Cisco Expo
2010

Безопасность и виртуализация в центрах обработки данных

Андрей Гречин

Инженер-консультант

План

- Тенденции развития современных ЦОД
- Технологии виртуализации инфраструктуры
- Сервисы безопасности на уровне агрегации
- Защита уровня доступа
- Заключение

Тенденции развития ЦОД

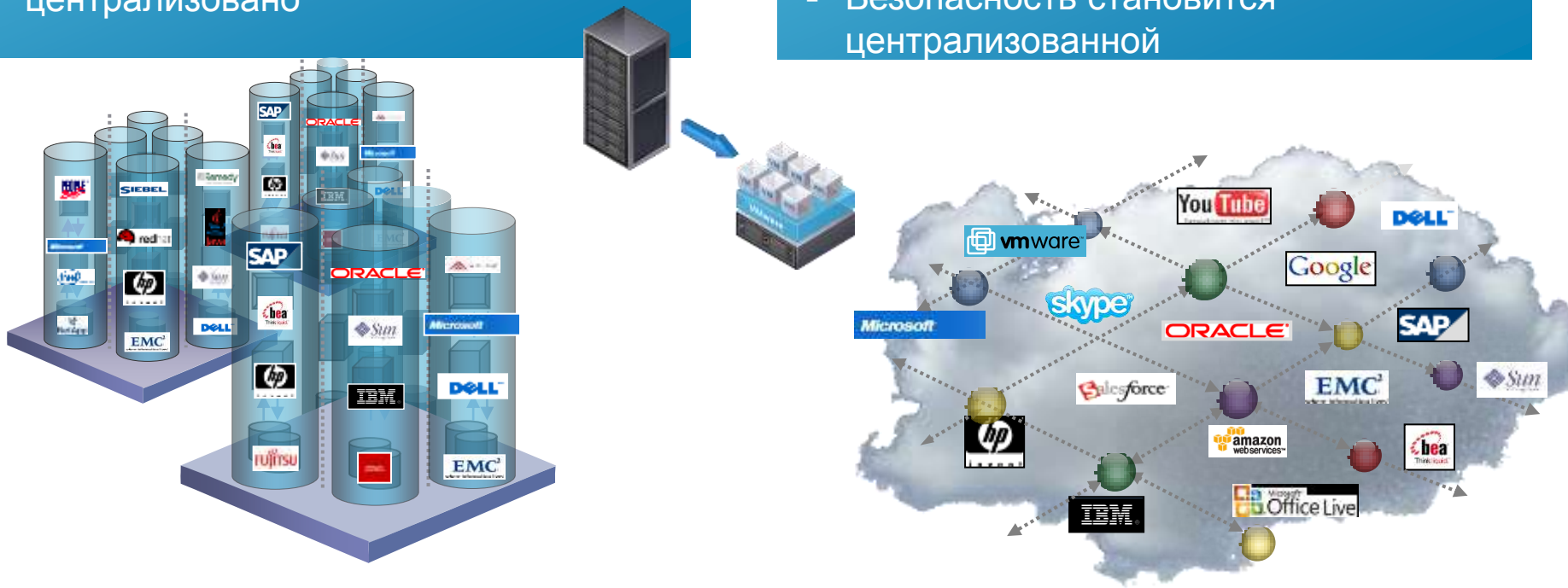
Смена парадигмы

Раньше

- Наложенная архитектура
- Приложения внедрены в определенных точках
- Предсказуемые потоки информации
- Безопасность внедряется не централизовано

