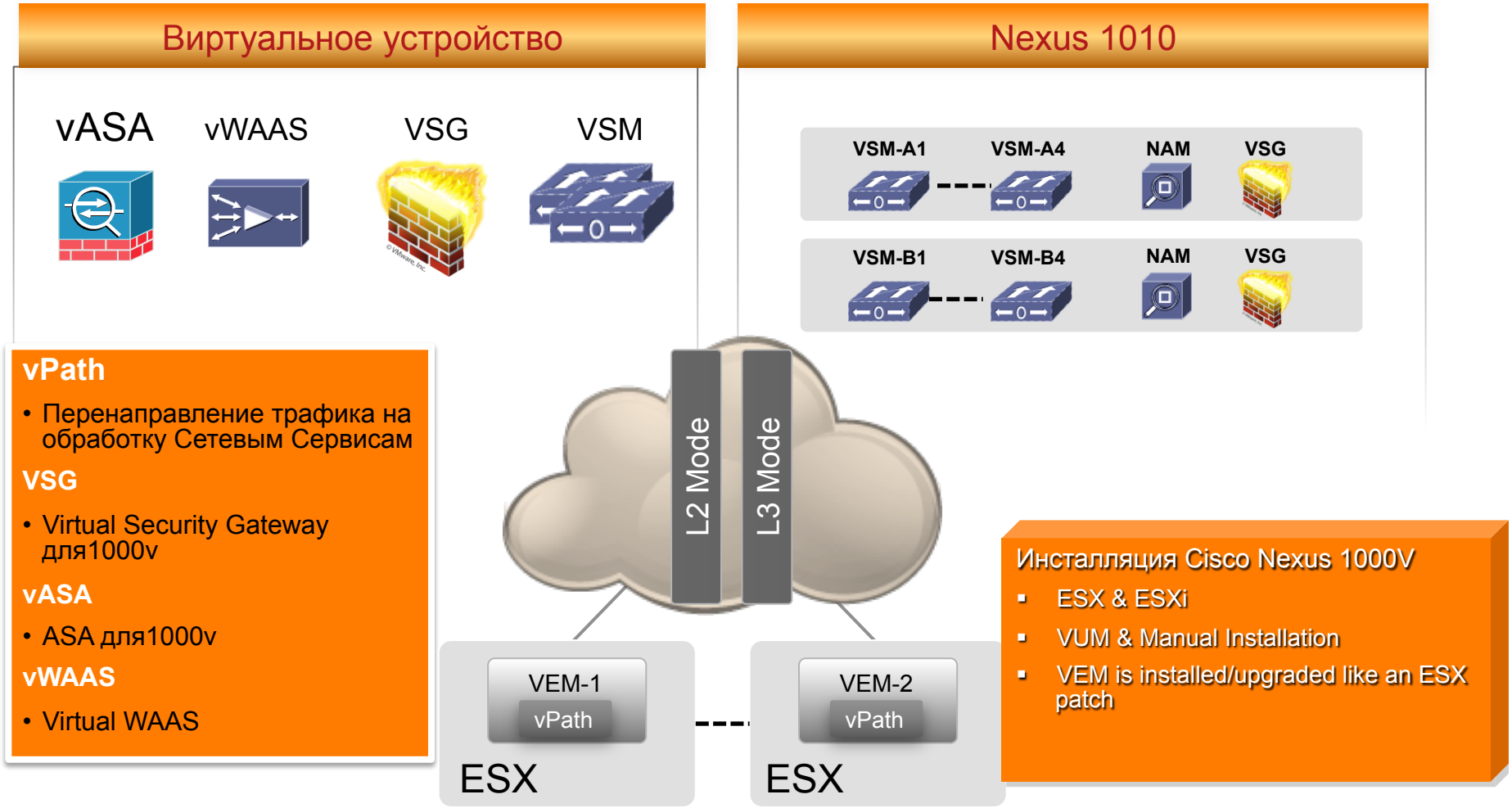
# Архитектура Nexus 1000V




- 200+ vEth портов на VEM
- 64 VEMs на1000V
- 2K vEths на1000V
- Multiple 1000Vs can be created per vCenter

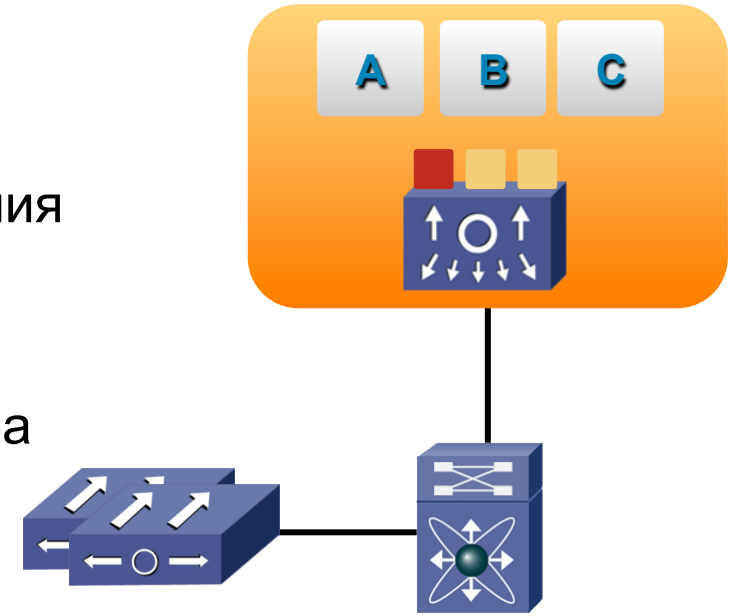
VSM: Virtual Supervisor Module
VEM: Virtual Ethernet Module

# Nexus 1010—Платформа для Сервисов



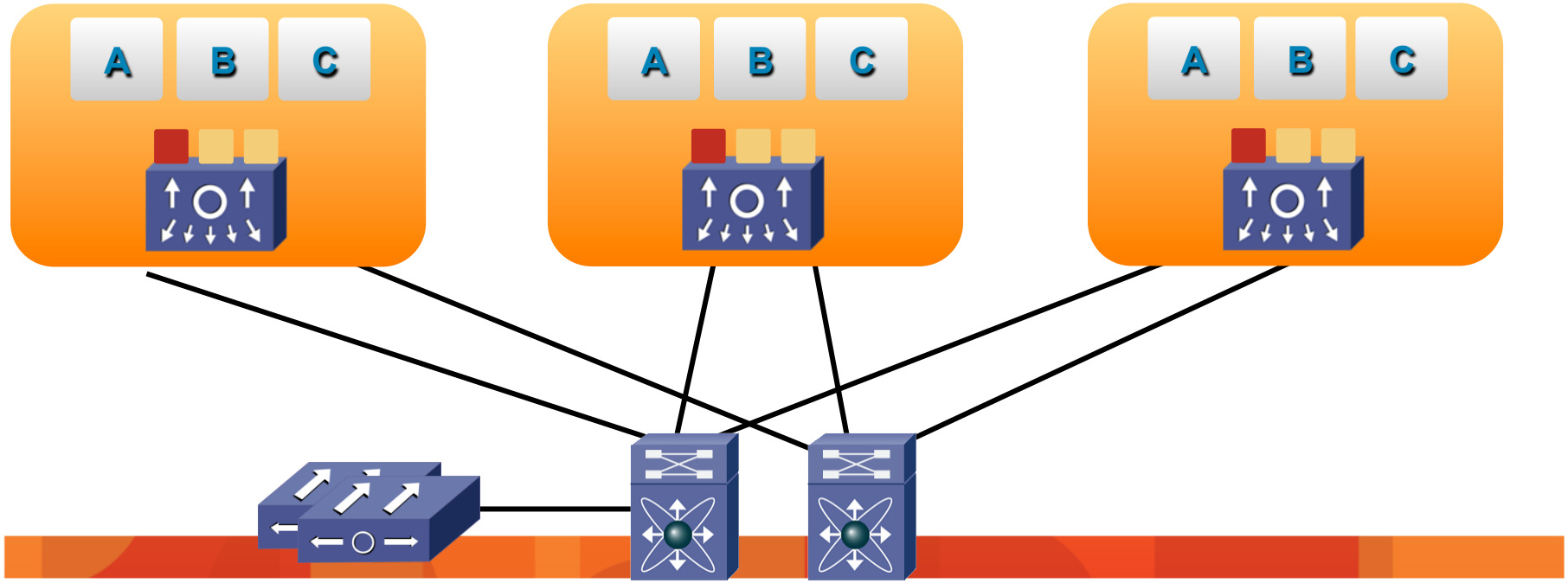
# Централизованный Контроль и Управление

- Даже учитывая то, что 1000V распределенный коммутатор, Он представляется как единый логический  коммутатор с точки зрения управления и контроля
- Протоколы CDP, Netflow, SNMP управляются с помощью супервизора VSM (Virtual Supervisor Module)

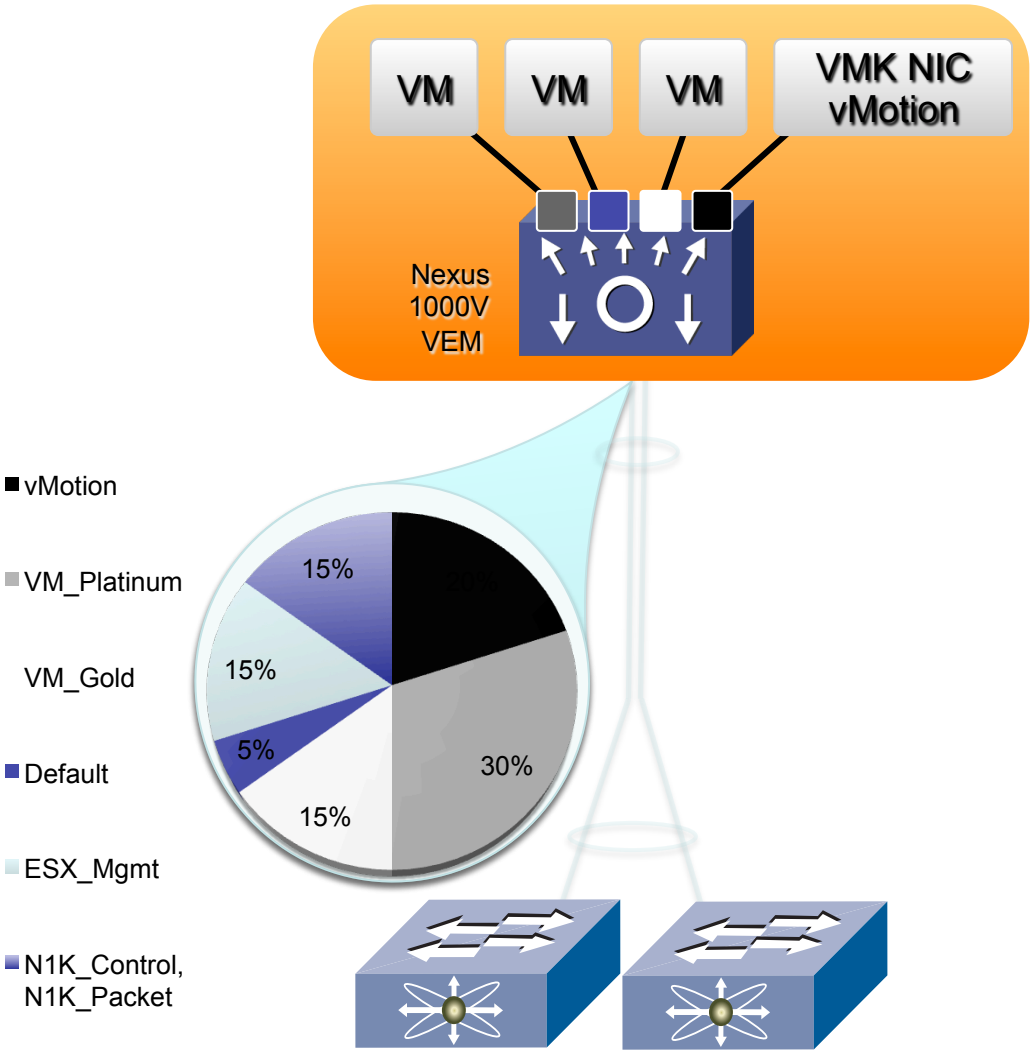


# Распределенный коммутатор

- Модуль Виртуального Ethernet (VEM) – передача данных
- Модуль Виртуальног Супервизора – контрольный трафик и управление
- Каждый Модуль Виртуального Ethernet коммутирует пакеты не зависимо от другого модуля



# Качество Сервиса

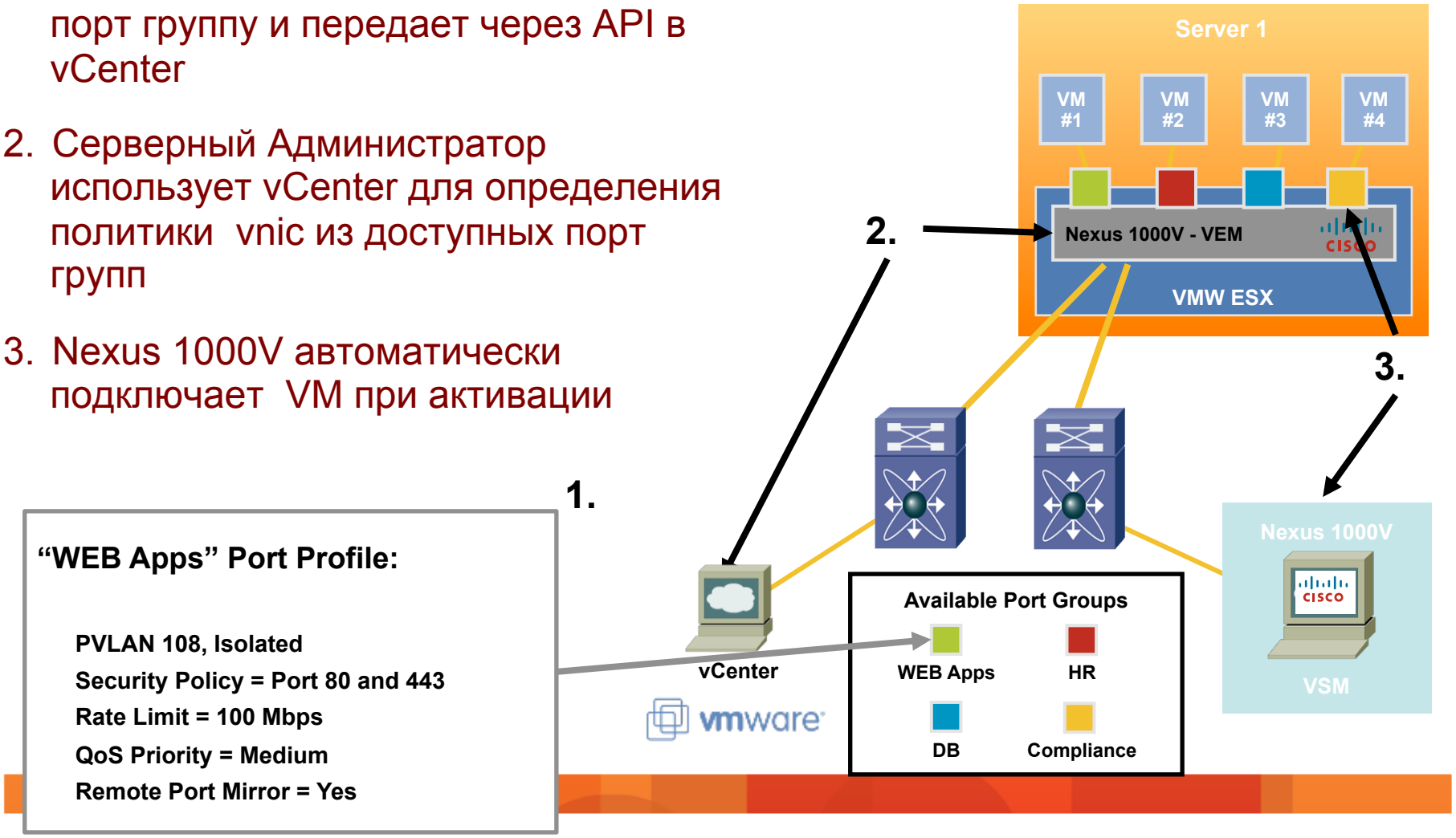



- Основан на классах Weighted Fair Queuing (CB-WFQ)
- Гарантирование пропускной полосы для 16 очередей на аплинках
- Определяемые пользователем Очереди
- 8 Пред-определенных классов
  - Для протоколов VMware и1000V
- Очереди конфигурируются модульным QoS CLI (MQC)

