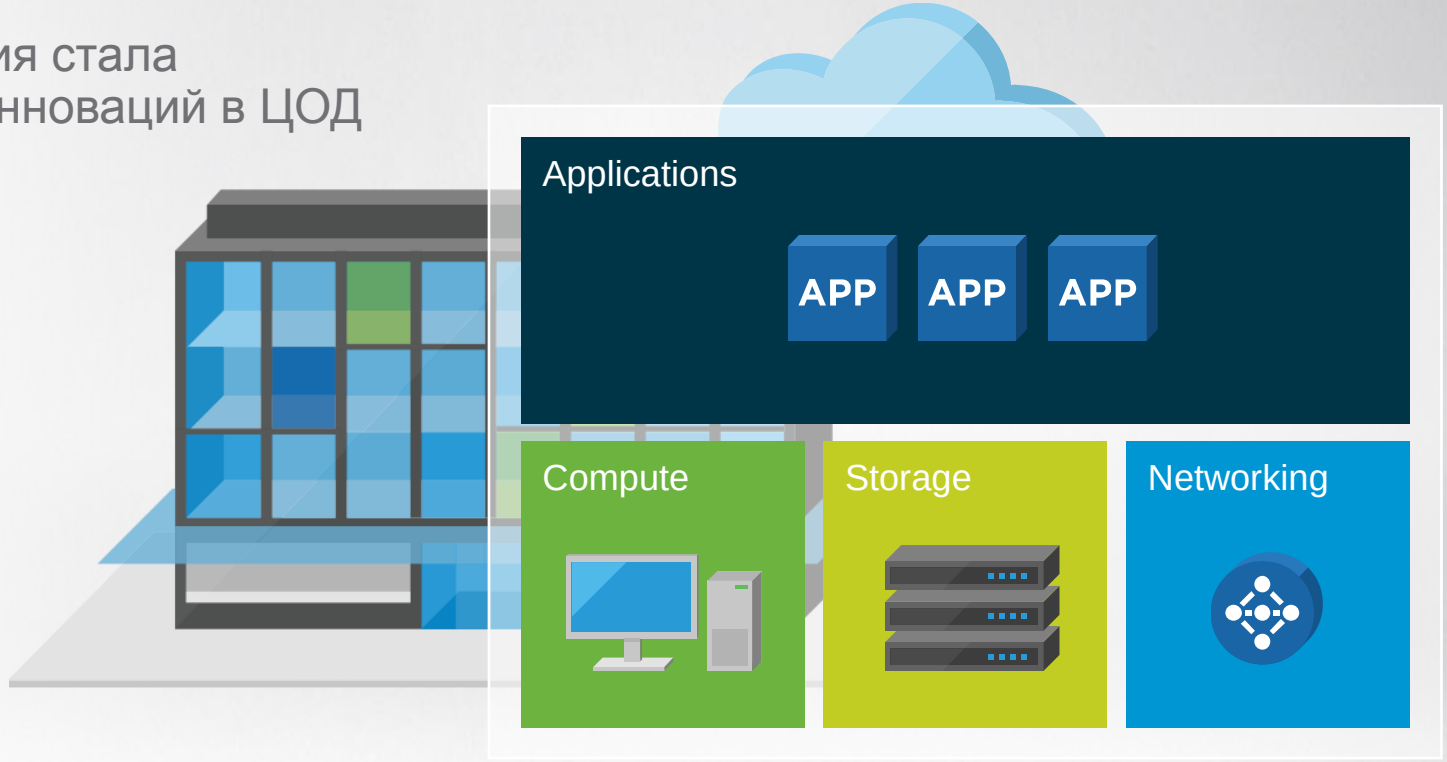
# Программно-определяемая безопасность

Александр Кренев
akrenev@vmware.com

© 2015 VMware Inc. All rights reserved.

# Компоненты типового ЦОД

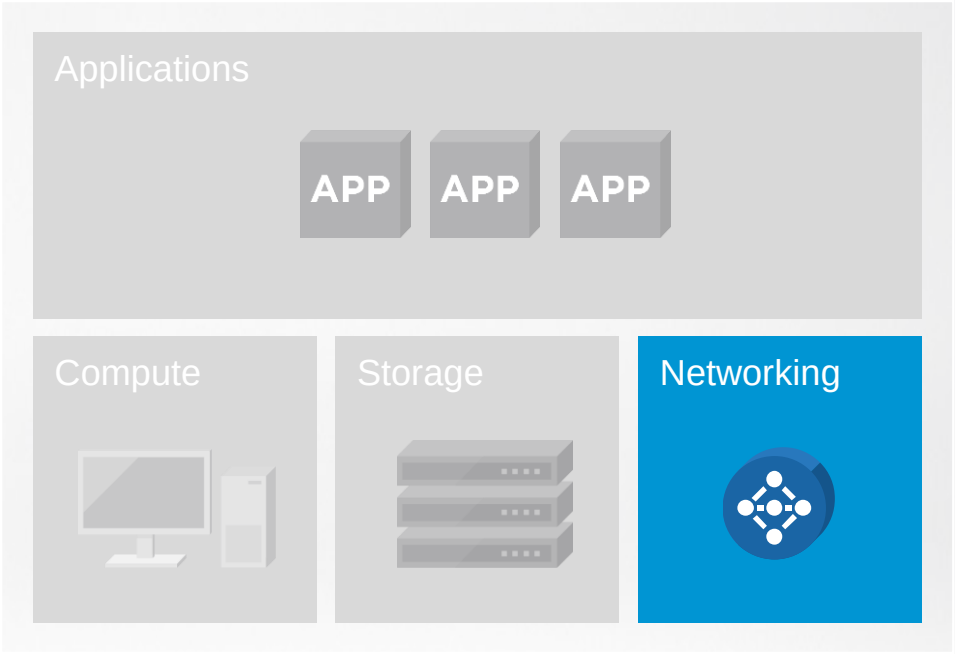
Виртуализация стала
двигателем инноваций в ЦОД



# Сети оставались привязанными к оборудованию

Отсутствие виртуализации сети существенно усложняет развитие современных ЦОД:

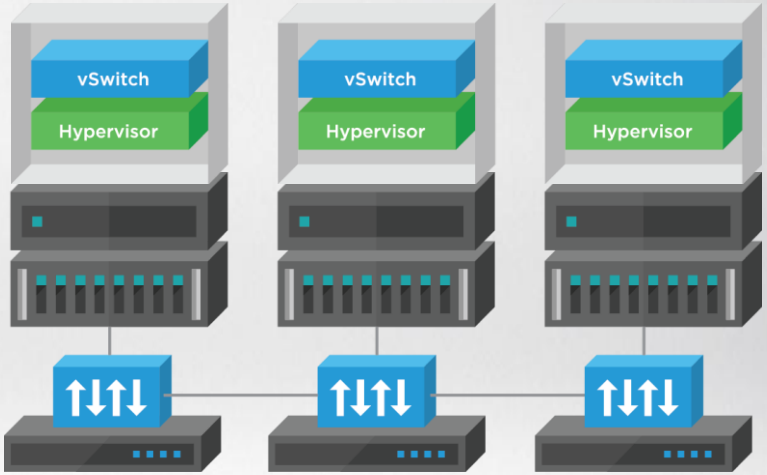
- Низкая скорость развертывания и внесения изменений
- Безопасность ограничена сетью
- Архитектура и функции сетевых устройств не меняются с 80-х гг.