QoS White Paper Available

# Порт Профайл

1. Nexus 1000V автоматически создает порт группу и передает через API в vCenter
2. Серверный Администратор использует vCenter для определения политики  vnic из доступных порт групп
3. Nexus 1000V автоматически подключает  VM при активации

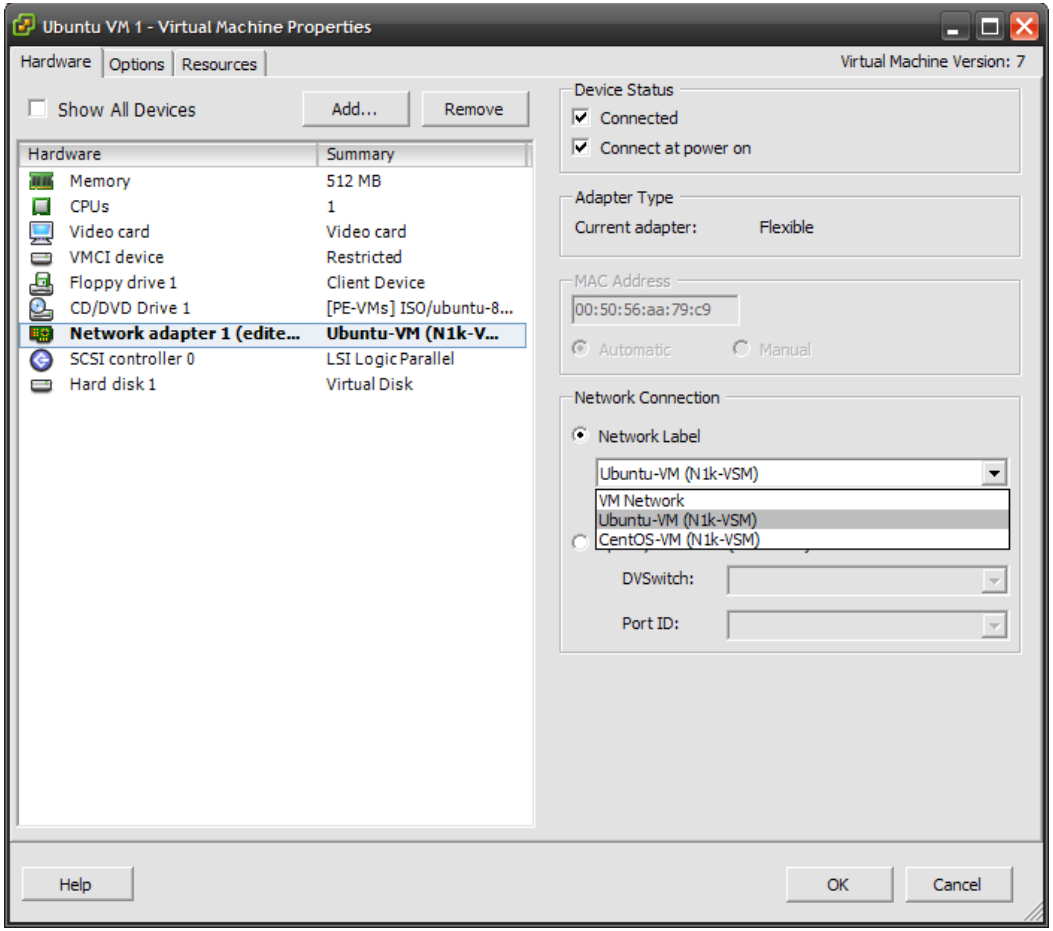


# Профиль порта: для сети и серверов

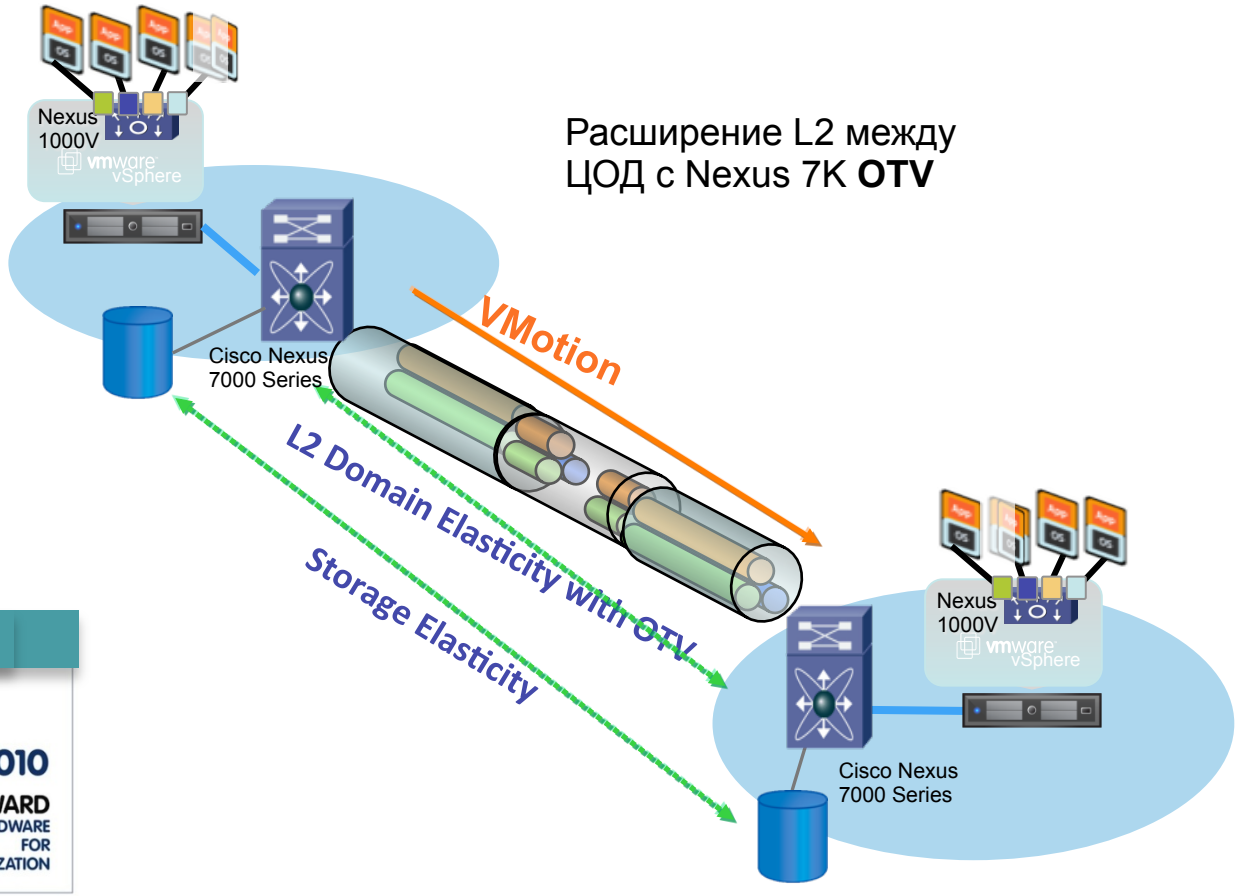
## Администратор сети

```
N1k-VSM# sh port-profile name Ubuntu-VM

port-profile Ubuntu-VM

  description:

  status: enabled

  capability uplink: no

  capability l3control: no

  system vlans: none

  port-group: Ubuntu-VM

  max-ports: 32

  inherit:

  config attributes:

    switchport mode access

    switchport access vlan 95

    no shutdown

assigned interfaces:

    Vethernet2

    Vethernet4
```

## Администратор серверов



# Long Distance vMotion




Расширение L2 между
ЦОД с Nexus 7K **OTV**

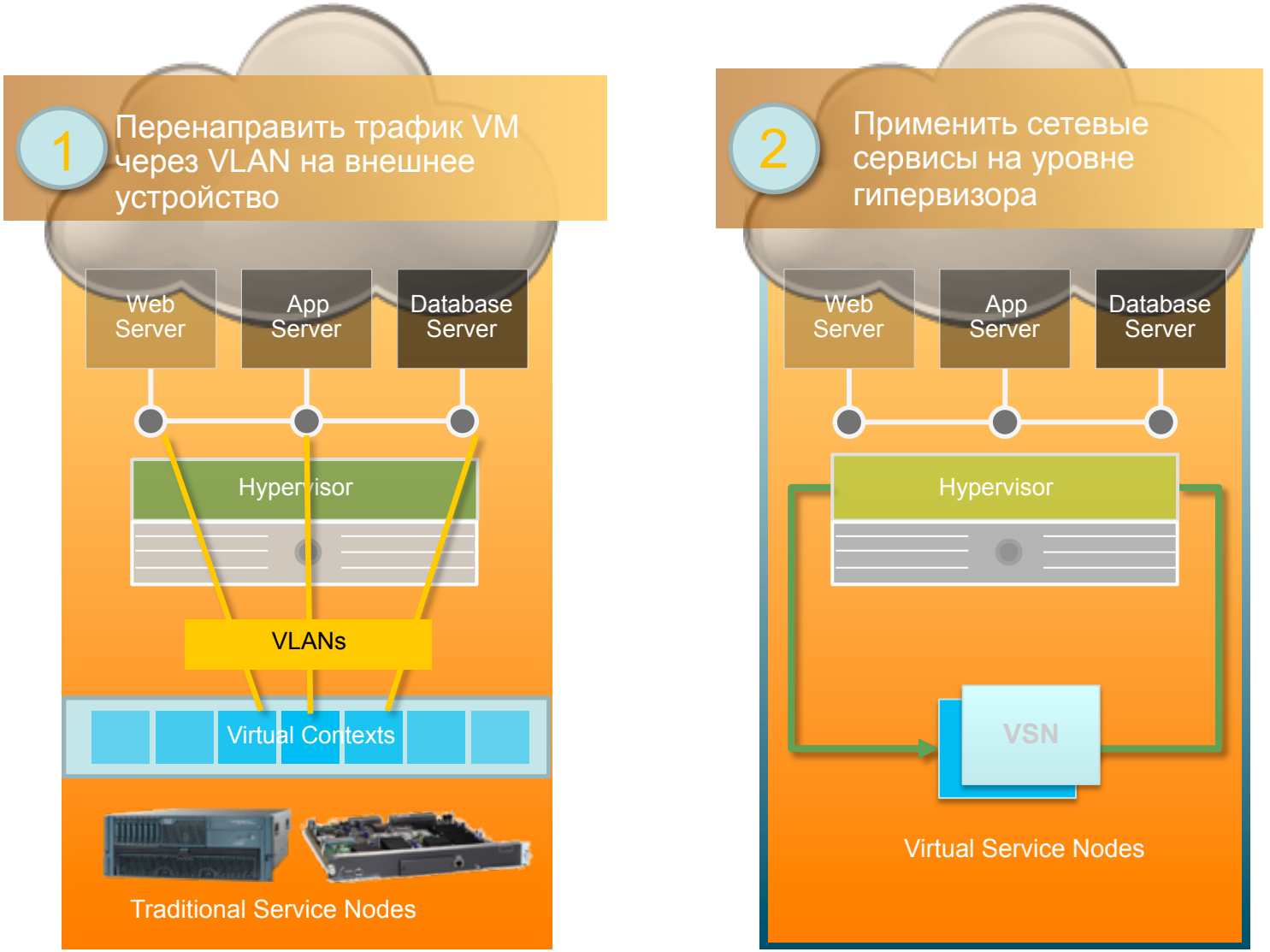
O T V

SearchServerVirtualization.com
BEST OF
vmworld 2010
GOLD AWARD
HARDWARE
FOR
VIRTUALIZATION

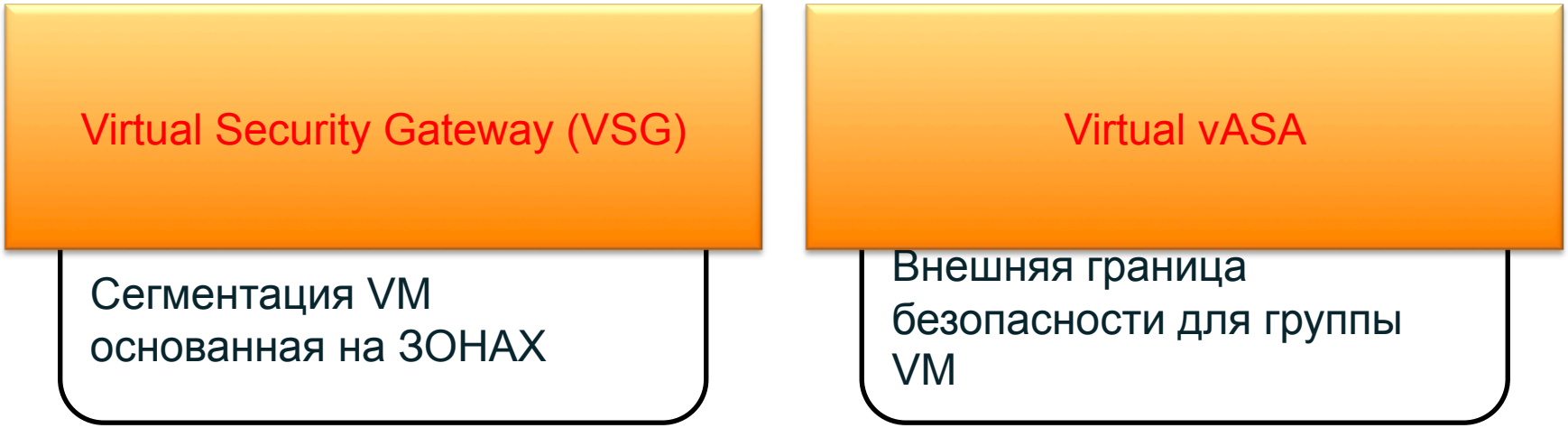
OTV: Overlay Transport Virtualization

# Виртуальные Сервисы для Виртуализованных Серверов

# Варианты Сетевых сервисов



# Портфель Сервисов Безопасности



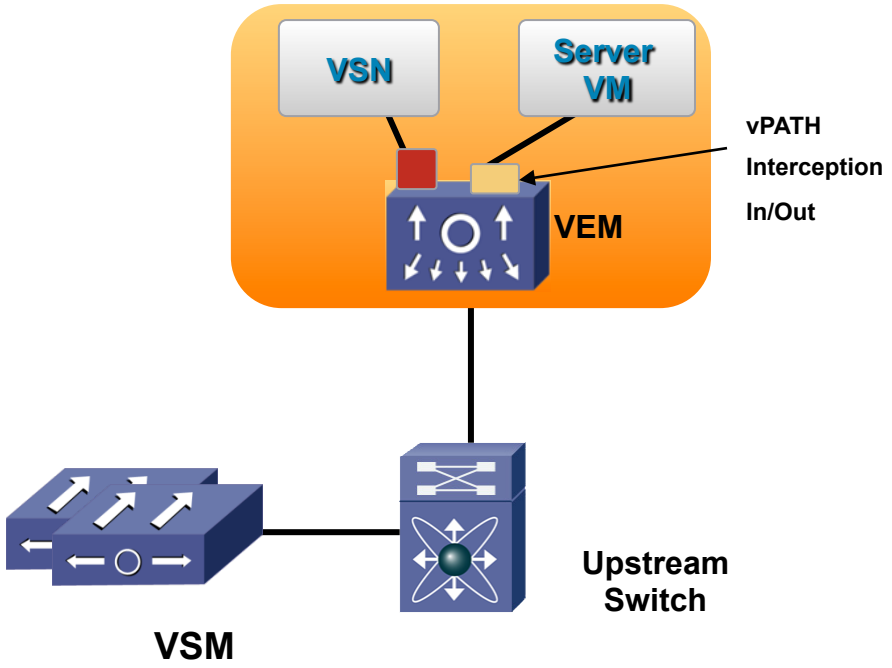

VMWare vSphere

Nexus 1000V

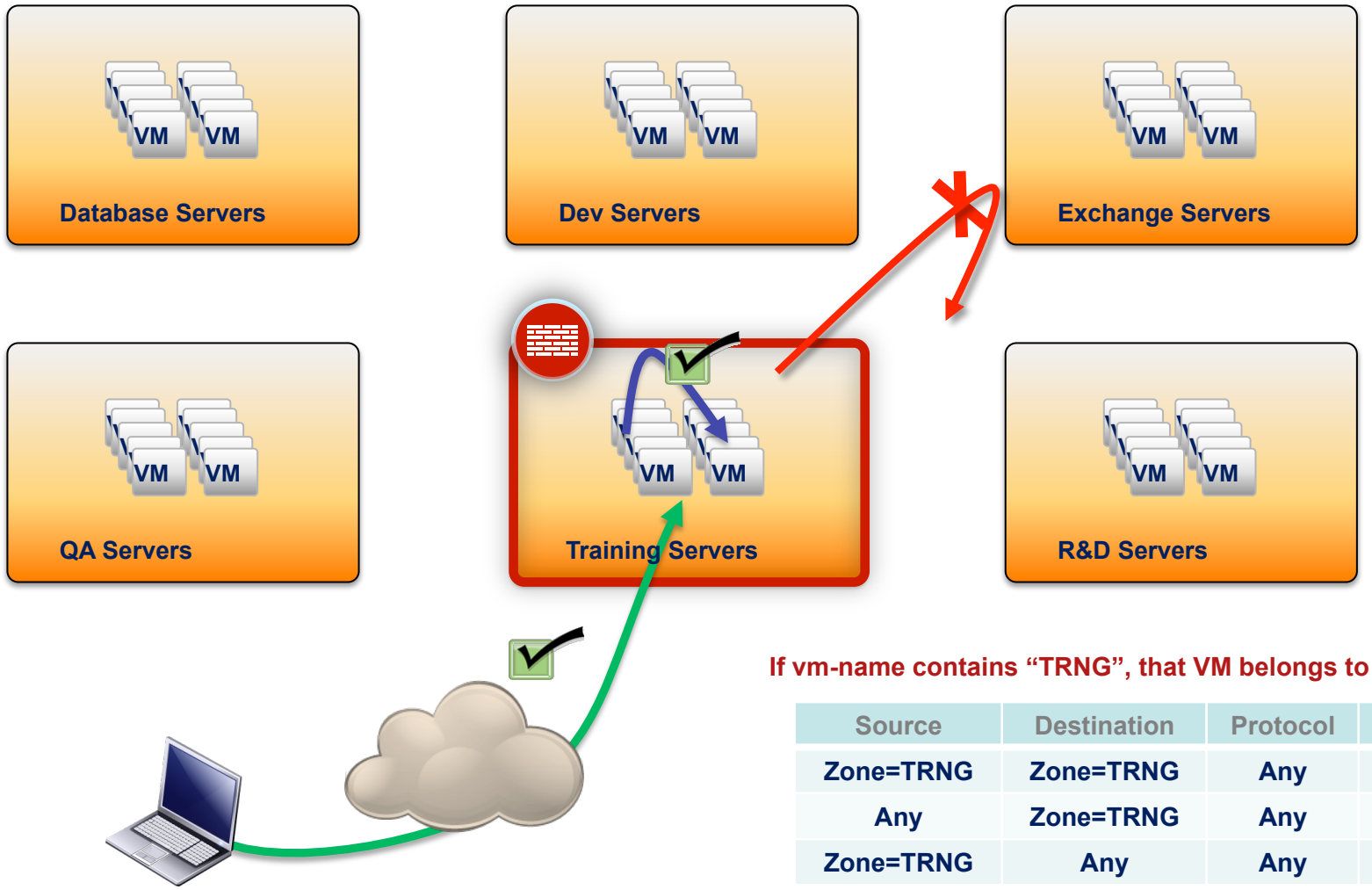
VNMC

# Технология «перехвата» трафика vPATH в Nexus 1000v

- vPATH перехватывает трафик на порту подключения VM в обоих направлениях и отправляет на обработку в сетевые сервисы
- Последовательный трафик передается напрямую после инсталляции ACL.



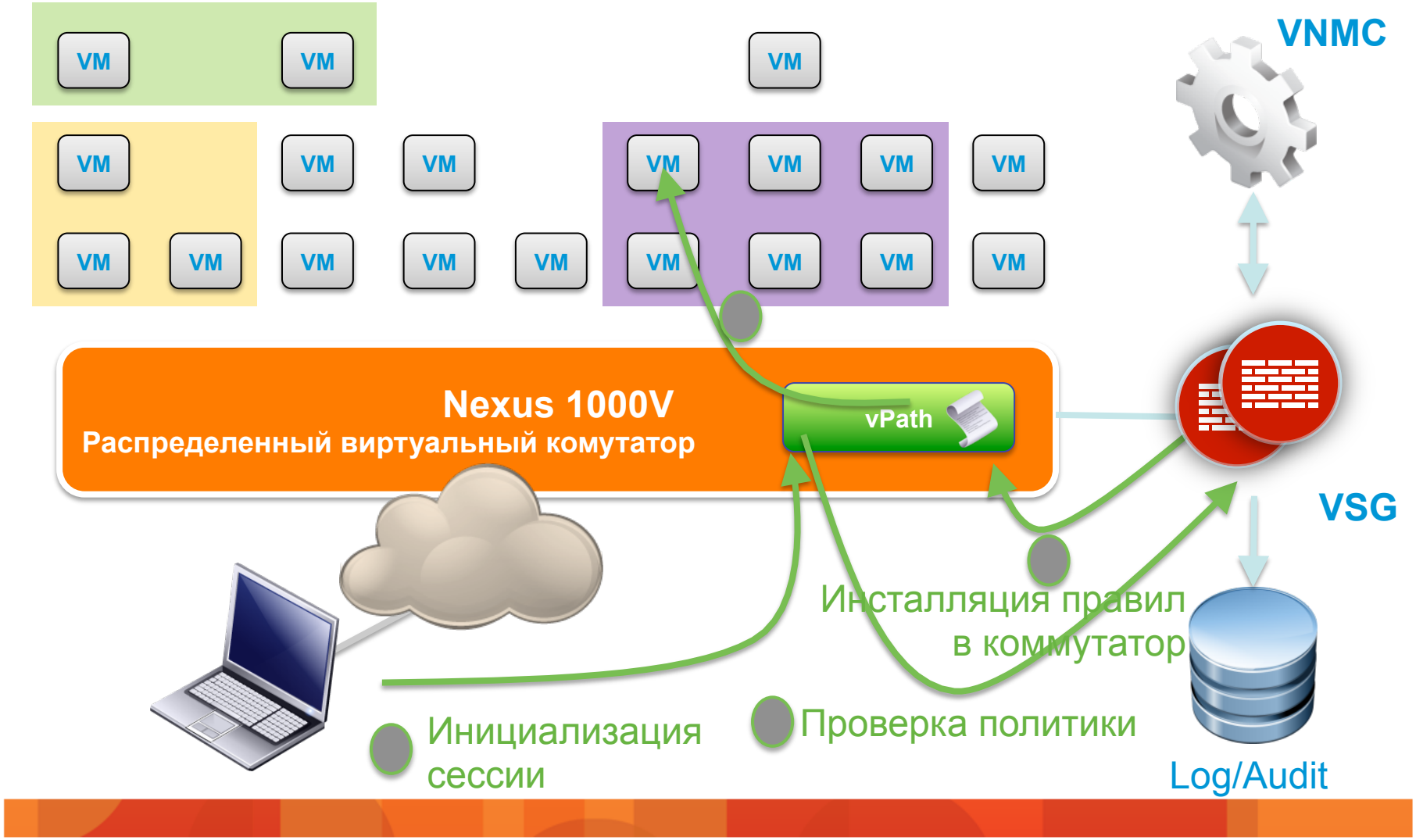
# Пример VSG
## Логические Зоны, vMotion & масштабирование



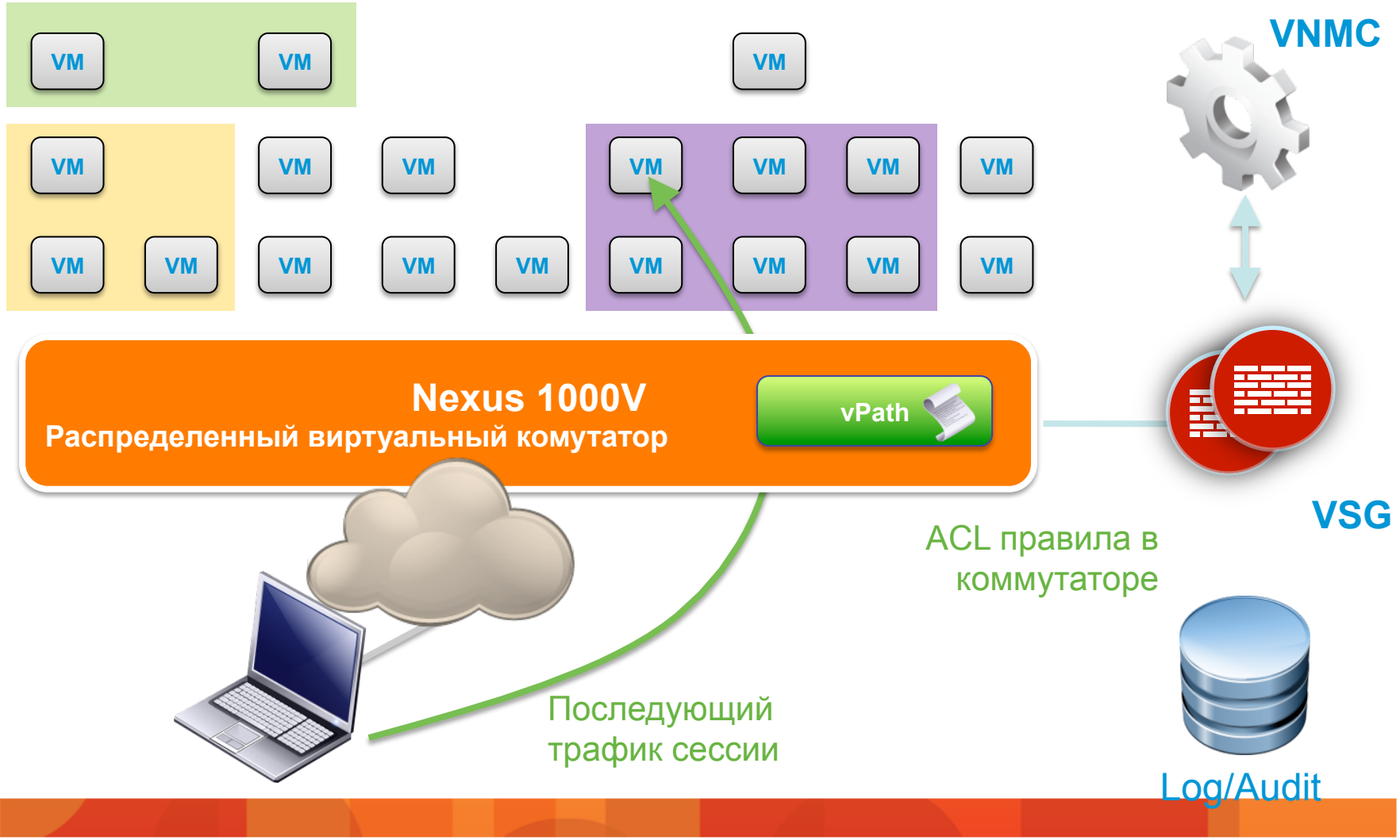

If vm-name contains “TRNG”, that VM belongs to TRNG zone

| Source | Destination | Protocol | Action |
|---|---|---|---|
| Zone=TRNG | Zone=TRNG | Any | Permit |
| Any | Zone=TRNG | Any | Permit |
| Zone=TRNG | Any | Any | Drop |