# Сетевая виртуализация с NSX

Важнейший компонент для программного ЦОД

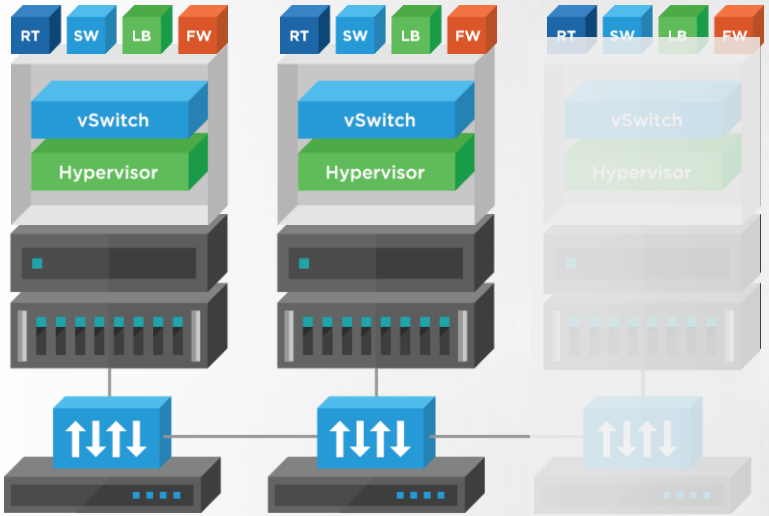
- Уровень виртуализации
- Существующее или новое оборудование: сеть, СХД, серверы

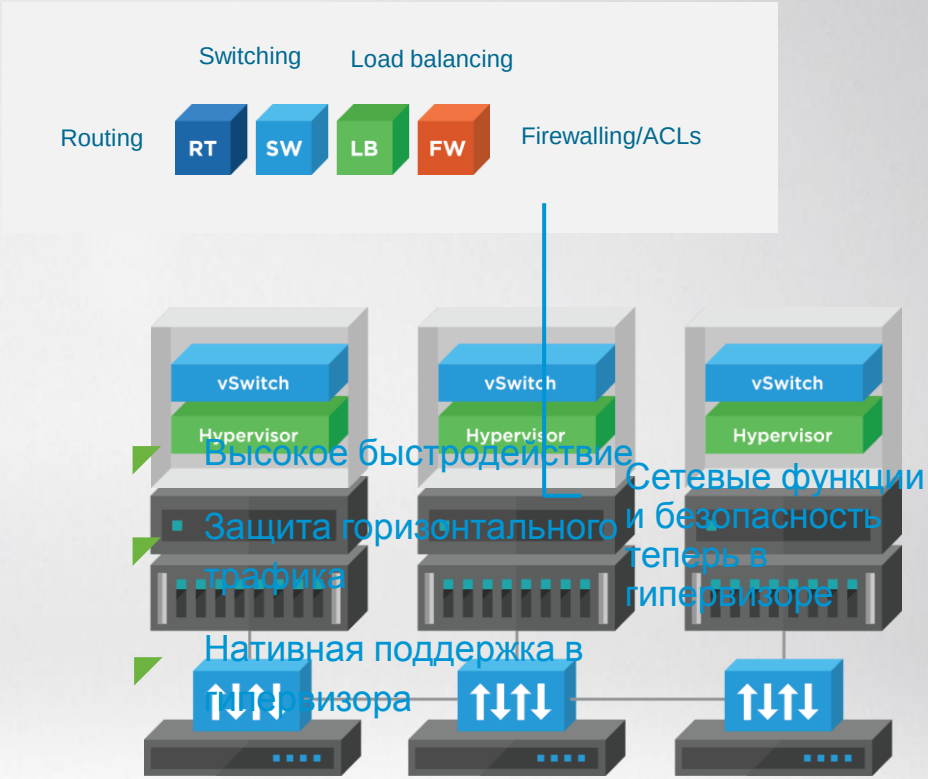





vmware

# Сетевая платформа нового поколения

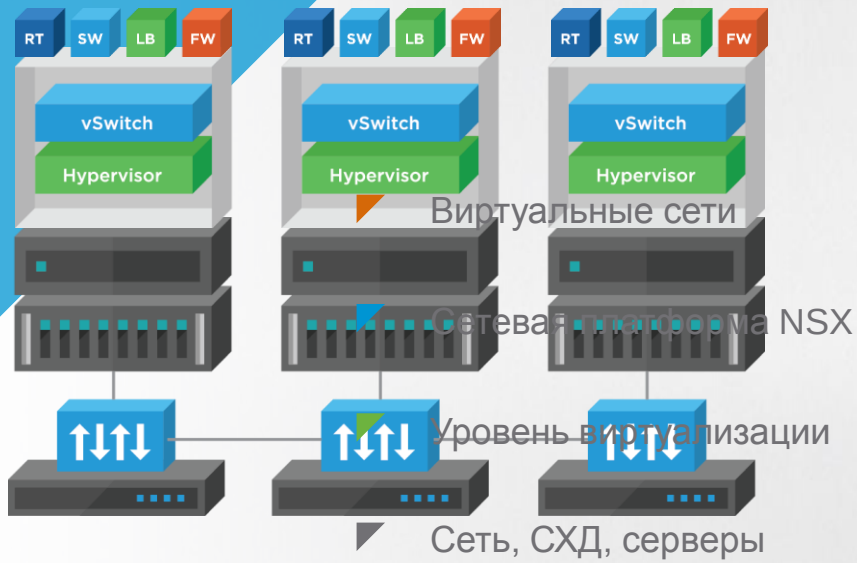





vmware

# Сетевая виртуализация с NSX

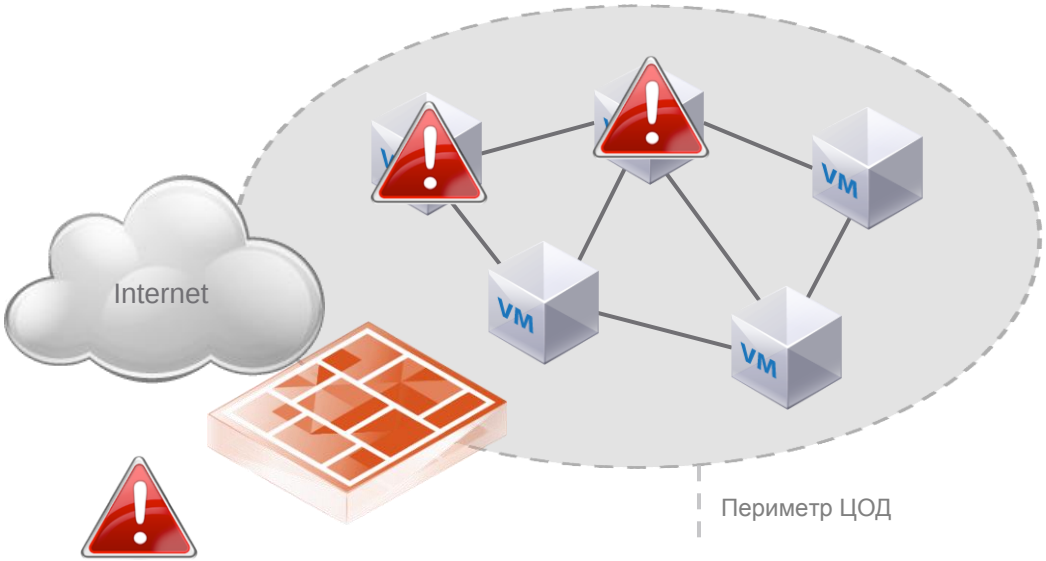


vmware

# Основные причины инцидентов в ЦОД

## Свободный обмен данными

Низкий (или отсутствующий) контроль внутри ЦОД



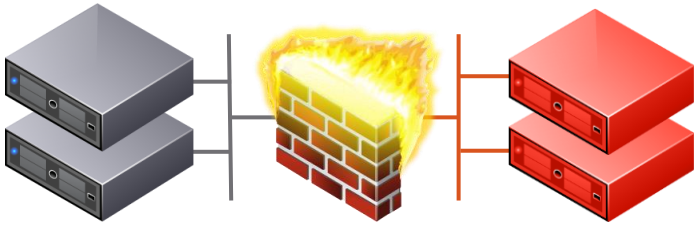
Низкоприоритетные, «забытые» серверы становятся целью атакующего

После проникновения злоумышленник свободно перемещается по сети

Информация может собираться месяцами

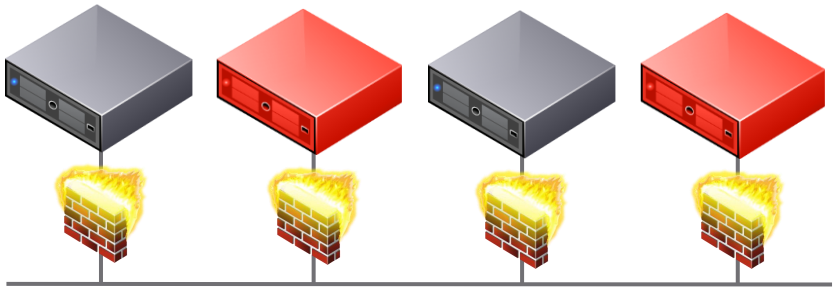
# Защита периметра vs. защита каждого сервера