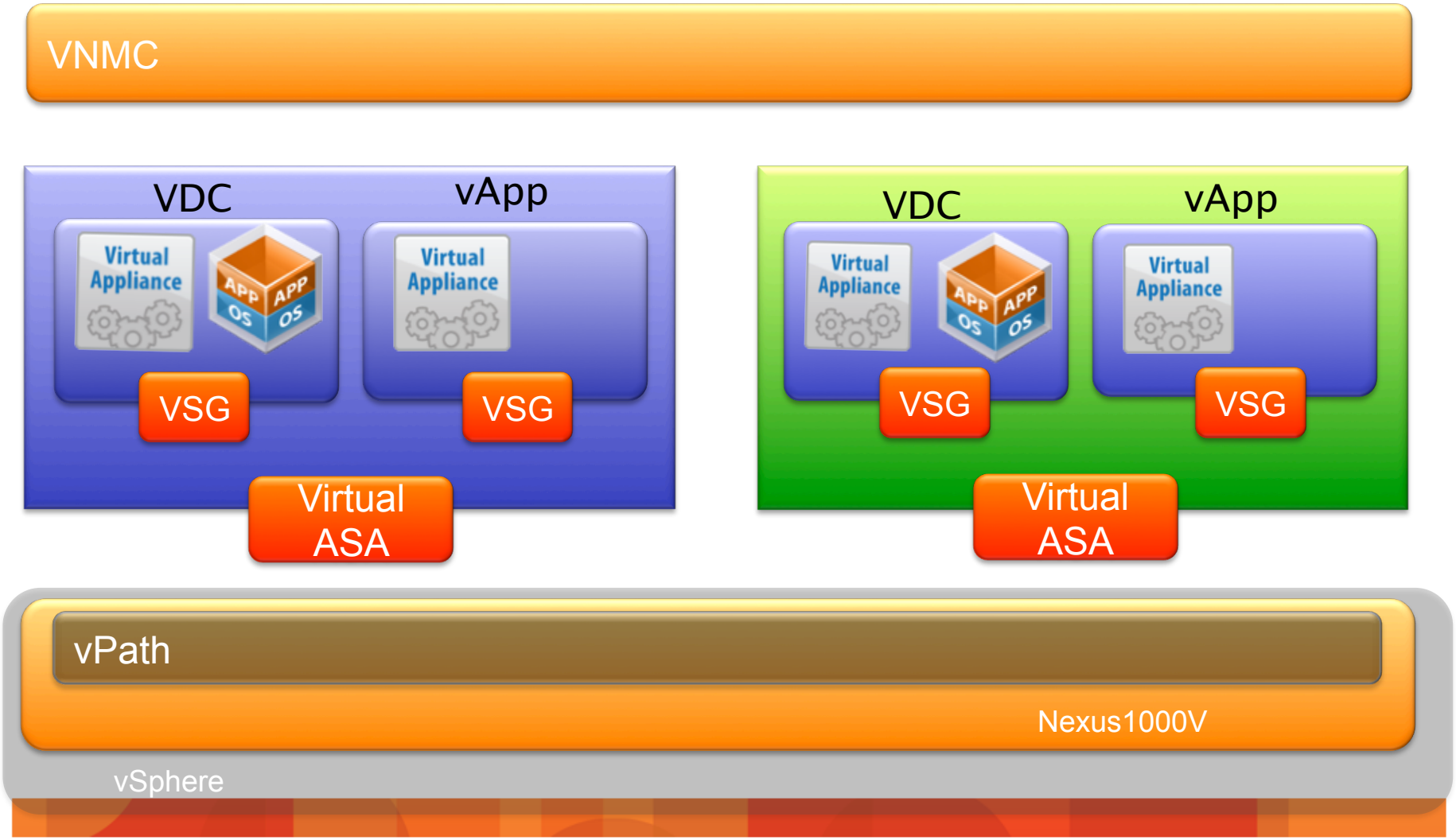
# vPath: Высокая Производительность



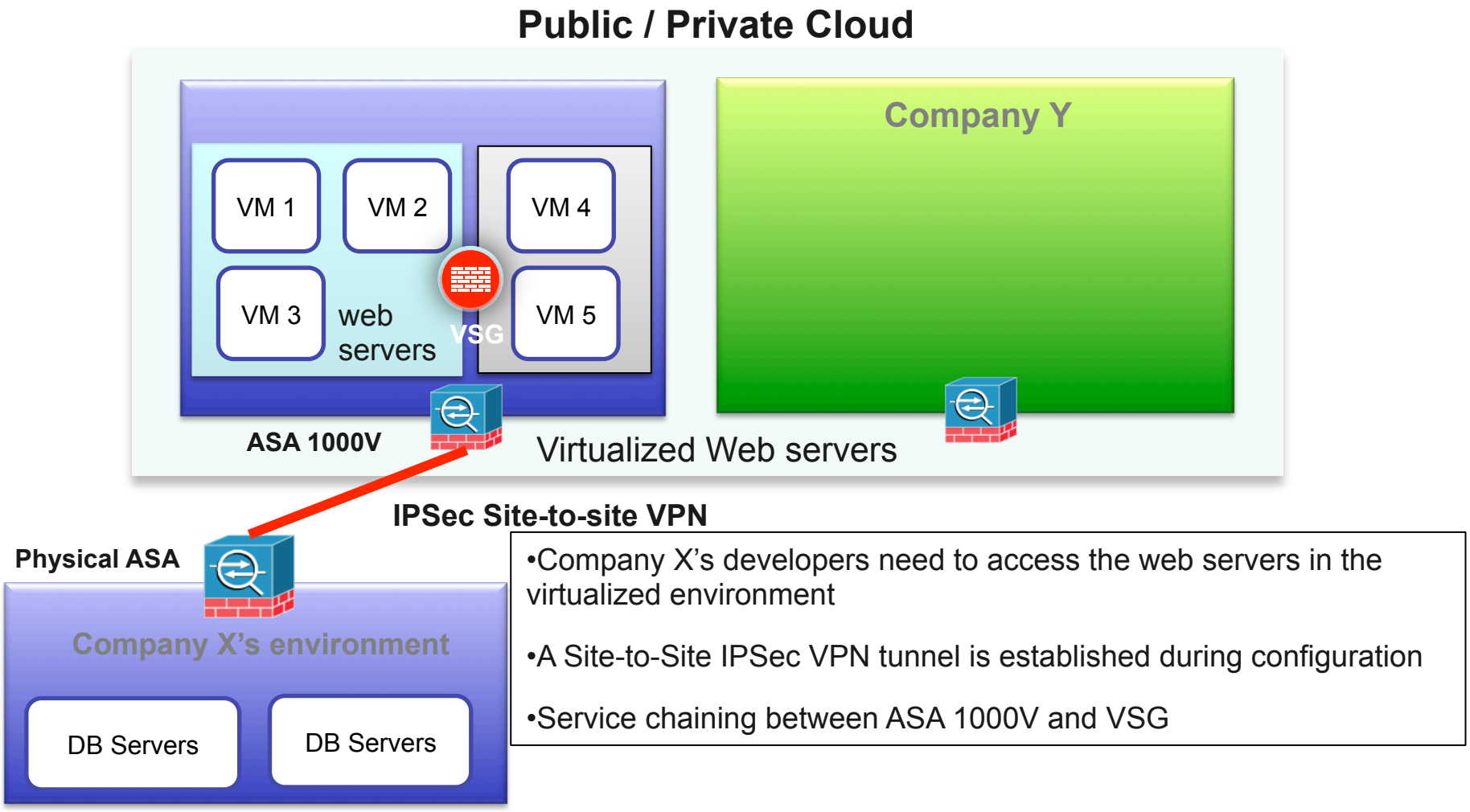
# VSG: Высокая Производительность



# Внедрение Сетевых Сервисов для Виртуализованных серверов

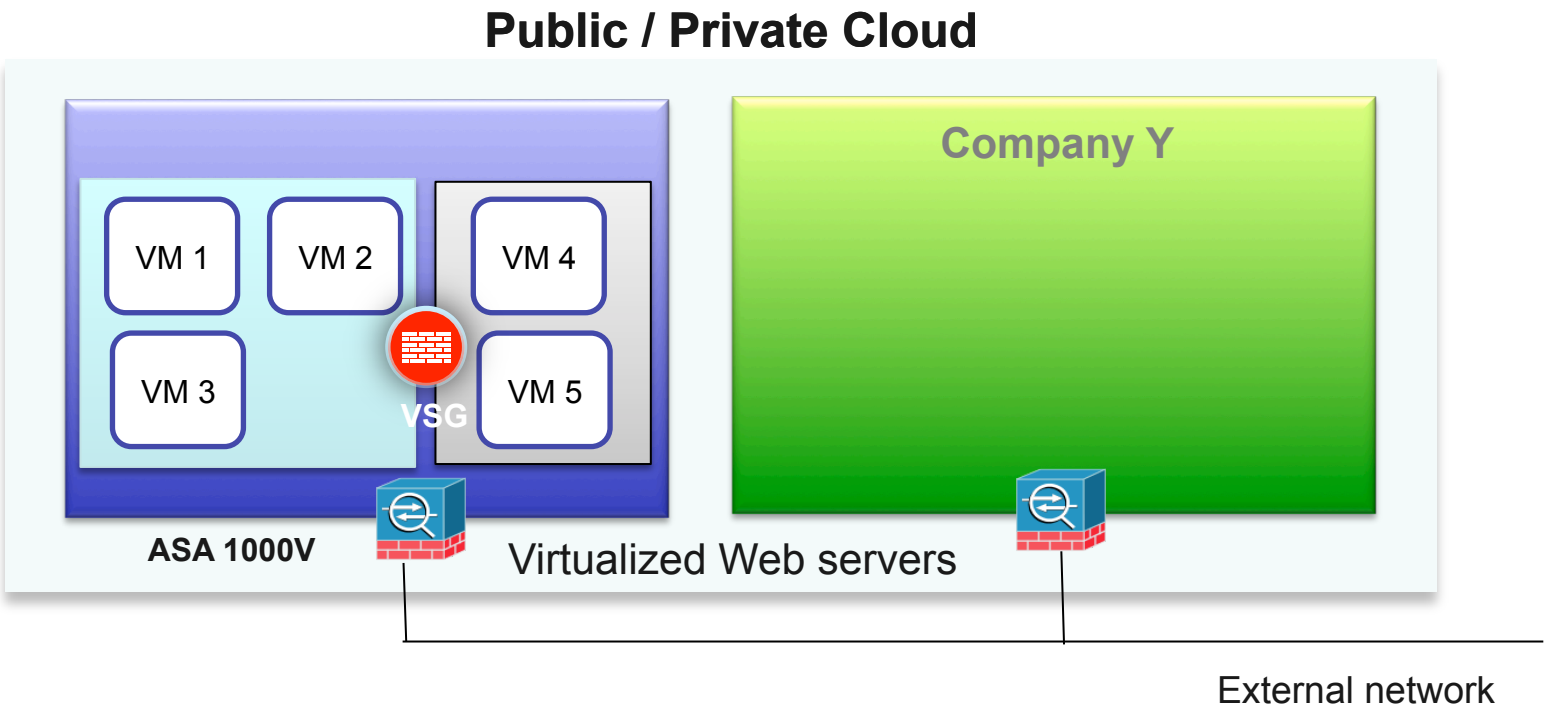


# Пример: VPN



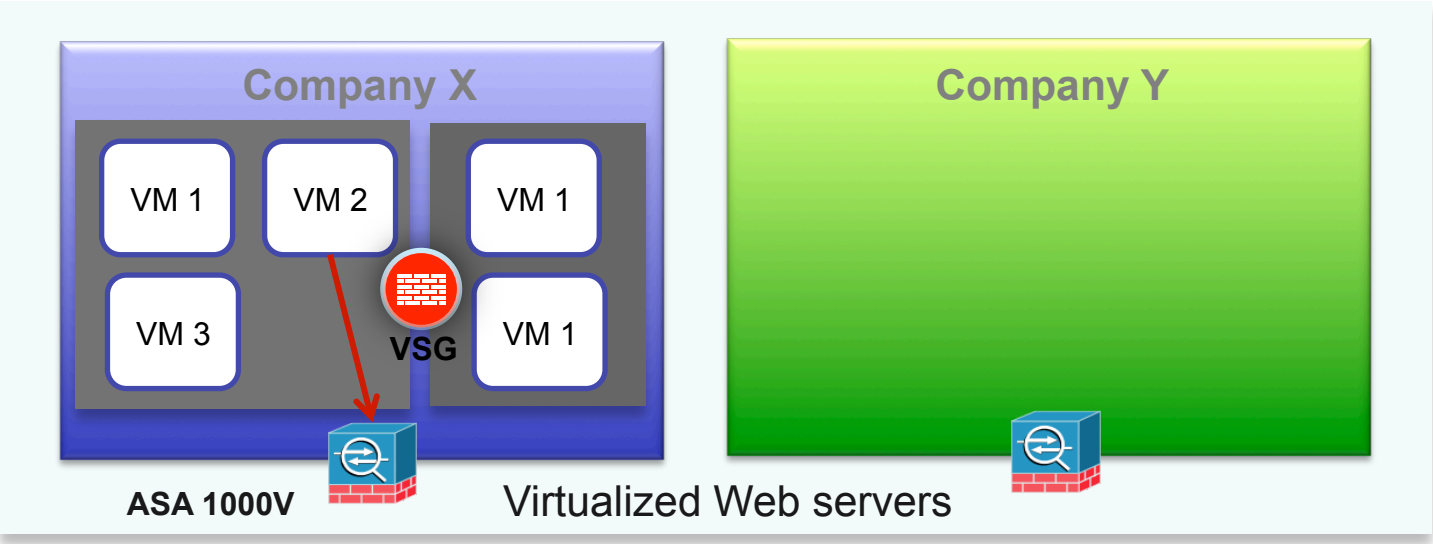

- Company X's developers need to access the web servers in the virtualized environment
- A Site-to-Site IPSec VPN tunnel is established during configuration
- Service chaining between ASA 1000V and VSG

# Пример: NAT



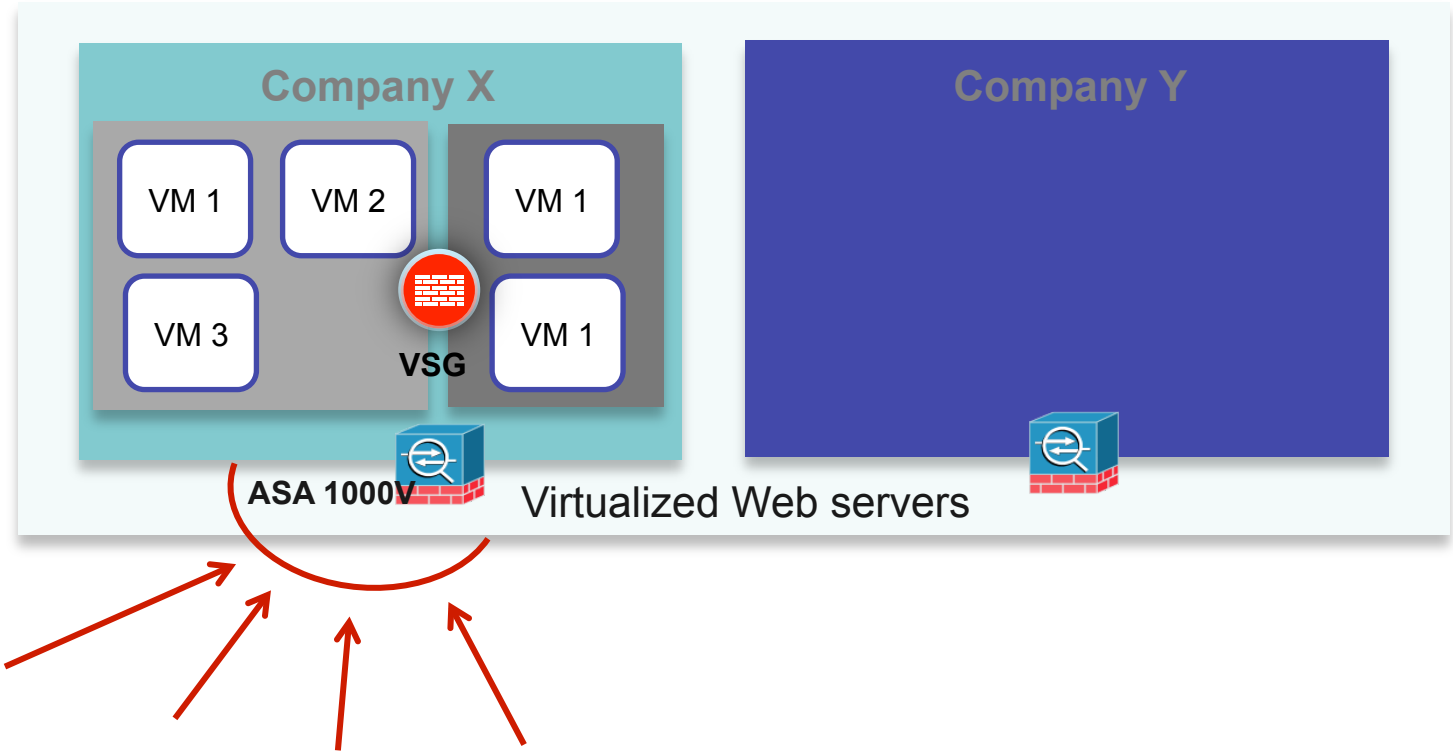

- Company X clones it's tenant resulting in overlapping IP addresses between the two tenants
- ASA 1000V allows customers to isolate the overlapping addresses networks using dynamic NAT while communicating with the external network

# Пример: DHCP




ASA 1000V acts as a DHCP server and allocates IP addresses when request is received from any of the VMs within the tenant.

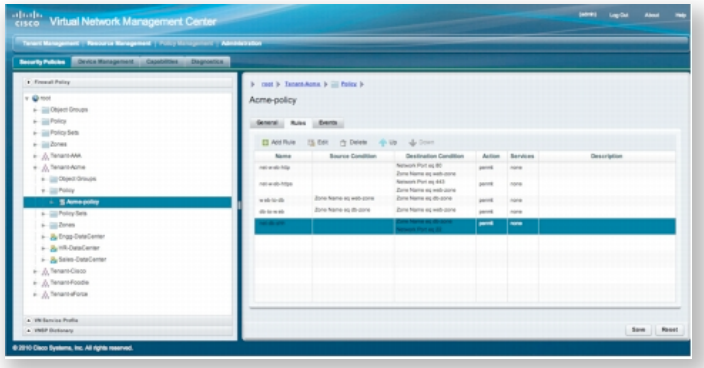
# Пример: Предотвращение Атак




- Basic IDS Support: Supports a basic list of signatures
- The customer can configure ASA 1000V to raise alarm on traffic that matches a signature

# Центр Управления Виртуальными сервисами

- Управление политиками Безопасности в VSG vASA




VNMC GUI

## Multi Tenant
Different Customers, different needs

## Security Profiles
Simple, policy based security config

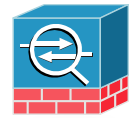
## XML API
3rd party integration ready

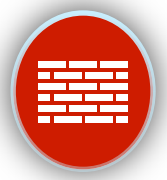
## Role Based Access Controls
Different users, different privileges, LDAP/AD AuthN

## Nexus 1000V &vCenter
Port profiles refer to security profiles

## Dynamic provisioning
One stop configuration of network & security

Virtual ASA



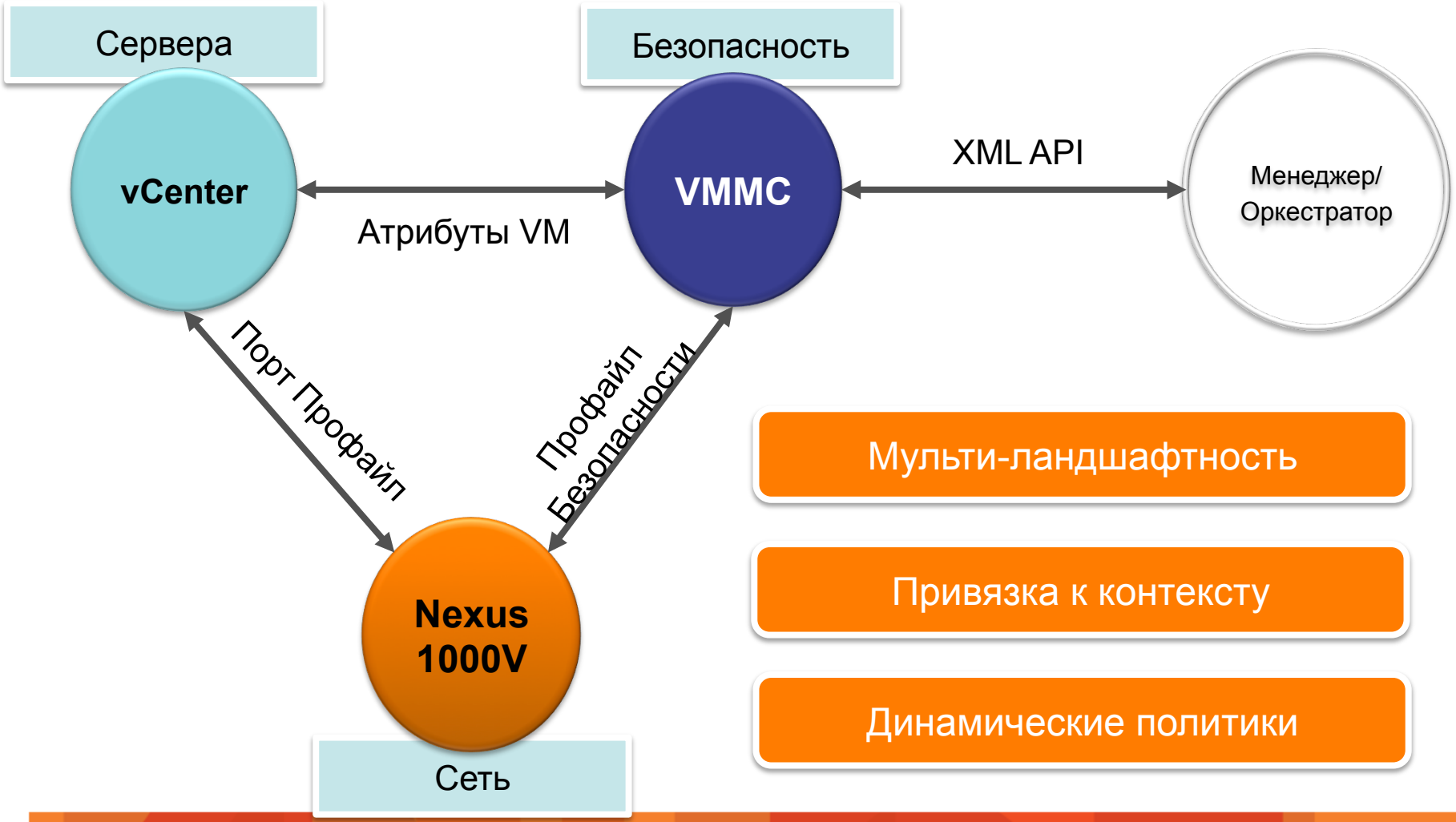


Virtual Security Gateway

Virtual Network Management Center (VNMC)

# Virtual Network Management Center

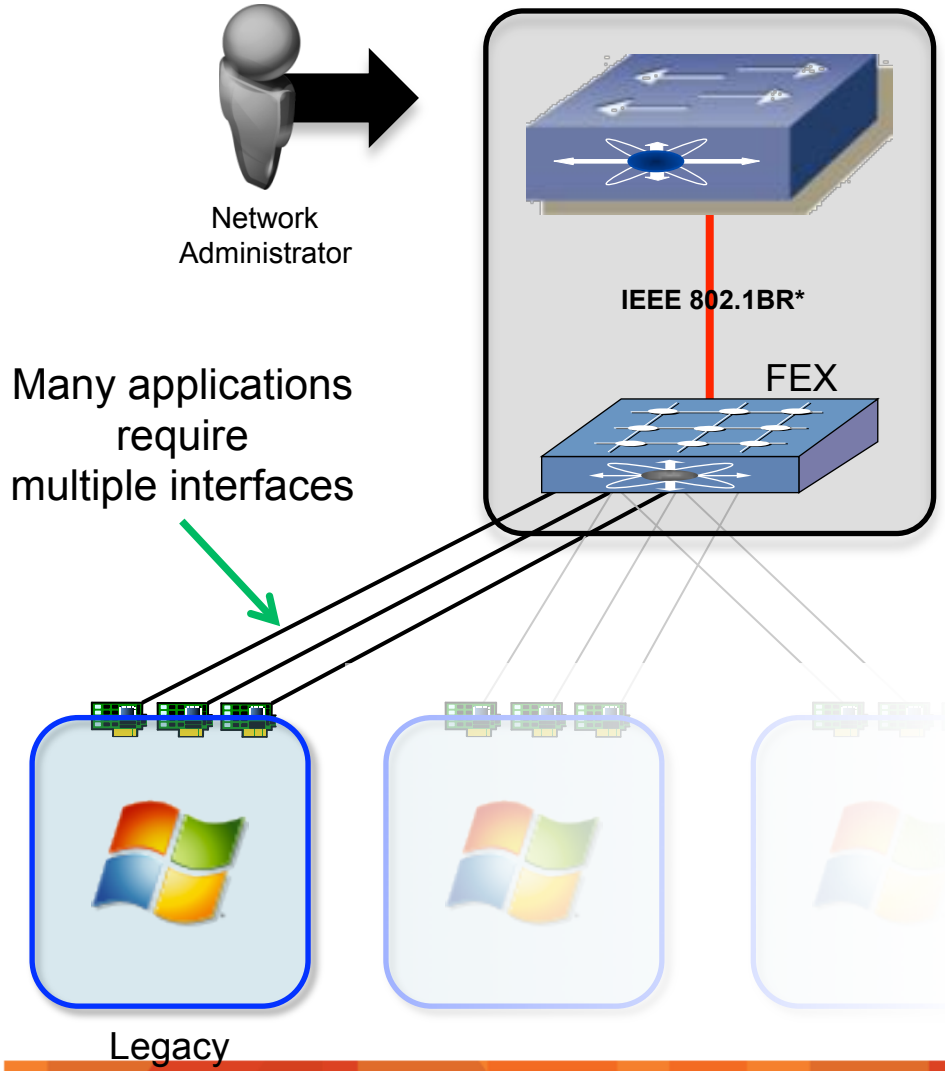
## *Операционная модель & Управление Политиками*



# Концепция модулей расширения Фабрики

# Эволюция технологии Fabric Extender

## Распределённый коммутатор до уровня стойки, интерфейсов сервера и VM




# Единое устройство

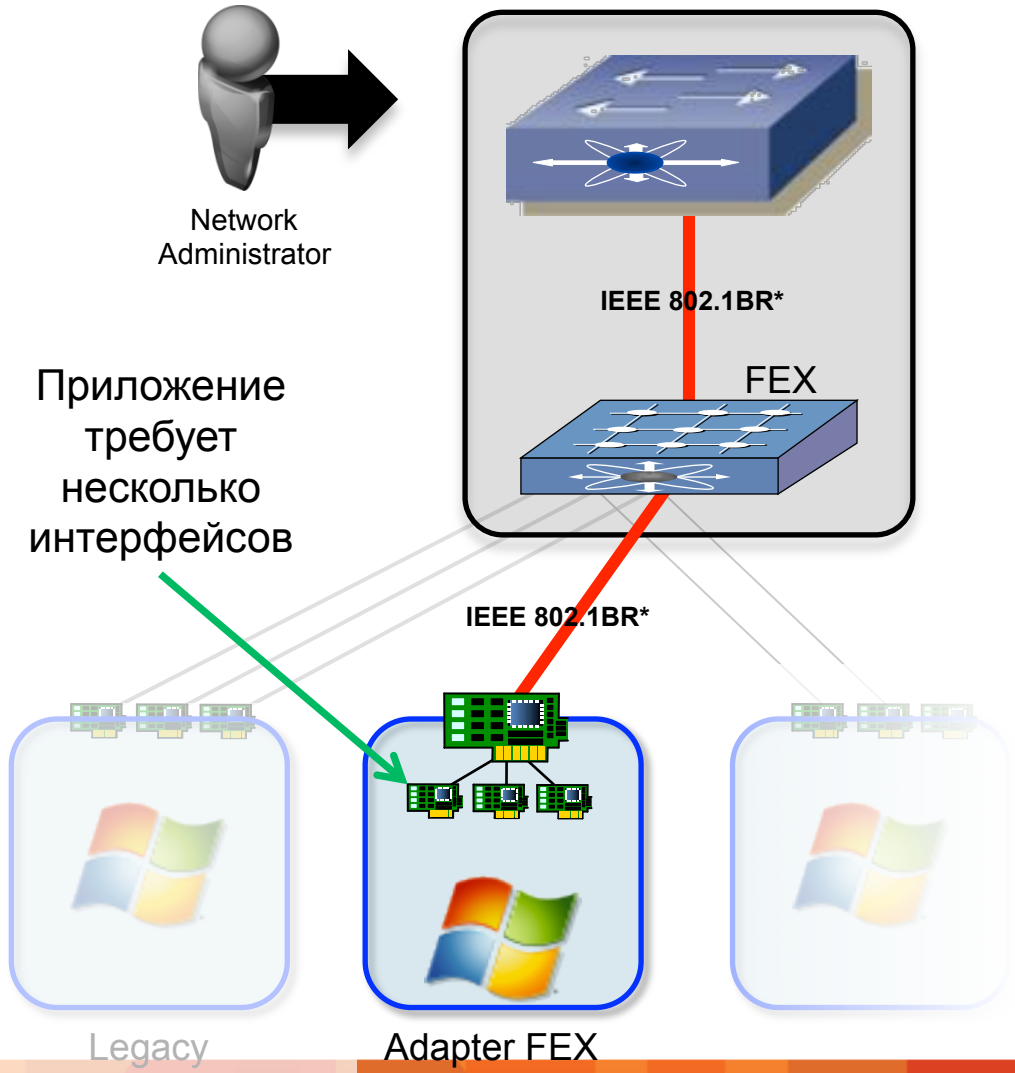
### Fabric Extender

- Консолидация управления сетью
- FEX является частью «родительского коммутатора»
- Использует пре-стандартную реализацию IEEE 802.1BR

*IEEE 802.1BR pre-standard

# Эволюция технологии Fabric Extender

## Распределённый коммутатор до уровня стойки, интерфейсов сервера и VM




# Единое устройство

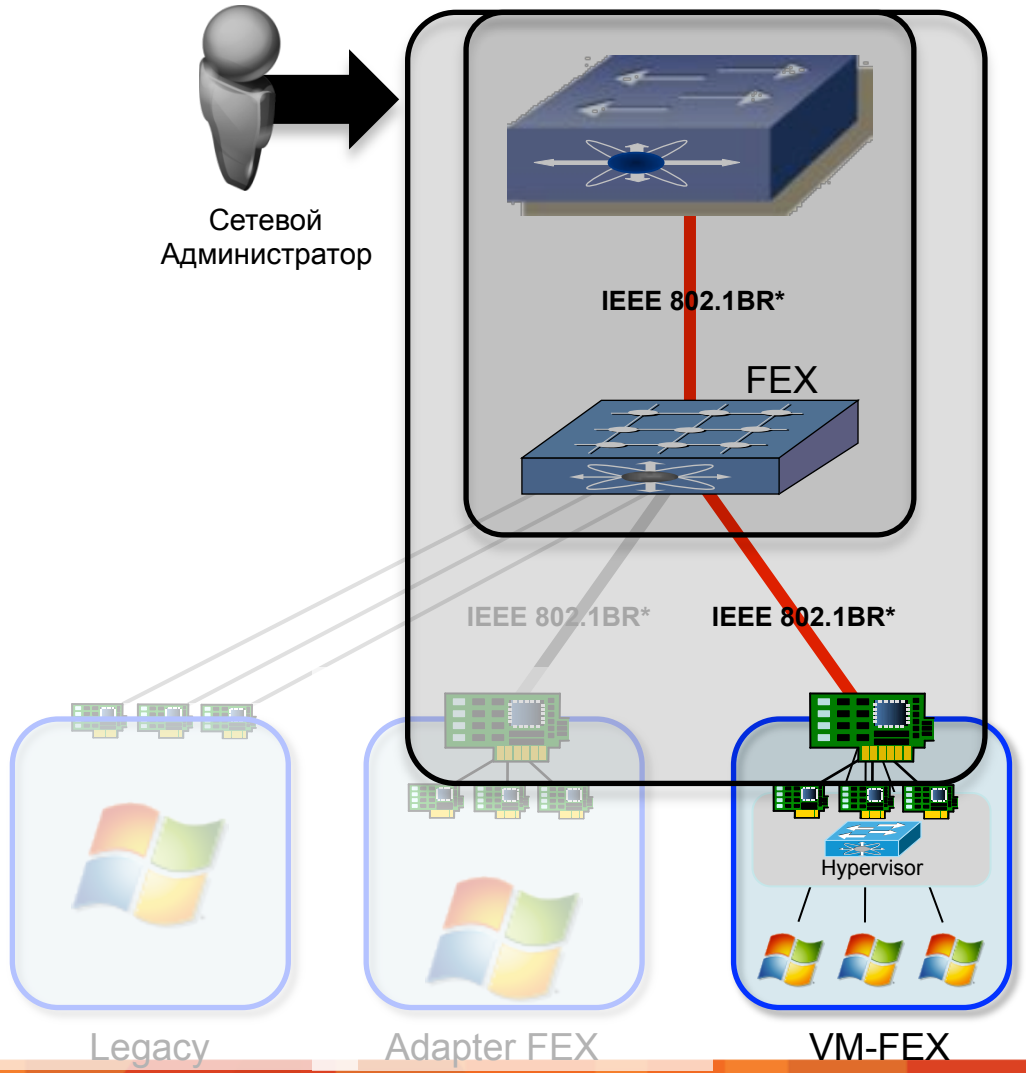
### Adapter FEX

- Консолидация многих 1GE интерфейсов в единое 10GE подключение
- Расширение сети внутрь сервера
- Использует пре-стандартную реализацию IEEE 802.1BR