## Традиционный подход



- Защита сегментов, а не серверов
- Инцидент в сегменте — под угрозой все серверы
- Инцидент на сервере — под угрозой весь сегмент
- При перемещении сервера защита теряется

## Распределенный МСЭ

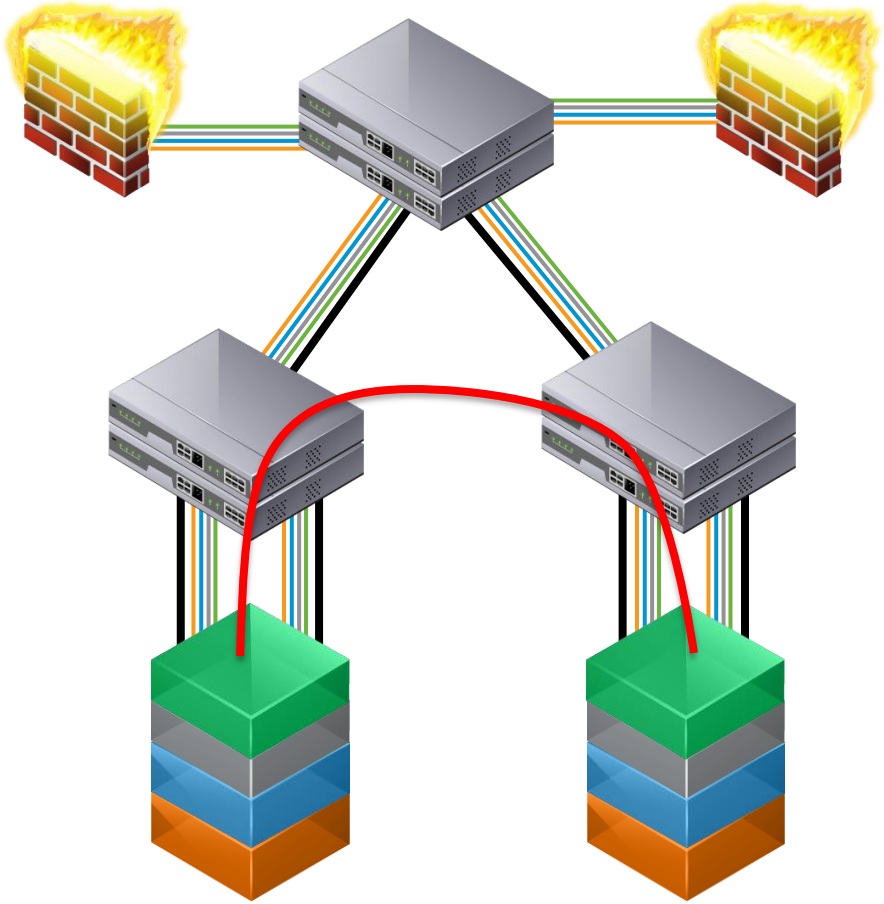


- Защищен каждый сервер
- Защита сервера от остальной сети и наборот
- Сетевая сегментация не требуется для защиты серверов
- При перемещении сервера перемещается и МСЭ

# Сложность #1: Ограничения сети

Необходимо направлять ВЕСЬ трафик к централизованному МСЭ

- Нужно связать каждый сервер с МСЭ
- каждое изменение требует настройки сетевого оборудования
- весь трафик направляется в одну точку – сложность масштабирования
- Каждый сегмент требует отдельный VLAN/интерфейс на МСЭ



**Безопасность не должна быть привязана к физической сетевой инфраструктуре**

# Сложность #2: Управление правилами

Подход №1

- Стараемся использовать максимально точные правила
- При этом внесение изменений будет крайне медленным

Подход №2

- Используются менее точные правила (упрощение) и группировка сетей
- Приводит к старому сегментному подходу

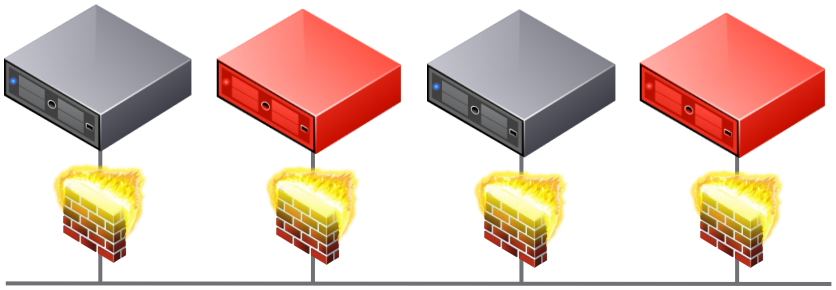
<u>Требуемое решение:</u>
Правила МСЭ должны быть абстрагированы, позволяя автоматизировать создание индивидуальных правил на интерфейсах

| |
|---|
| any -> IP1:80 allow<br>eng -> IP1:445 allow<br>eng -> IP1:3389 allow<br>… |
| any -> IP2:80 allow<br>sale -> IP2:445 allow<br>sale -> IP2:3389 allow<br>… |
| any -> IP3:80 allow<br>field -> IP3:445 allow<br>field -> IP3:3389 allow<br>… |
| any -> IP4:80 allow<br>ext -> IP4:445 allow<br>ext -> IP4:3389 allow<br>… |

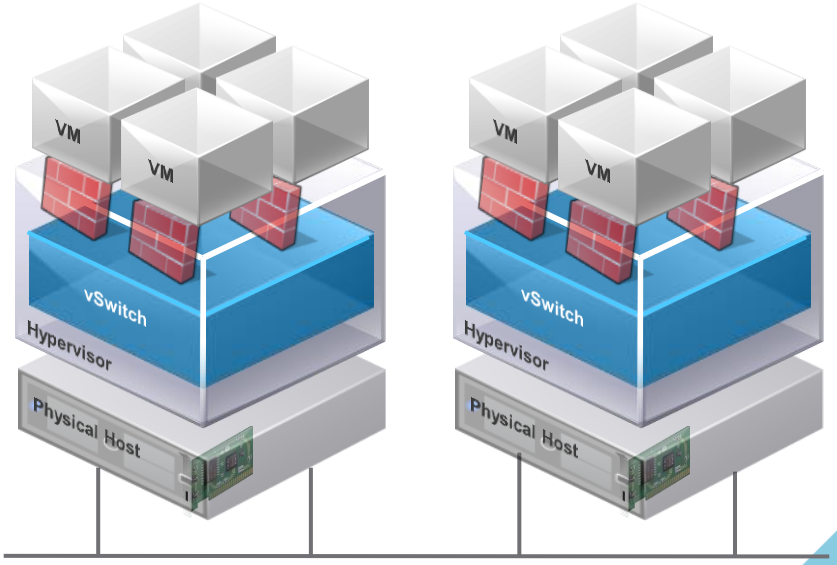
# Решение – Часть 1: распределенный МСЭ для каждого сетевого порта

- МСЭ на каждом vNIC независимо от физической сети
- Встроен в гипервизор — не часть гостевой ОС
- Трафик не перемещается на периметр для инспекции
- вместо этого инспекция перемещается к источникам трафика
- Сетевая инфраструктура не мешает безопасности

Дано:



Решение



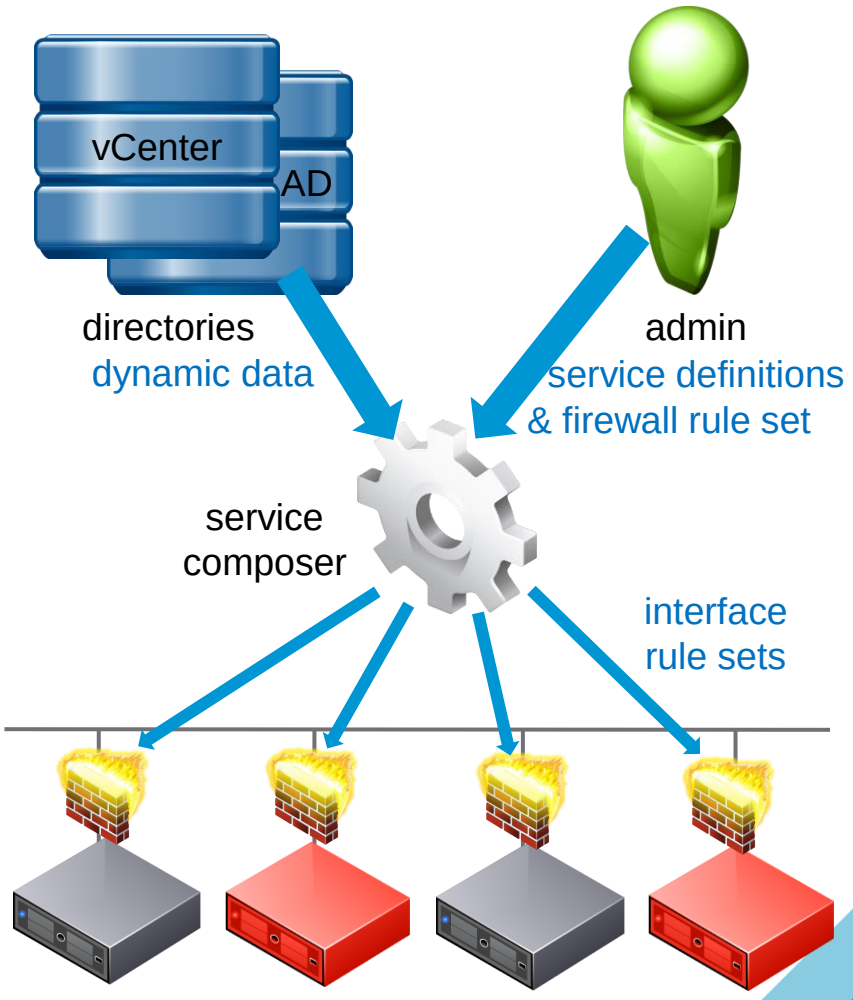
# Решение – Часть 2: Автоматизация правил

Условия для автоматизации:

- Динамические источники данных — представляют изменяющиеся состояния системы
- Уровень абстракции — верхнеуровневое определение способ реакции на изменения

В NSX DFW мы используем:

- vCenter & Active Directory — источники информации об объектах и пользователях
- “Service Composer” в NSX динамически транслирует политики в таблицу правил на интерфейсах ВМ



# МСЭ для каждого виртуального порта

- Невозможно обойти
  - Поскольку МСЭ работает на уровне vNIC, его невозможно обойти, даже если переключить ВМ в другой виртуальный коммутатор
- Невозможно атаковать МСЭ
  - Распределенный МСЭ не имеет интерфейсов в сетях ВМ, не является частью гостевой ВМ
- Высокая производительность
  - Благодаря работе на уровне ядра, распределенный МСЭ дает более 15 Гбит/с на каждый сервер виртуализации.

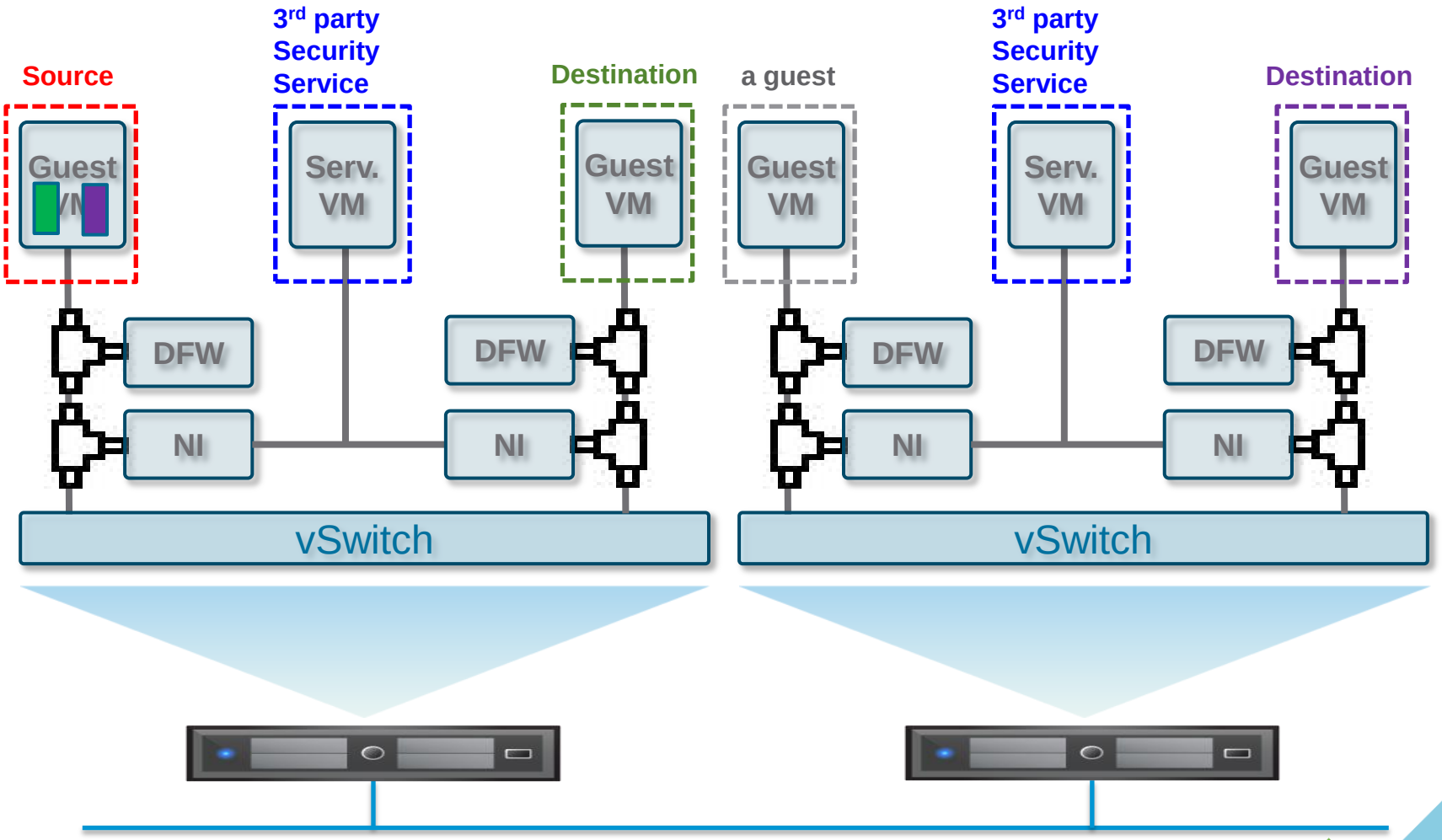
# Service Composer: возможности

- Distributed Firewall (DFW)
  stateful L4+ firewall (L4+ = “Application Layer Gateway”);
- Guest Introspection (GI)
  проверки гостевых систем: RAM/File System
- Network Introspection (NI)
  L7/L7+ (L7 = protocol; L7+ = content): IDS/IPS, NGFW, URL Filtering

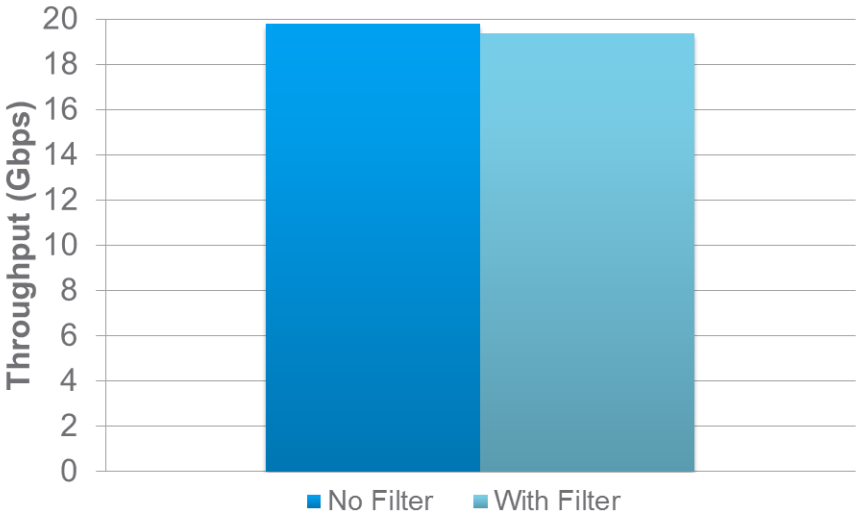
Особенности реализации:

- Не требуется установка компонентов/драйверов в гостевые ОС
- Данные инспектируются локально на каждом сервере-гипервизоре