*IEEE 802.1BR pre-standard

# Эволюция технологии Fabric Extender

## Распределённый коммутатор до уровня стойки, интерфейсов сервера и VM




# Единое устройство

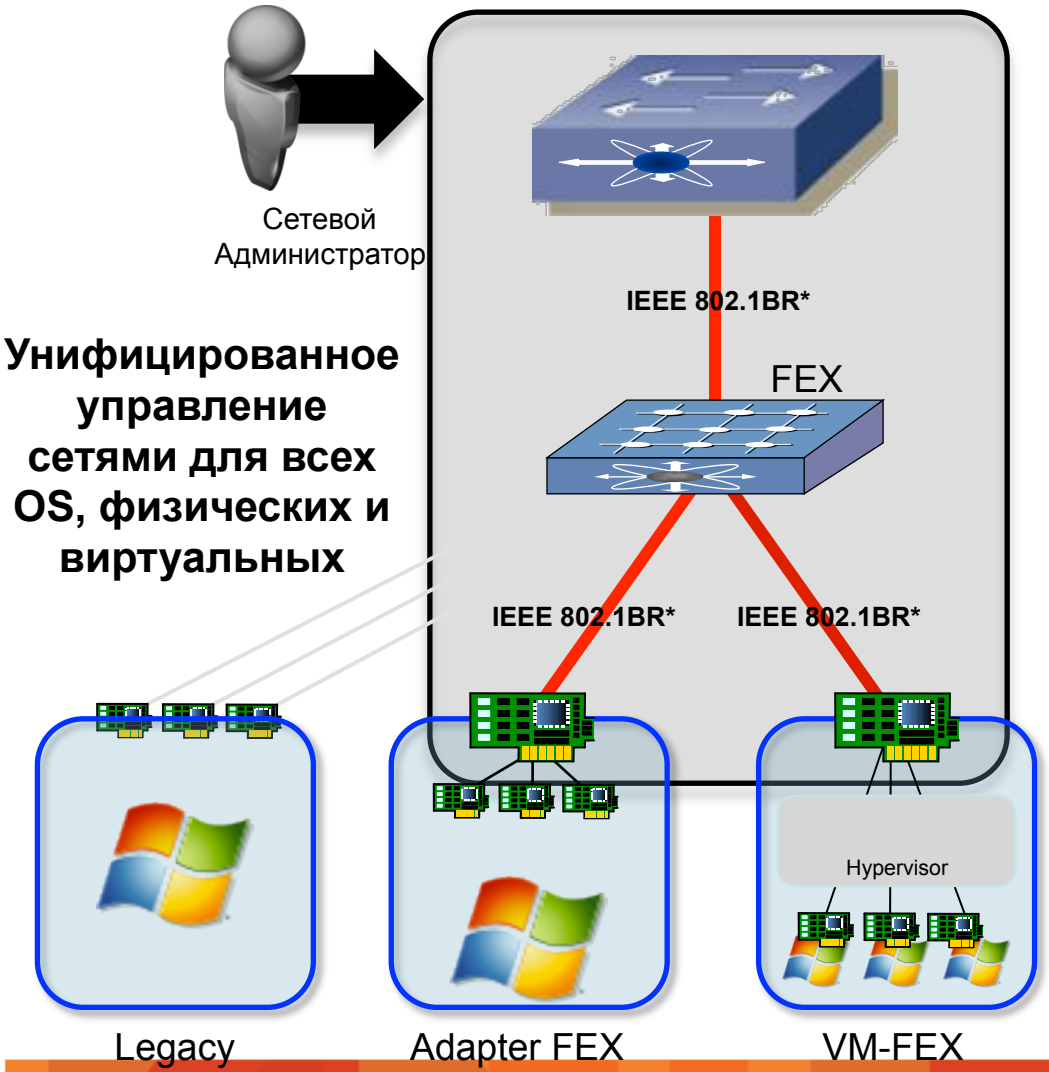
### VM-FEX

- Консолидация физической и виртуальной сети
- Каждая VM получает порт на распределённом коммутаторе
- Использует пре-стандартную реализацию IEEE 802.1BR

*IEEE 802.1BR pre-standard

# Эволюция технологии Fabric Extender

## Распределённый коммутатор до уровня стойки, интерфейсов сервера и VM




**Унифицированное управление сетями для всех OS, физических и виртуальных**

## Единое устройство

- •Порты коммутатора
- •Порты FEX
- •Виртуальные адаптеры
- •Виртуальные машины

### Fabric Extender

- Консолидация управления
- FEX выглядит линейной картой головного коммутатора

### Adapter FEX

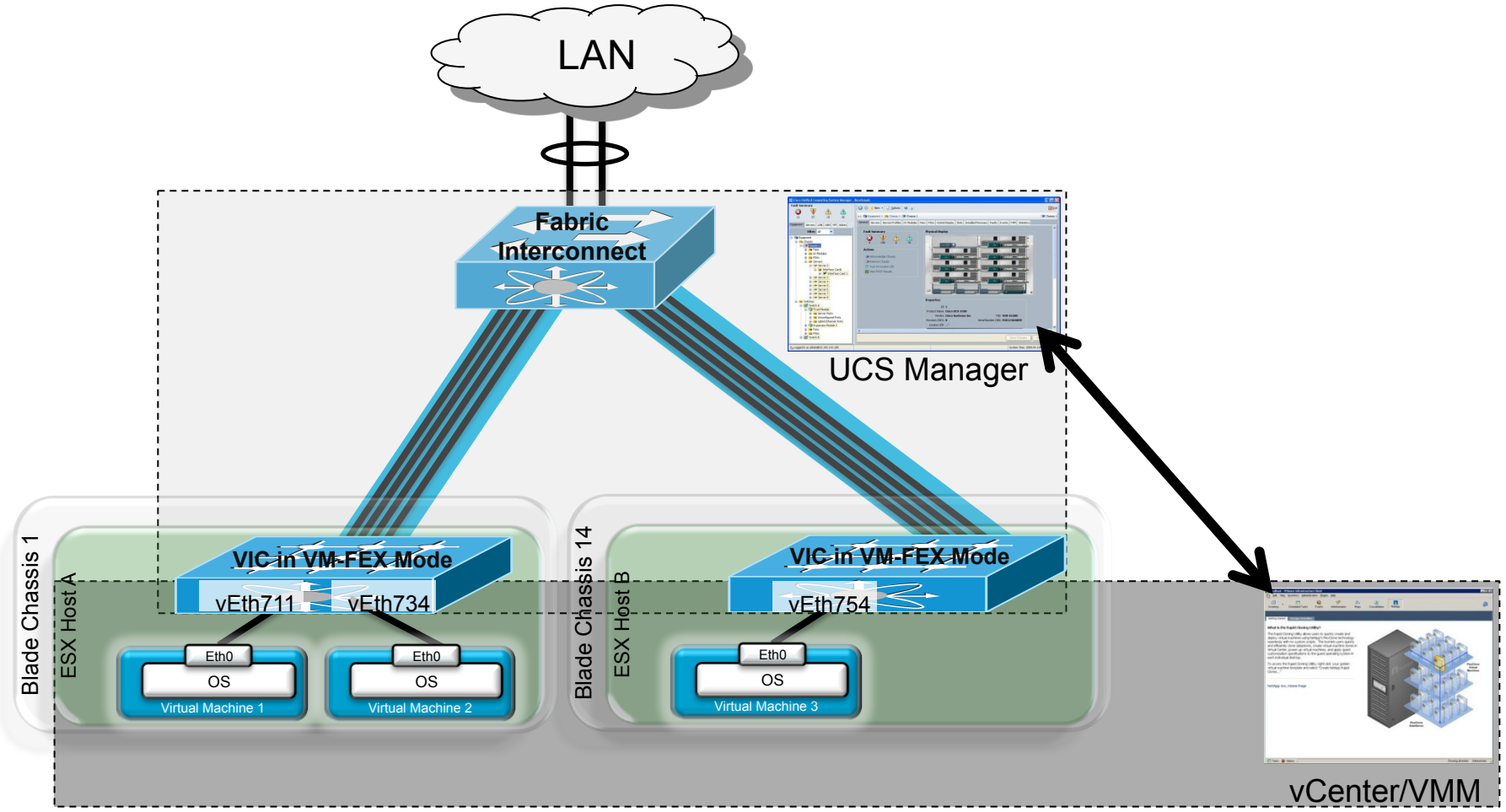
- Консолидация многих интерфейсов в единое 10GE подключение
- Расширение сети внутрь сервера

### VM-FEX

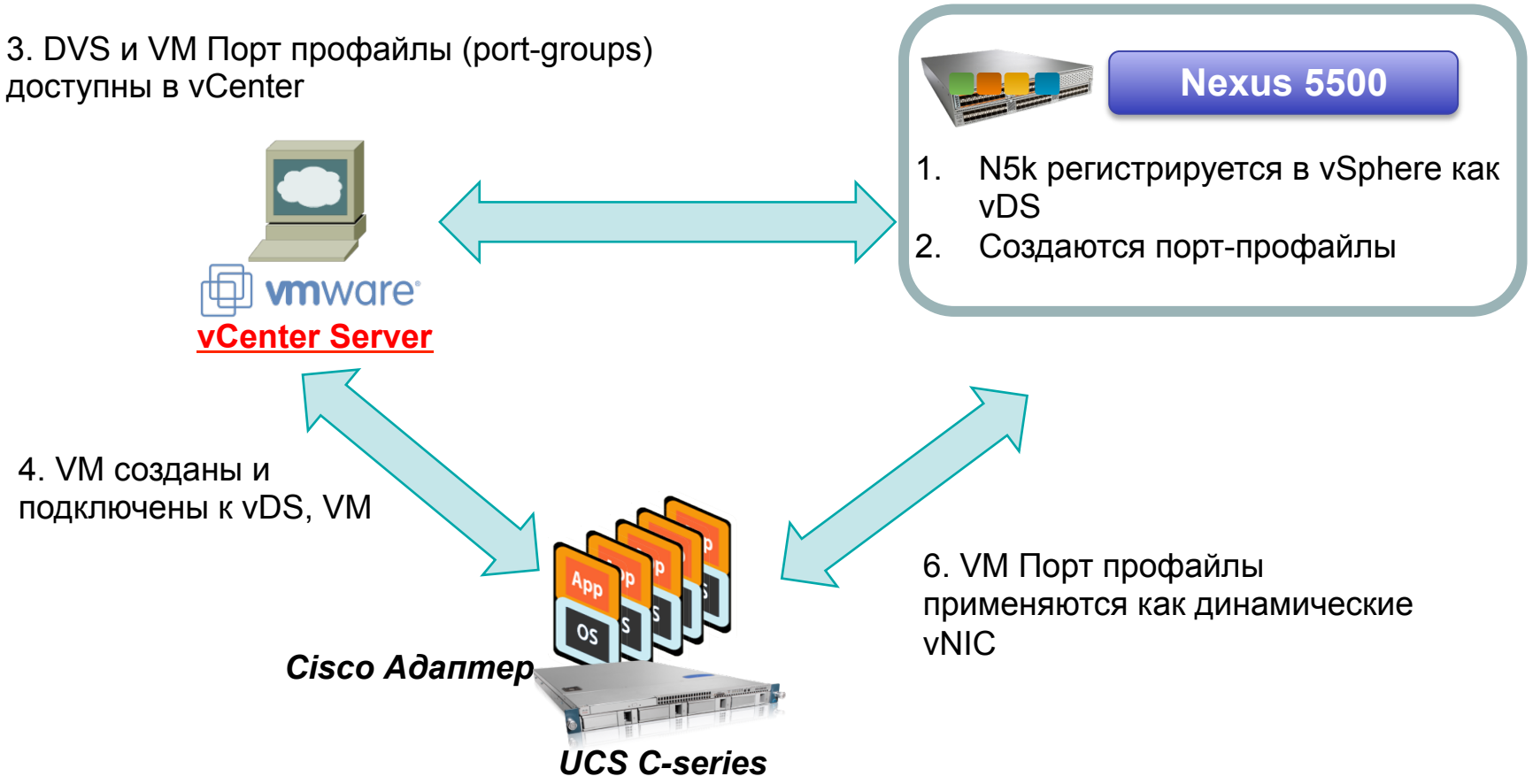
- Консолидация физической и виртуальной сети
- Каждая VM получает порт на распределённом коммутаторе

*IEEE 802.1BR pre-standard

# Cisco UCS
# Операционная целостность VM-FEX

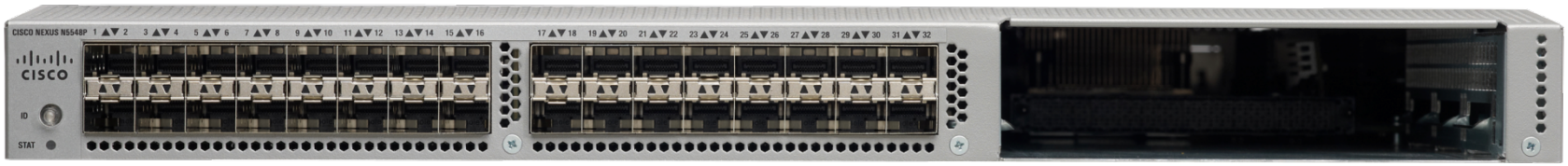


# Cisco Nexus
# Операционная целостность VM-FEX



# Cisco Nexus 5500

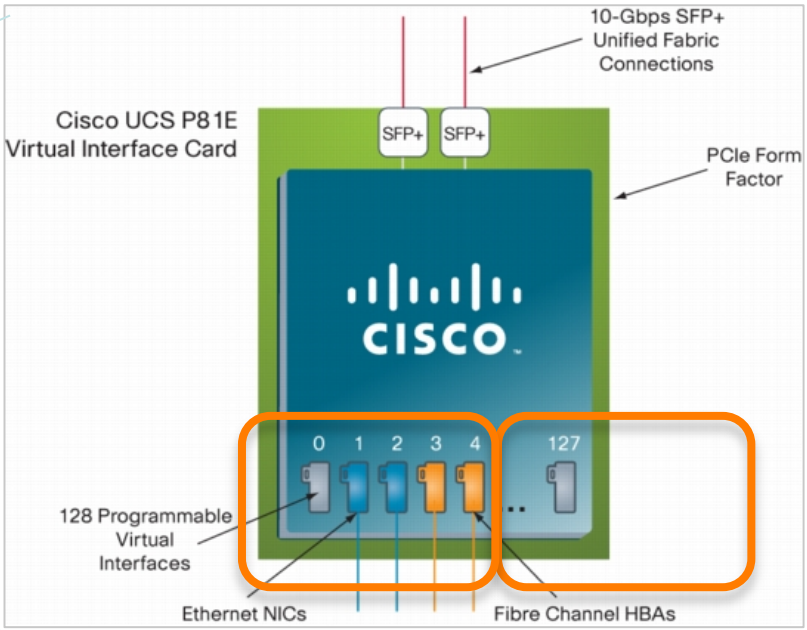
Первый коммутатор фабрики ЦОД с A-FEX и VM-FEX



Nexus 5548UP

Nexus 5596UP

# Cisco UCS Адаптер



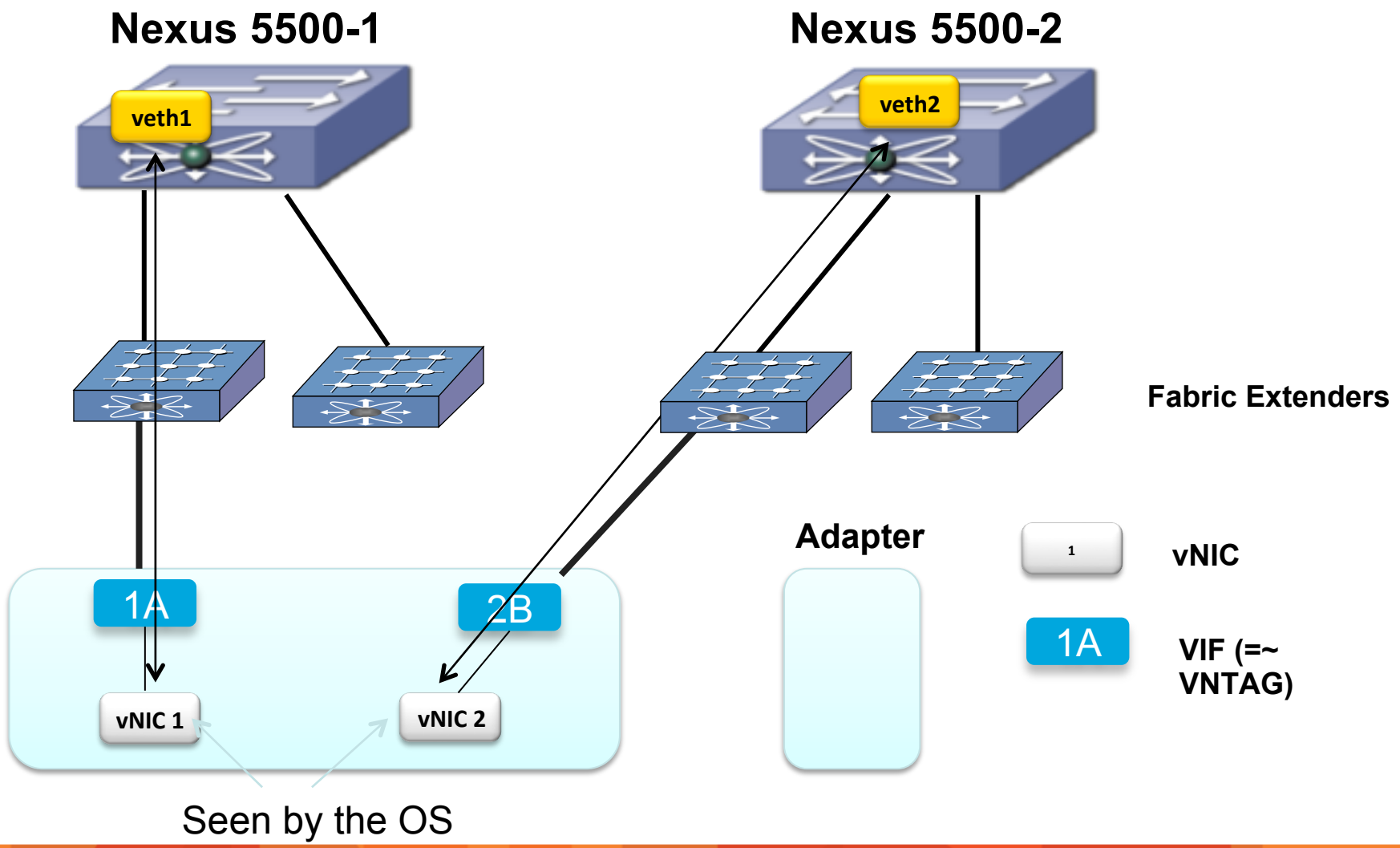

•Adapter Failover:
Полностью прозрачно для OS

•Нет транка к серверу
(улучшена безопасность и
масштабируемость)

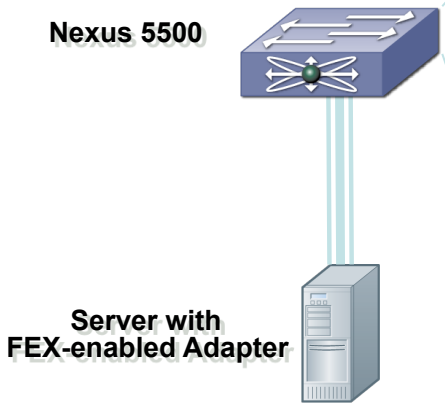
Статические vNIC
16 максимум A-FEX

Динамические vNIC
56-96-116 VM-FEX
для виртуализации

# Ассоциация vNIC с veth

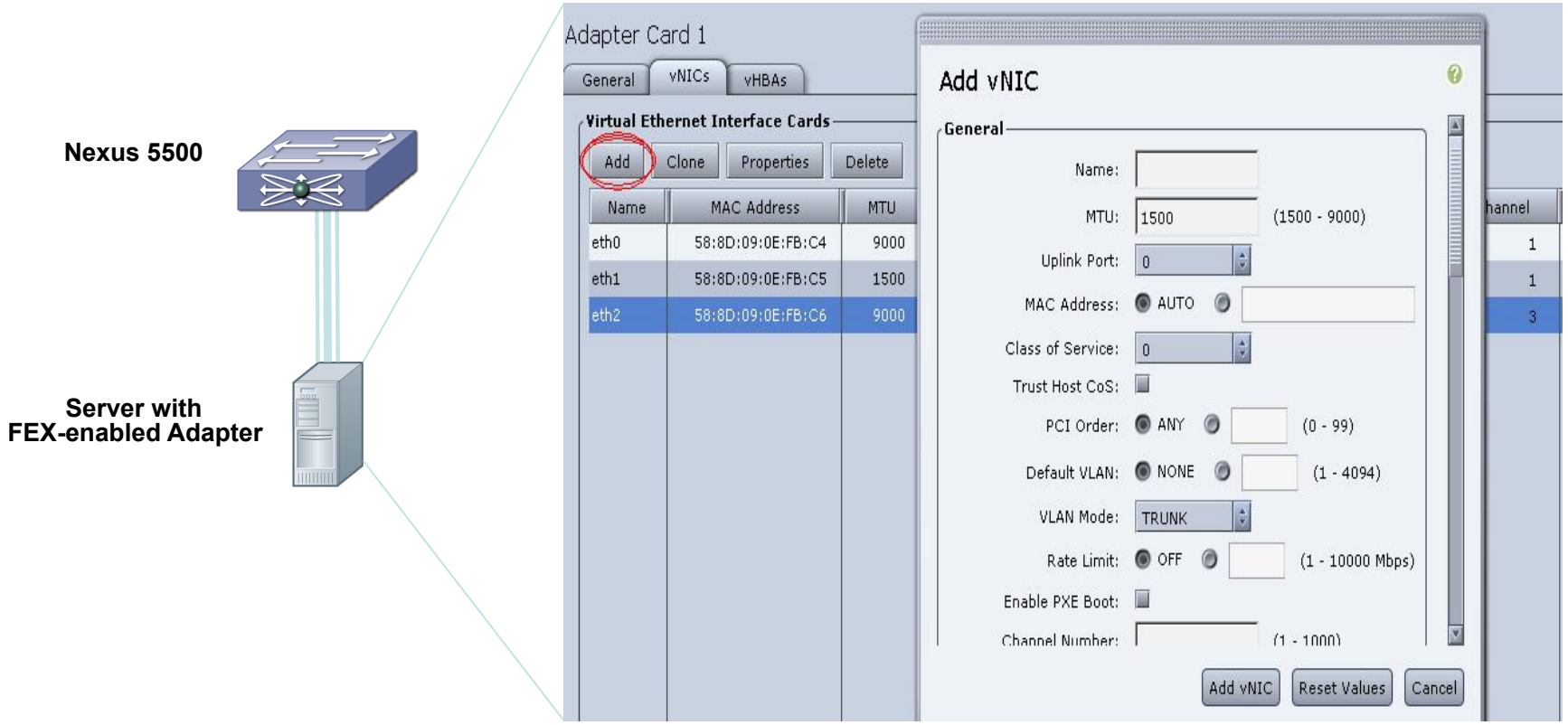


# Nexus 5500 Configuration

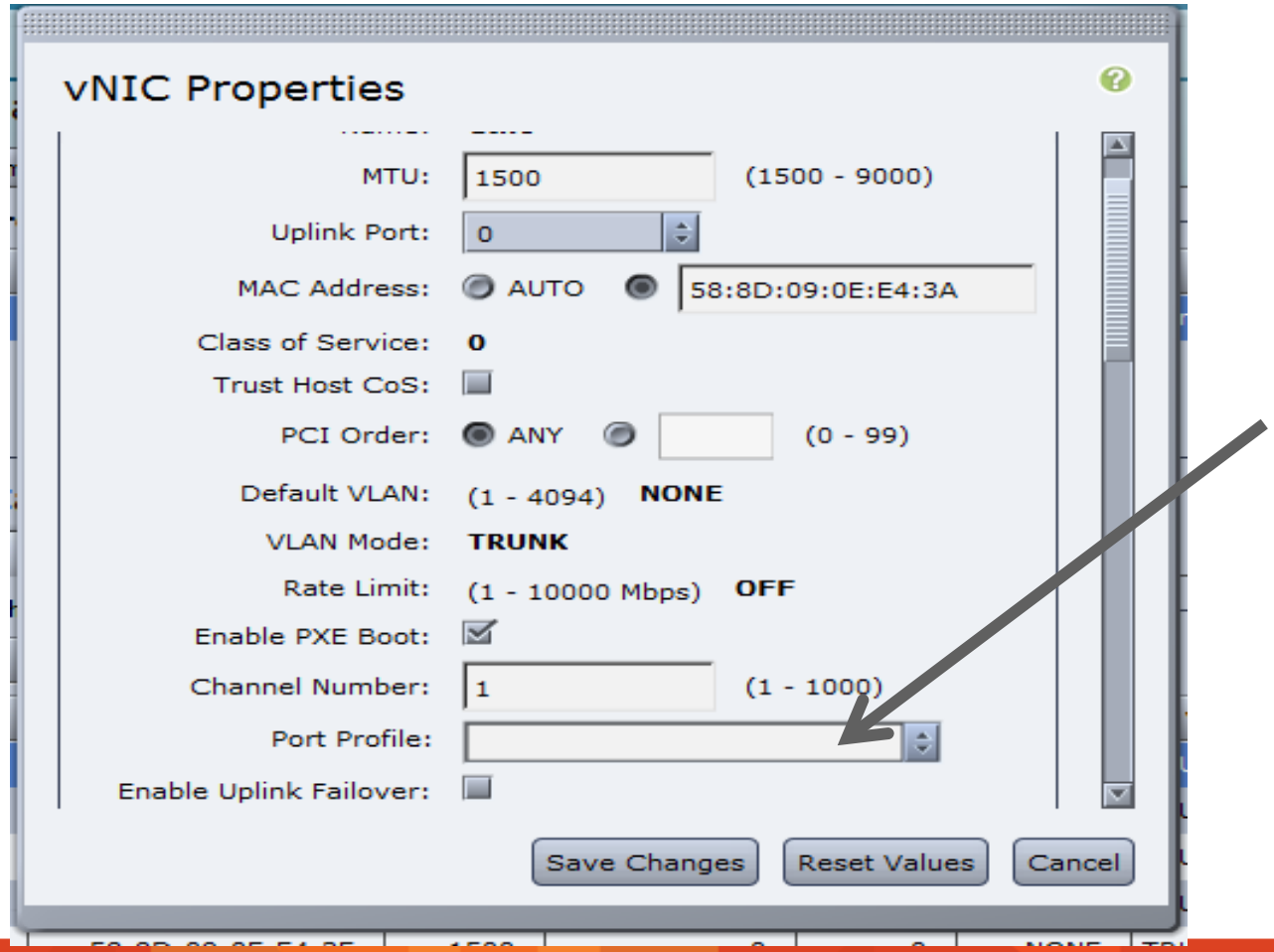



```
feature adapter-fex

port-profile type vethernet user_data
    switchport trunk allowed vlan 2-100
    switchport trunk native vlan 2
    switchport mode trunk
    state enabled

port-profile type vethernet user_management
    switchport access vlan 1
    state enabled

port-profile type vethernet user_backup
    switchport mode trunk
    switchport trunk allowed vlan 2-100
    switchport trunk native vlan 2
state enabled

interface Ethernet1/5
    description ucs_vic2/0
    switchport mode vntag
```

# Создание vNIC
## *Из CIMC или BIOS или OS-утилит*



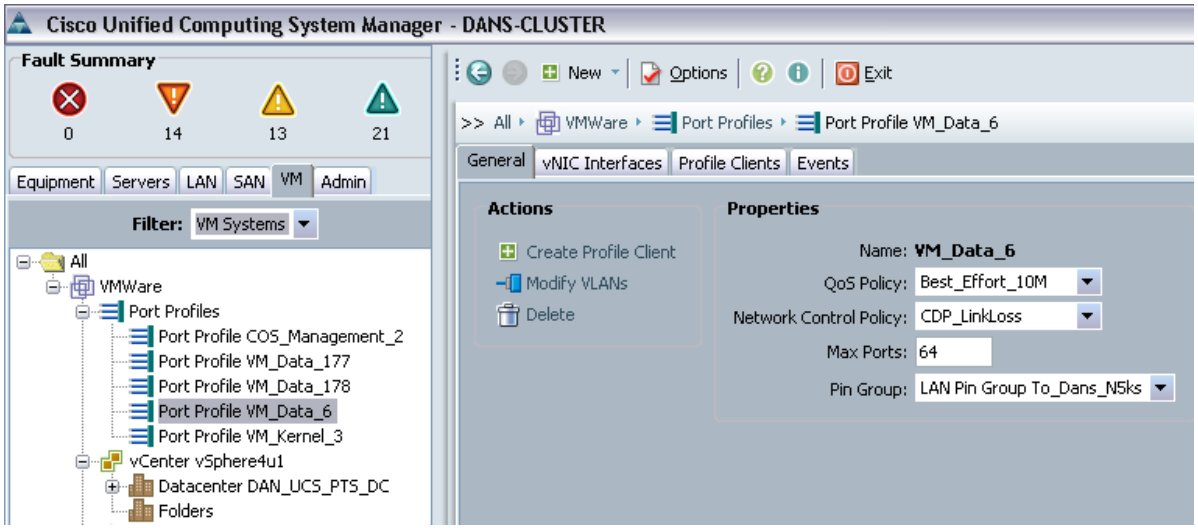
# Server Admin chooses the port-profile



# Профиль порта Cisco VIC в UCS

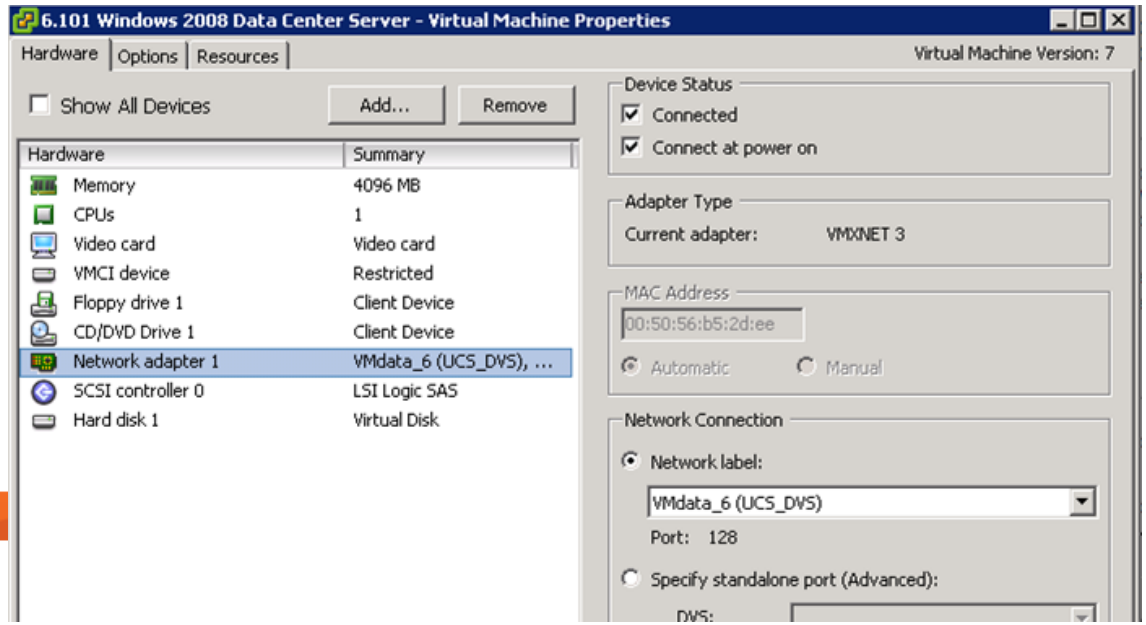
Администратор UCS

- Создаёт профиль порта
- Настраивает:
  - Структуру VLAN
  - QoS
  - Используемые аплинки
  - Сетевую политику