# Интеграция DFW и партнерских решений



# Быстродействие распределенного МСЭ

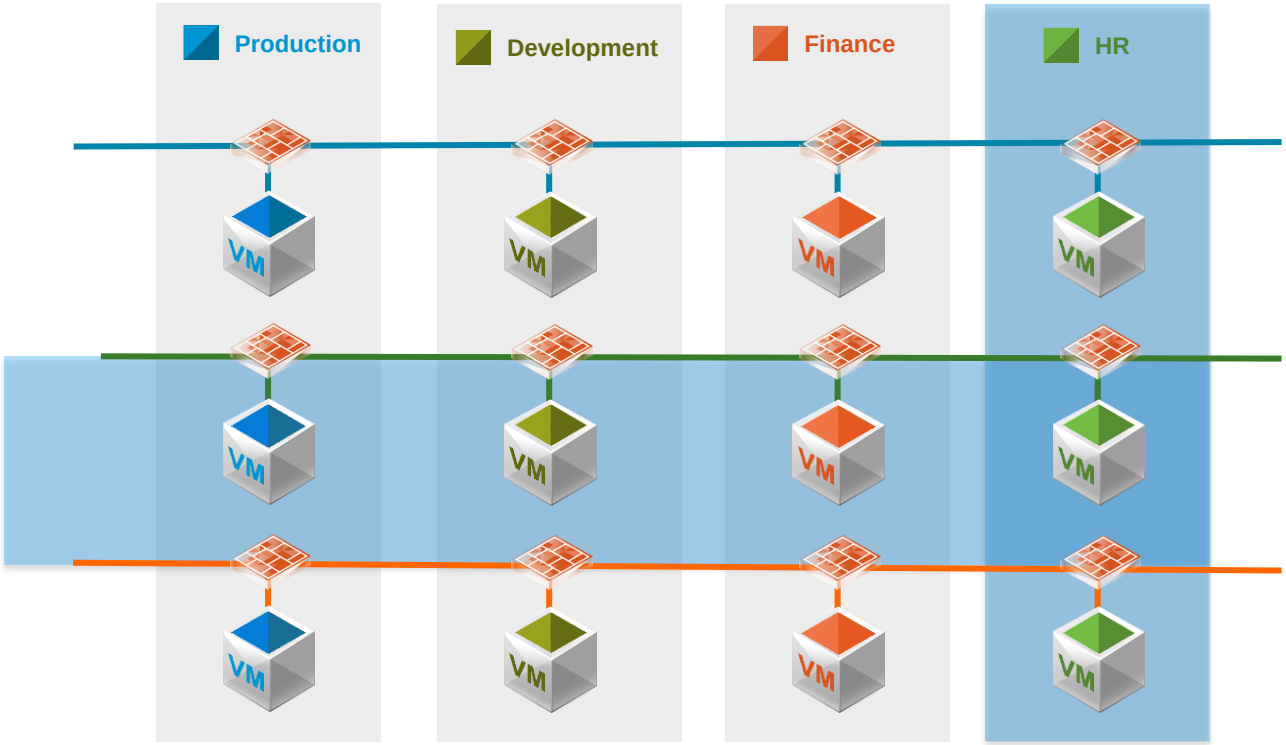



*~20 Гбит/с на каждый сервер виртуализации*

*Более 80000 CPS на сервер при 100+ правил*

Накладные расходы на CPU не превышают единицы %

# Сетевая безопасность становится проще для реализации



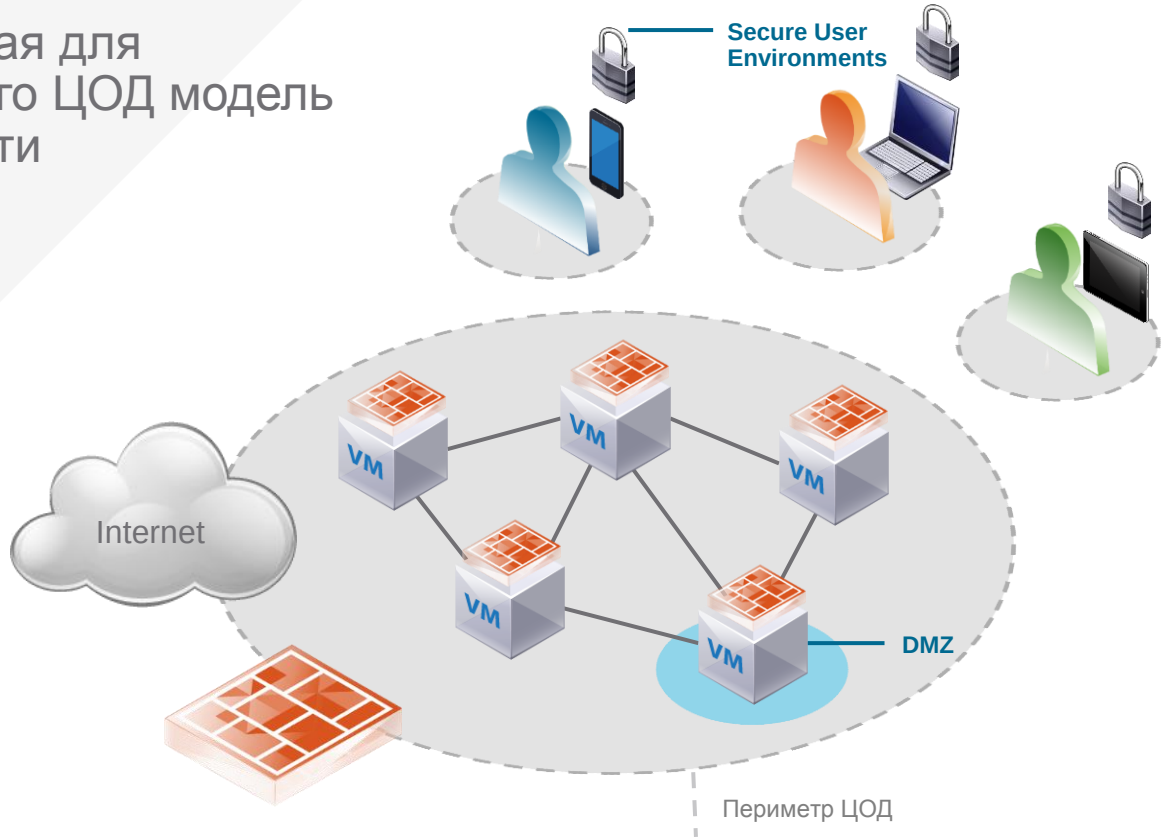

- Политики больше не привязаны к физической топологии и сочетаются с логическими группами ВМ
- Каждая ВМ может быть периметром безопасности
- Микросегментация предотвращает распространение угрозы

# Партнерская экосистема NSX

| Application delivery services | Security | Visibility & operations | Physical to cloud |
|---|---|---|---|
| APP | | | |
| f5 | HYTRUST Cloud Under Control, Symantec, Check Point Software Technologies Ltd., FORTINET, paloalto Networks, vmware NSX, TREND MICRO, RAPID7, intel Security | ARKIN, tufin, NETSCOUT, riverbed, Gigamon, EMC² | hp, cumulus networks, juniper networks, DELL, BROCADE, ARISTA |