Администратор vCenter

- Применяет профиль порта к виртуальной машине



# Решения A-FEX и VM-FEX


CISCO UCSM — A-FEX, VM-FEX

CISCO — A-FEX, VM-FEX

BROADCOM — A-FEX

CISCO — A-FEX, VM-FEX

BROADCOM — A-FEX, VM-FEX

EMULEX — A-FEX, VM-FEX

QLOGIC — A-FEX, VM-FEX

Доступно Q4 CY 2011

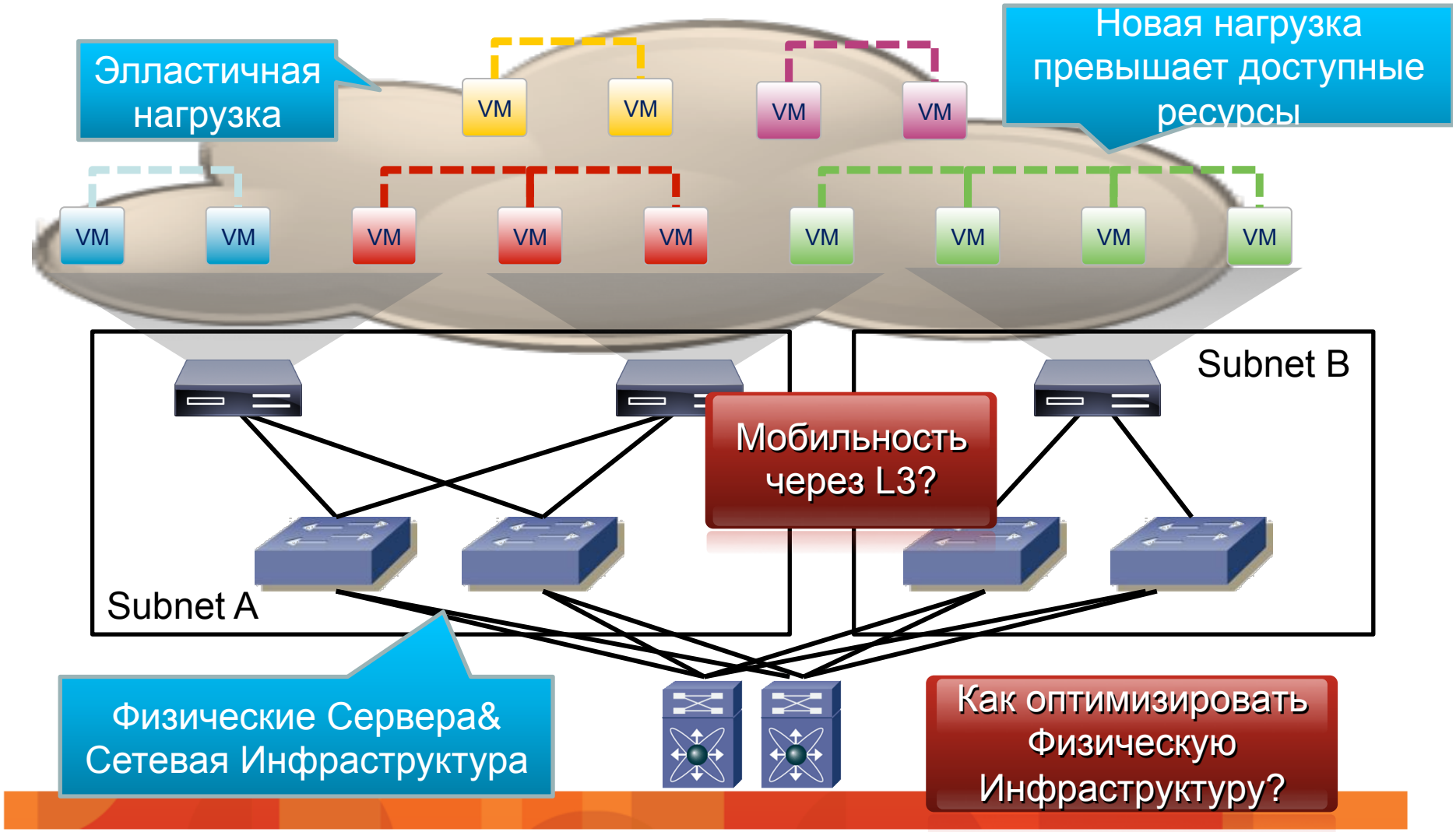
# Cisco Virtual Machine Networking Options

| Customer Need | Nexus 1000V | UCS VM-FEX | N5K VM-FEX |
|---|---|---|---|
| Server + Network management | | Y | |
| Heterogeneous Servers | Y | | Y (Future) |
| Heterogeneous 1st Hop Network | Y | | |
| Physical/Virtual Network Consolidation | | Y | Y |
| Feature Richness/ Velocity | Y | | |
| VM Density per Server | 216 VMs | 56 – 116* VMs | 96 * VMs |
| Hardware Performance | | Y | Y |

*Q4CY11

# Интеграция с Облачной инфраструктрой vCloud Director

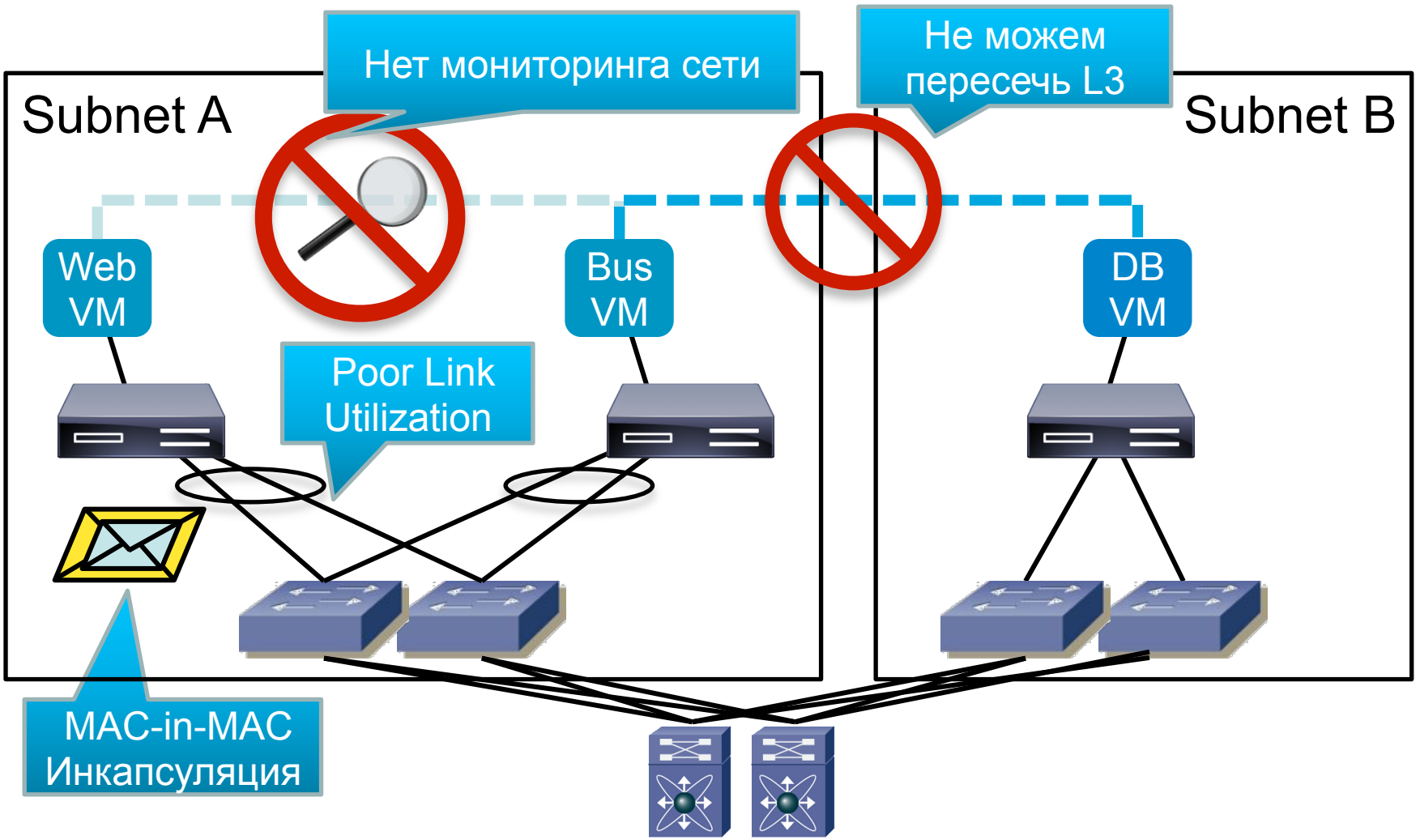
# Облако в Физическом ЦОД

# Сетевая Изоляция в vCloud Director

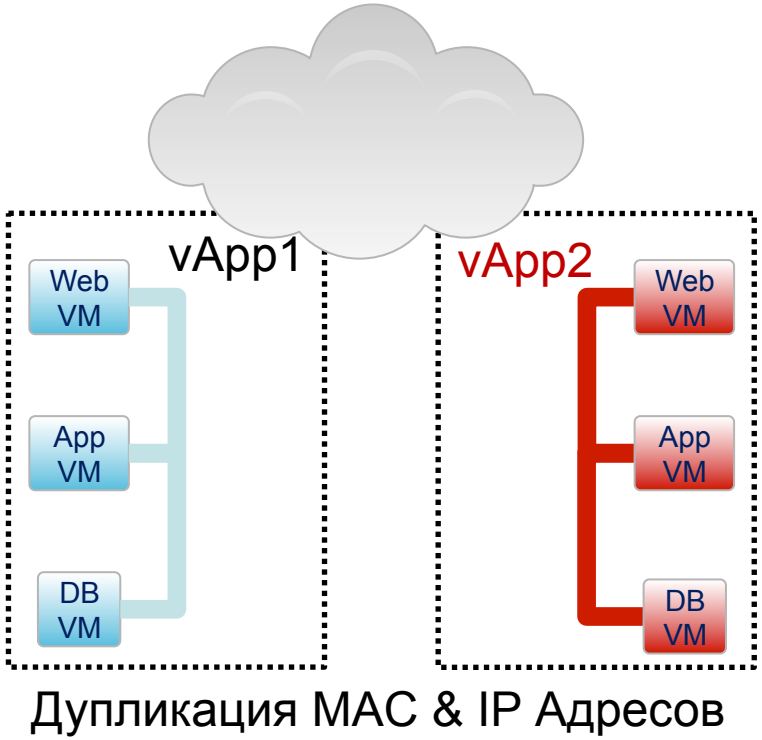
- Традиционные сервера имеют уникальные MAC и IP
- vCloud Director дуплицирует MAC и IP для VM в vApps
- Может появится блок VM с дублированными сетевыми атрибутами что вызовет сбой приложения
- Необходима сетевая изоляция

# Сетевая Изоляция в vCloud Director



# Virtual eXtensible LAN—VXLAN

- **Решение: VXLAN**
  - Миллионы LAN сегментов
  - Безопасность и Масштабирование
  - Мобильность vApp между ЦОД и Облаками
- **VXLAN - дружественный к сети**
  - Балансировка аплинков(port channel)
  - Поддержка NAT; контроль безопасности




**Submitted to IETF**
Support by Cisco, Vmware, others…

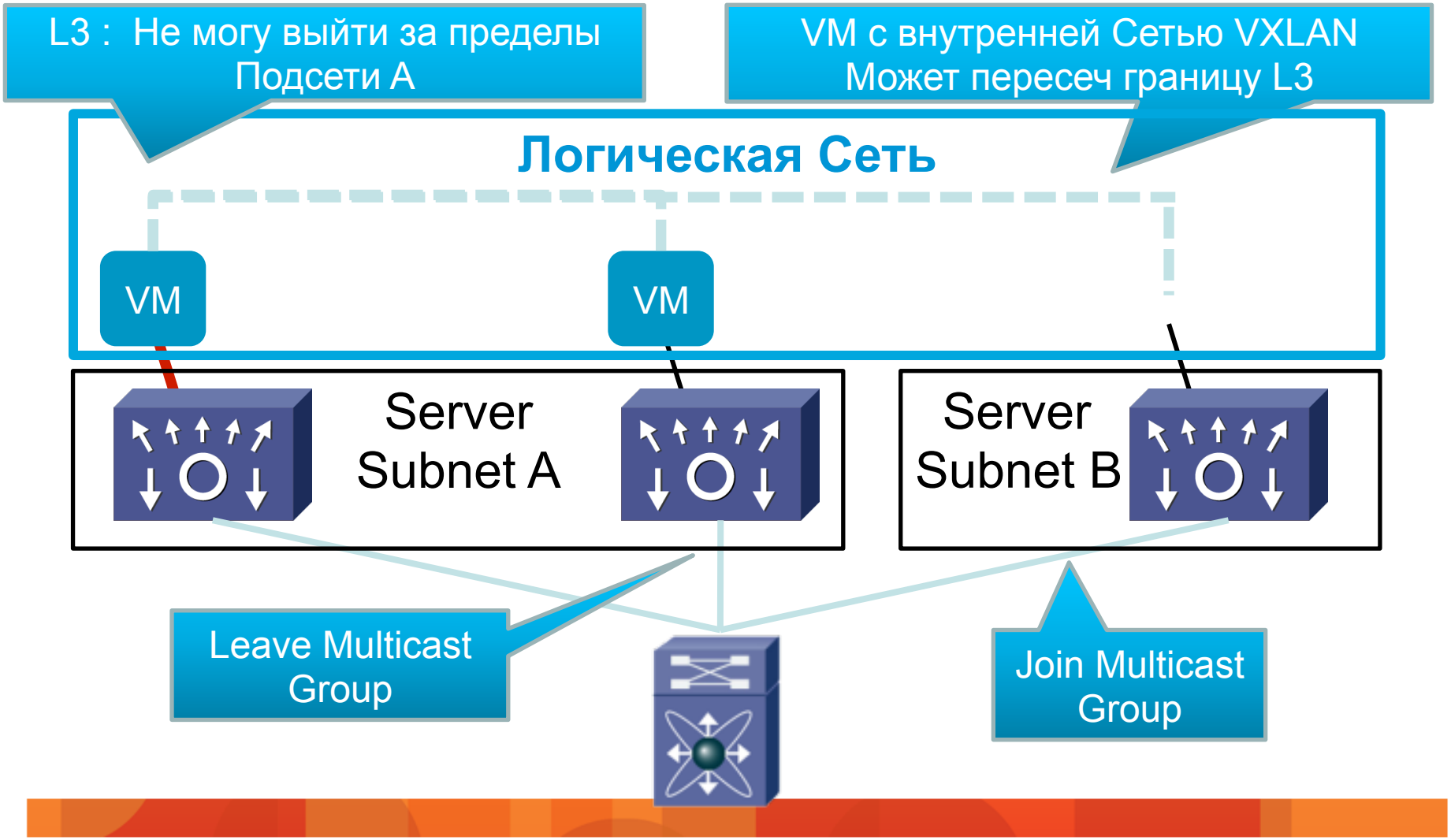
**Nexus 1000V & vCD September Beta**

**VXLAN IETF Draft:** http://datatracker.ietf.org/doc/draft-mahalingam-dutt-dcops-vxlan/

# Cisco и Vmware VXLAN: Virtual Extensible Local Area Network


- Ethernet в IP сети
  - L2 фрейм инкапсулирован в UDP
  - Общий формат Cisco и Vmware
- 24 бит на Идентификатор Сети VXLAN
  - 16 M логических сетей
- Туннель между Nexus 1kv VEM
  - VM подключена к портам доступа
  - VM НЕ ВИДИТ Network ID
- VXLAN может пересекать L3
- IP мультикаст для L2 бродкаст/ мультикаст

# Миграция VM с VXLAN через L3



Cisco Expo 2011

# Спасибо!

Просим Вас оценить эту лекцию.
Ваше мнение очень важно для нас.

Онлайн-анкеты: www.ceq.com.ua

innovate together

# Оцени контент Cisco Expo и получи приз!

Призы ждут всех, кто:

- посетил 2 и более дней конференции
- заполнил общую анкету
- заполнил 5 и более сессионных анкет
- заполнил анкеты по 2 и более плановым демо

Онлайн-анкеты доступны на сайте www.ceq.com.ua.

Анкеты также можно заполнить, воспользовавшись терминалами в зоне общения на первом этаже.