# Безопасность в виртуальном ЦОД

Естественная для виртуального ЦОД модель безопасности



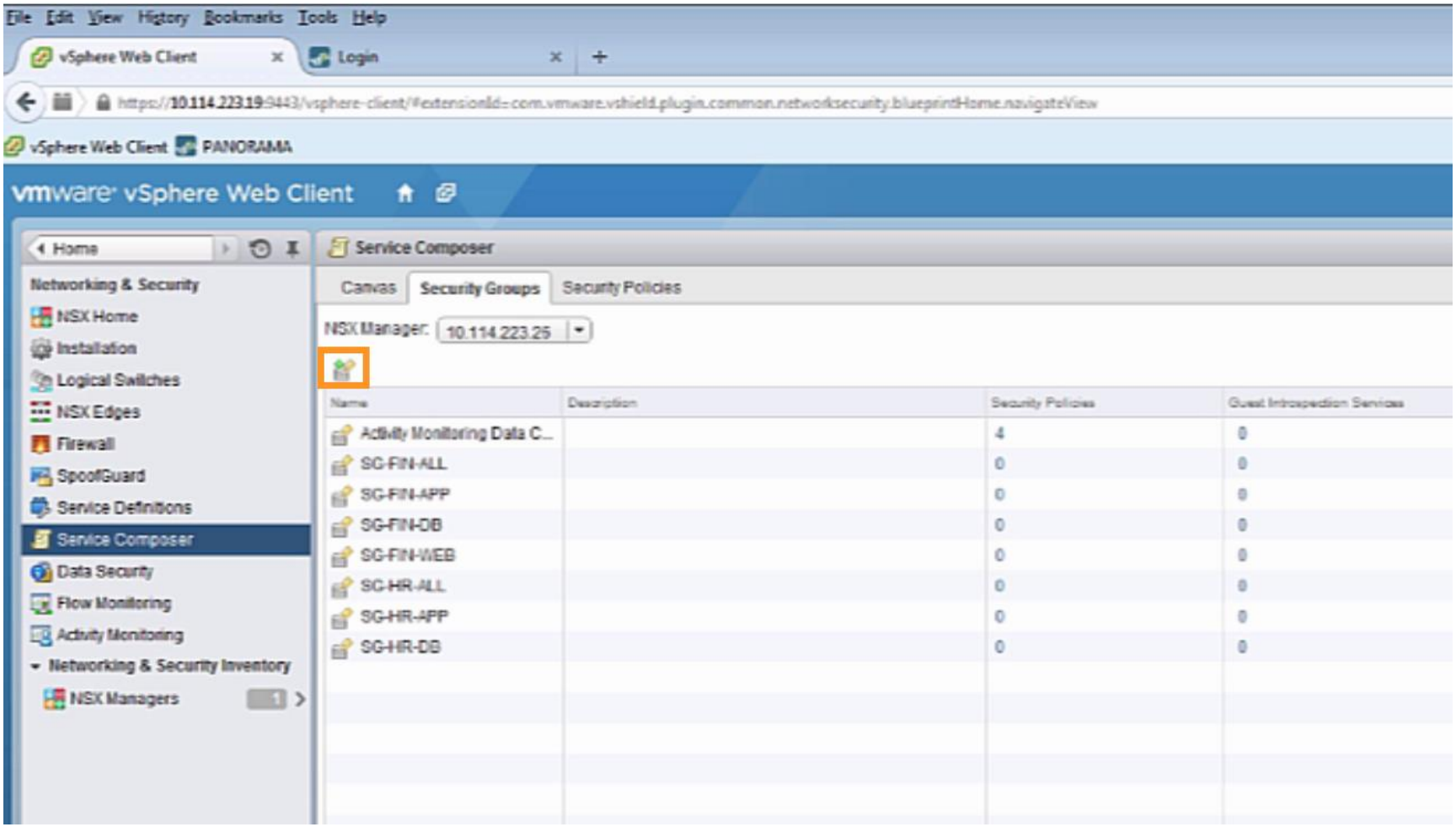

**Преимущества**

Безопасная инфраструктура существенно дешевле

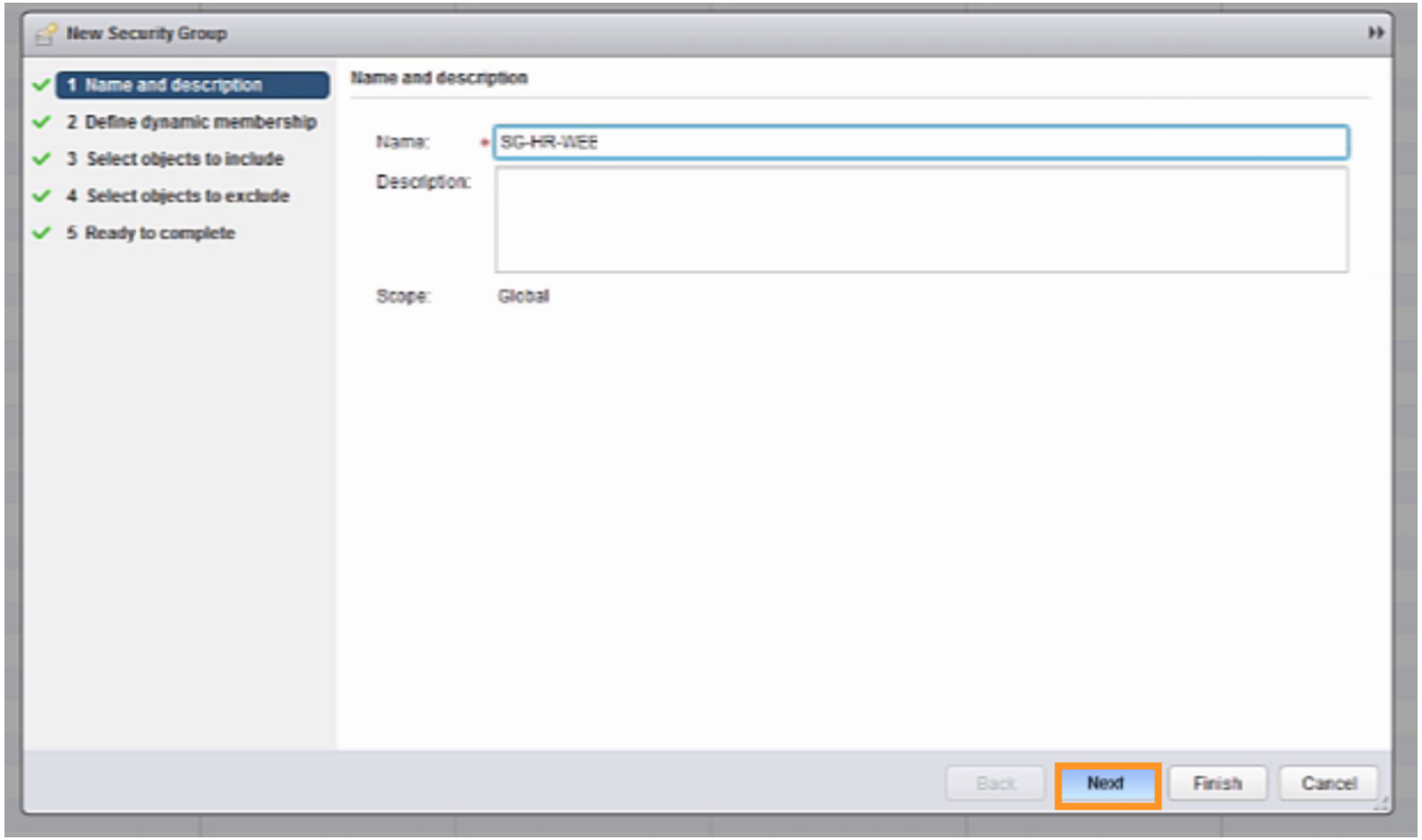
**Упрощение политик**

**Логические группы защиты**

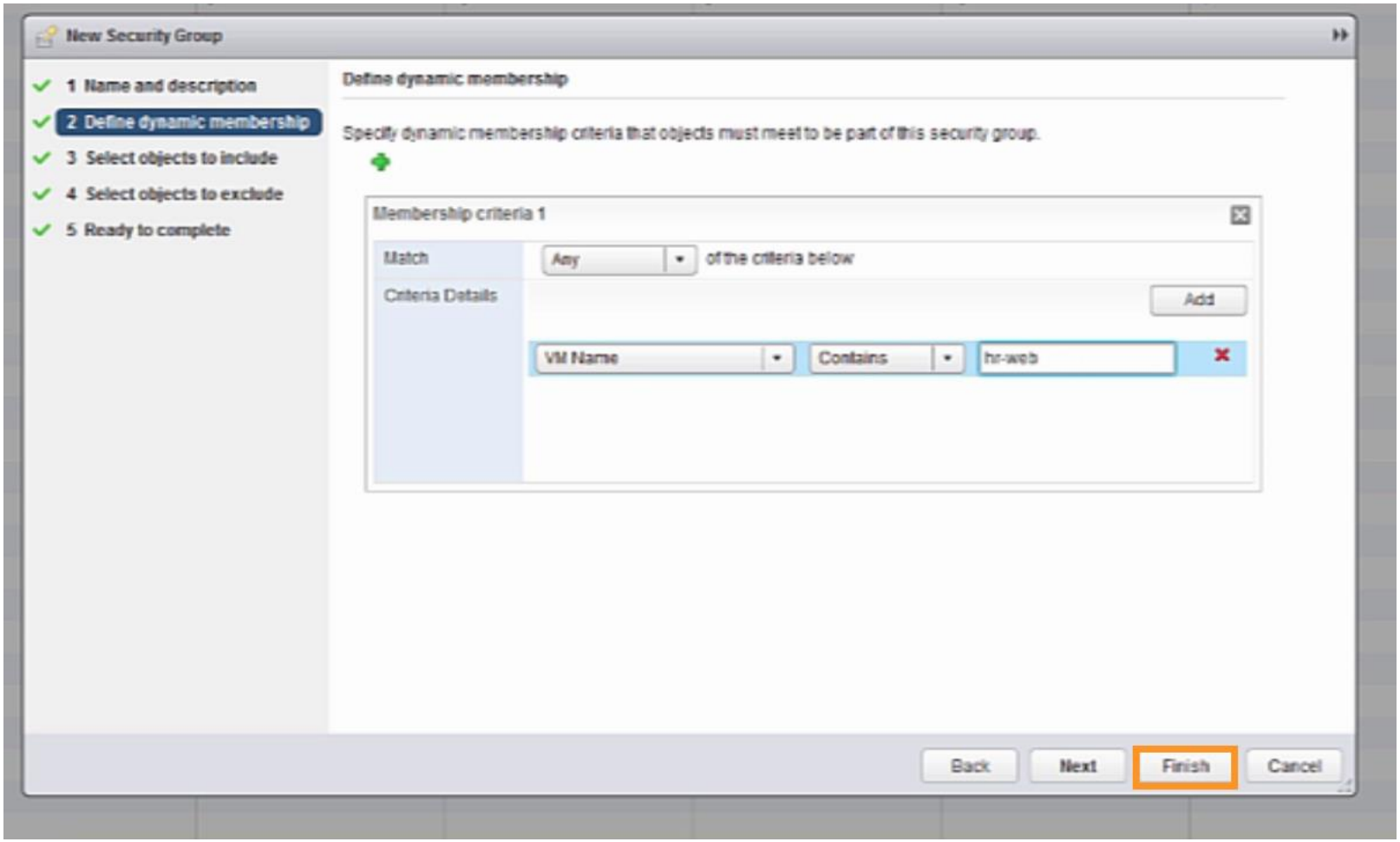
# Пример интерфейса (1/6)



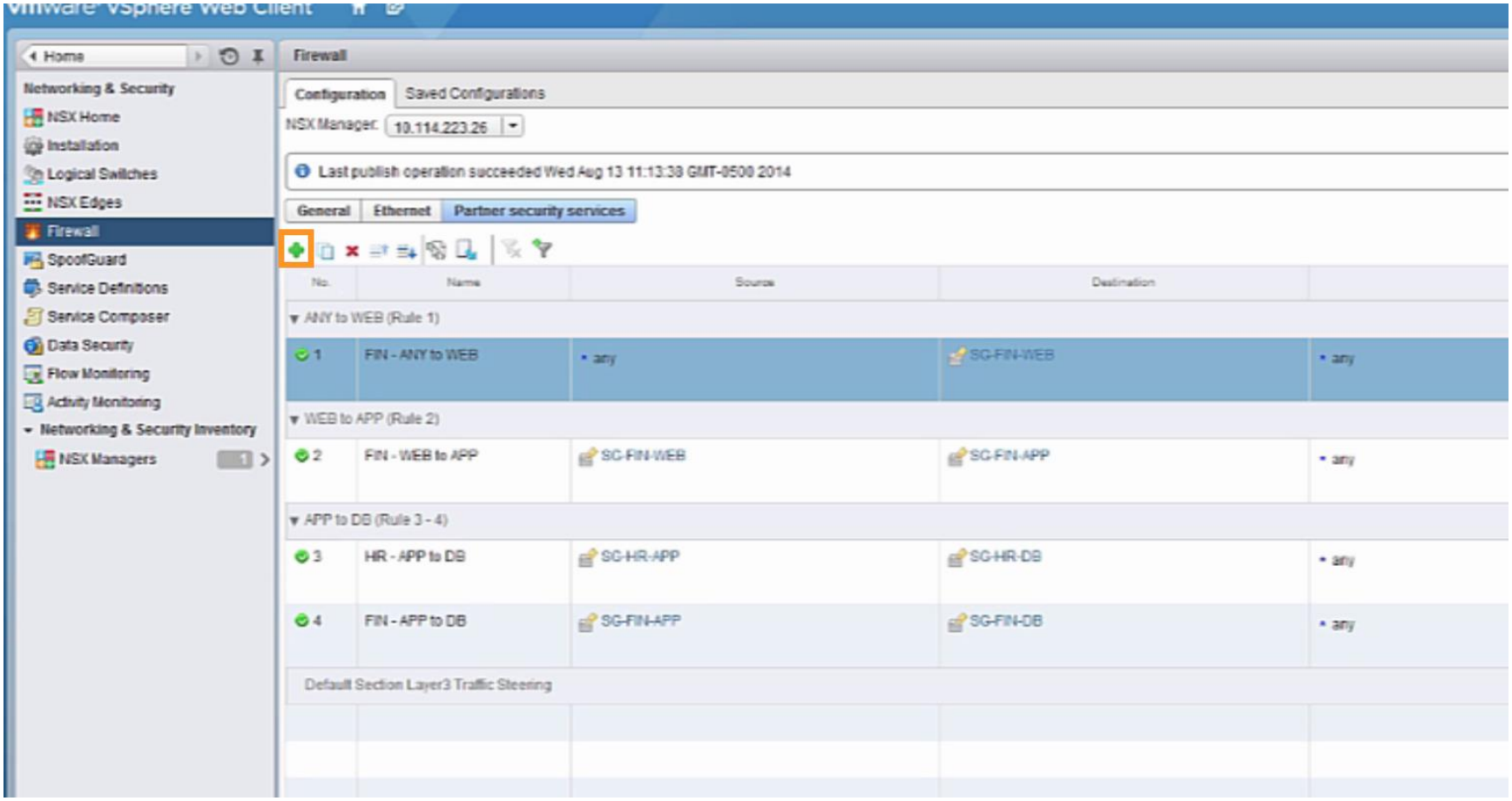
# Пример интерфейса (2/6)



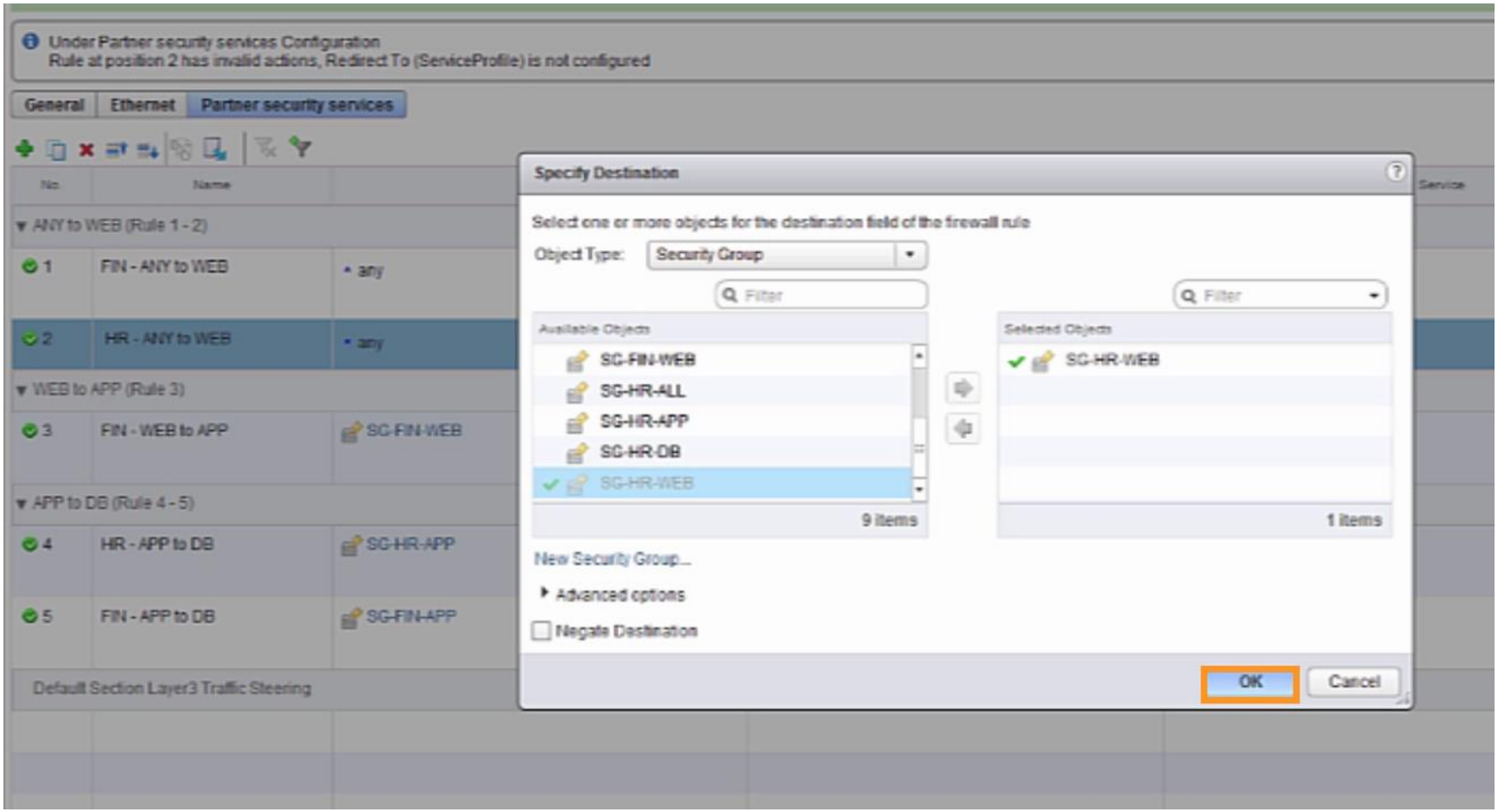
# Пример интерфейса (3/6)



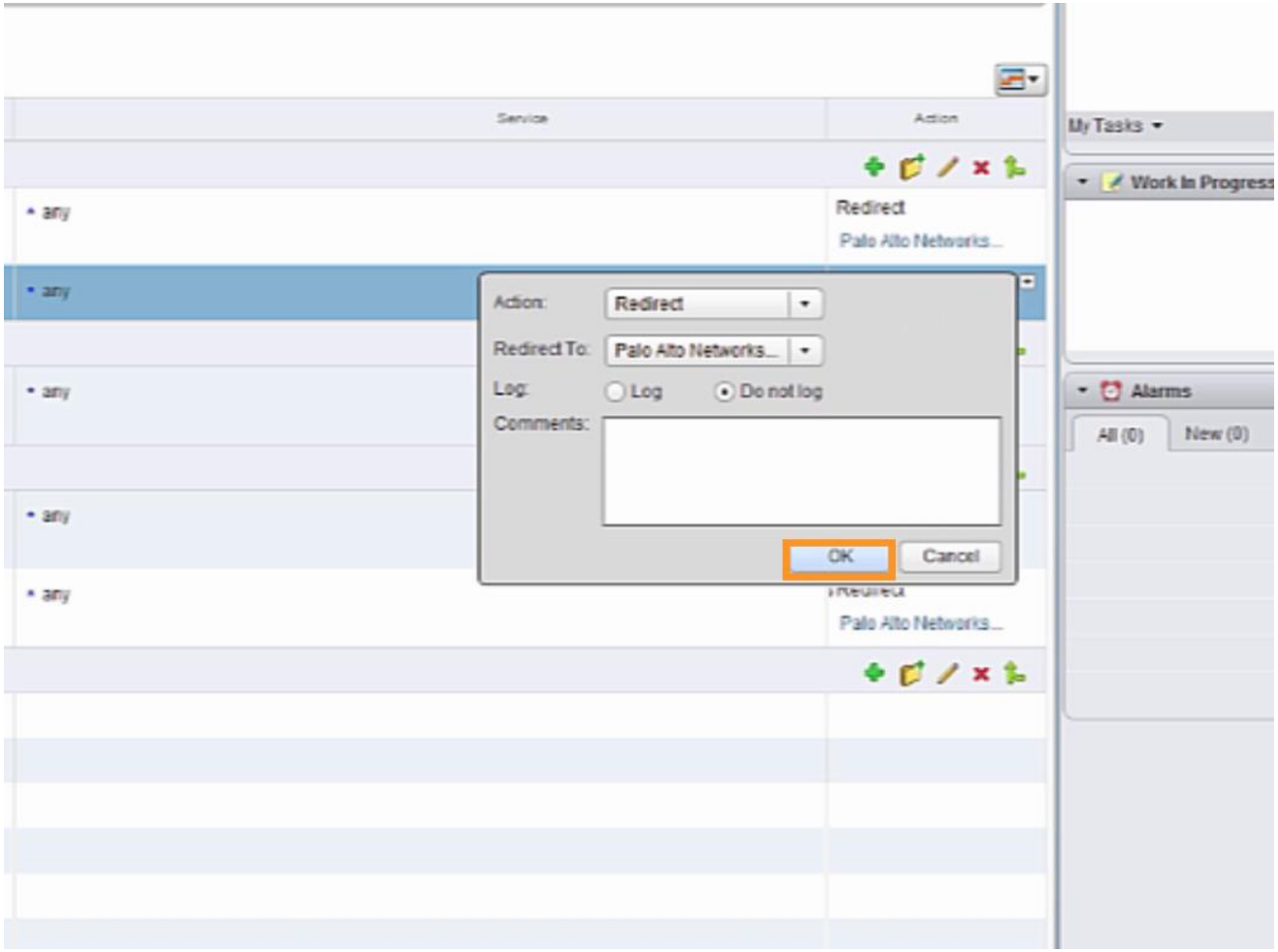
# Пример интерфейса (4/6)



# Пример интерфейса (5/6)



# Пример интерфейса (6/6)



# Основные преимущества NSX

## Для ИТ

- Конфигурация сети для новых приложений происходит быстрее, нет необходимости каждый раз перенастраивать оборудование
- Упрощения проектов по слиянию/поглощению, модернизации: не требуется менять адресацию приложений

## Для ИБ

- Теперь модель нулевого доверия в ЦОД можно реализовать на практике
- Меньше ручной настройки правил: динамические группы, автоматизация
- Защищать приложения можно быстрее и дешевле: подключение дополнительных сервисов (IDS/IPS и т.д.) происходит «на лету», независимо от физической сетевой топологии

## Для СиТ

- Можно упростить сетевую архитектуру, при этом повысить производительность, масштабируемость, а также сэкономить на оборудовании
- Преимущества технологии SDN можно получить на любом сетевом оборудовании
- Упрощения проектов по слиянию/поглощению, модернизации: не нужно менять/интегрировать сетевое оборудование

# Материалы для изучения (1/2)

- Общая информация:
  - Страница продукта на vmware.com: http://www.vmware.com/ru/products/nsx/
  - Технические ресурсы: http://www.vmware.com/products/nsx/resources.html
  - Презентация "Введение в VMware NSX": https://www.dropbox.com/s/v9uge3sx8dl7kjh/20151006%20-%20NSX%20Presentation.pdf?dl=0
  - The VMware NSX Network Virtualization Platform — Technical White Paper: http://www.vmware.com/files/ru/pdf/products/nsx/VMware-NSX-Network-Virtualization-Platform-WP.pdf
  - NSX Product walkthrough: http://featurewalkthrough.vmware.com/#!/nsx
- Лабораторные работы:
  - HOL-SDC-1603 - VMware NSX Introduction 2015 http://labs.hol.vmware.com/HOL/catalogs/lab/2125
  - HOL-SDC-1625 - VMware NSX Advanced http://labs.hol.vmware.com/HOL/catalogs/lab/2102

# Материалы для изучения (2/2)

- VMware Reference Architecture
  - The VMware® Software-Defined Data Center Foundation: http://www.vmware.com/files/pdf/techpaper/vmware-v2d-foundationRA.pdf
  - Automated Provisioning with the VMware® Software-Defined Data Center: http://www.vmware.com/files/pdf/techpaper/vmware-v2d-singleregionRA.pdf
- Books:
  - NSX for vSphere - A Foundation of SDDC: https://communities.vmware.com/thread/528879
- Design Guides:
  - VMware® NSX-v Brownfield Design and Deployment Guide: https://communities.vmware.com/docs/DOC-29556
  - VMware® NSX for vSphere Network Virtualization Design Guide: https://communities.vmware.com/docs/DOC-27683
- Planning for Operational Transformation with NSX: http://www.vmware.com/files/pdf/planning-for-operational-transformation-with-nsx.pdf

# Спасибо за внимание!

vmware®