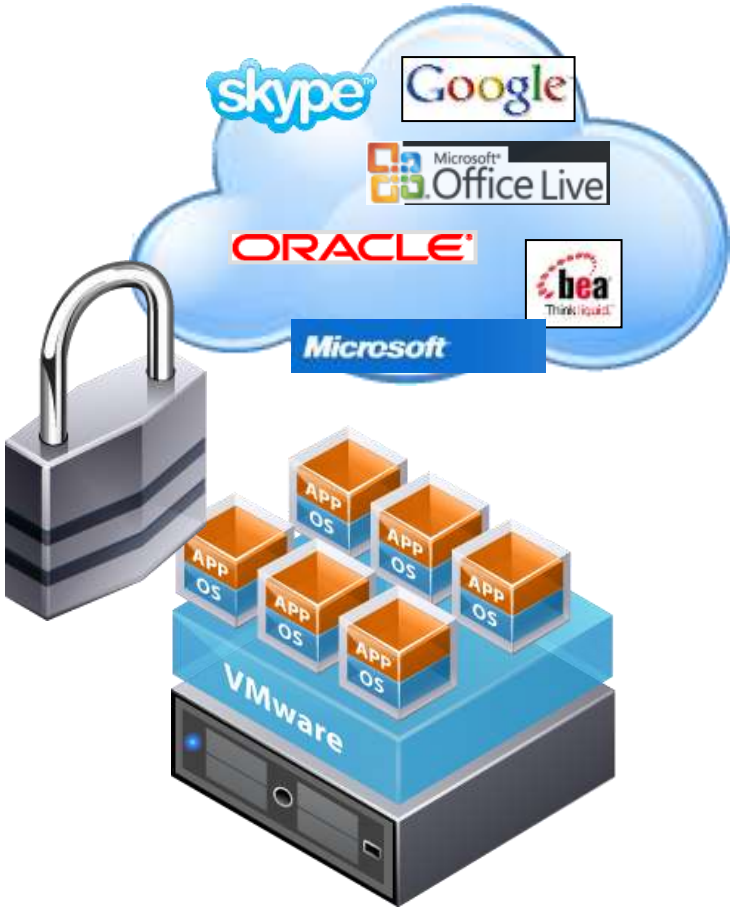
Новое

- Консолидация ЦОДов и серверов
- Виртуализация серверов
- «Любая» задача на «любом» сервере
- Непредсказуемые потоки трафика следующие за задачами
- Безопасность становится централизованной

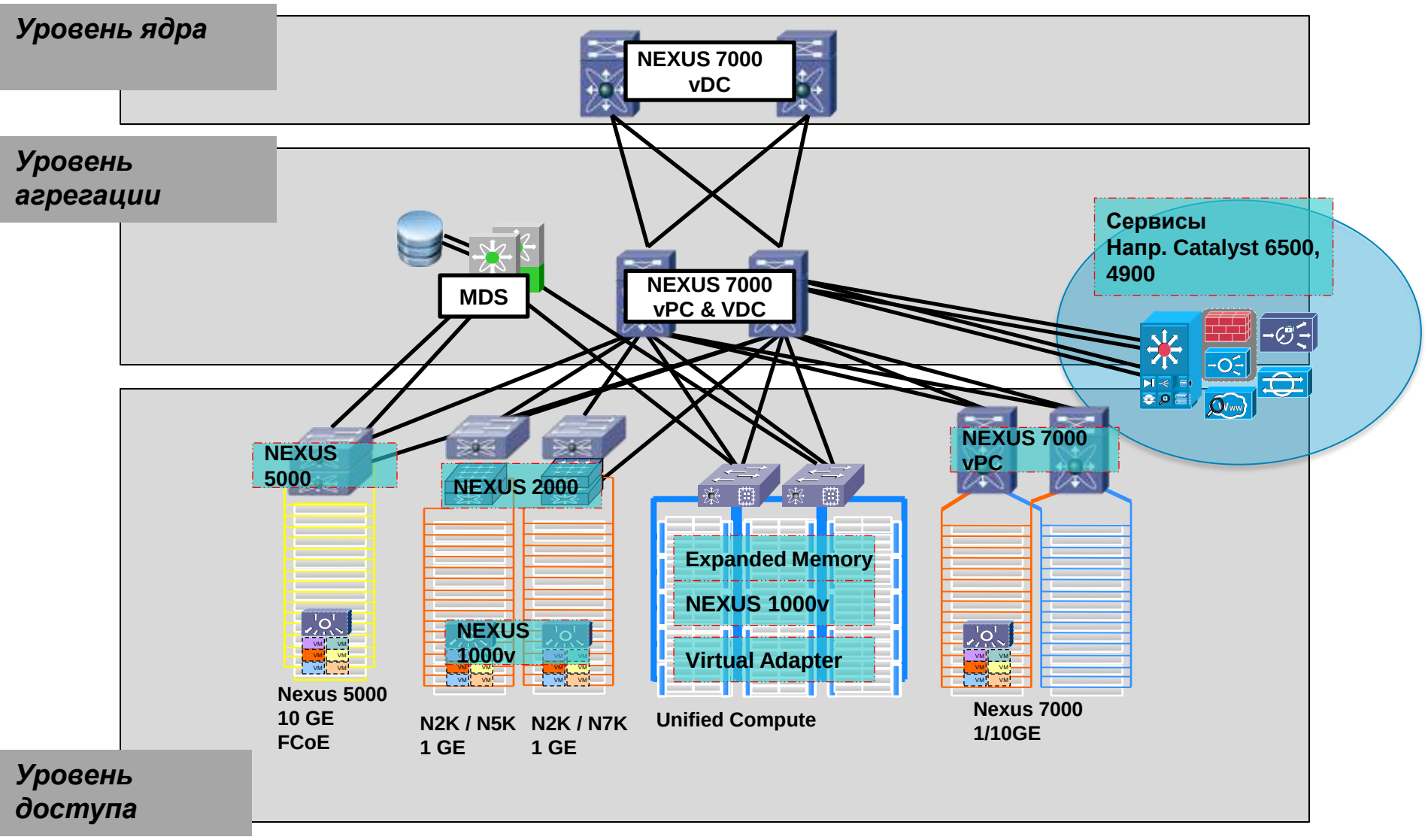


Проблемы обеспечения ИБ в ЦОД

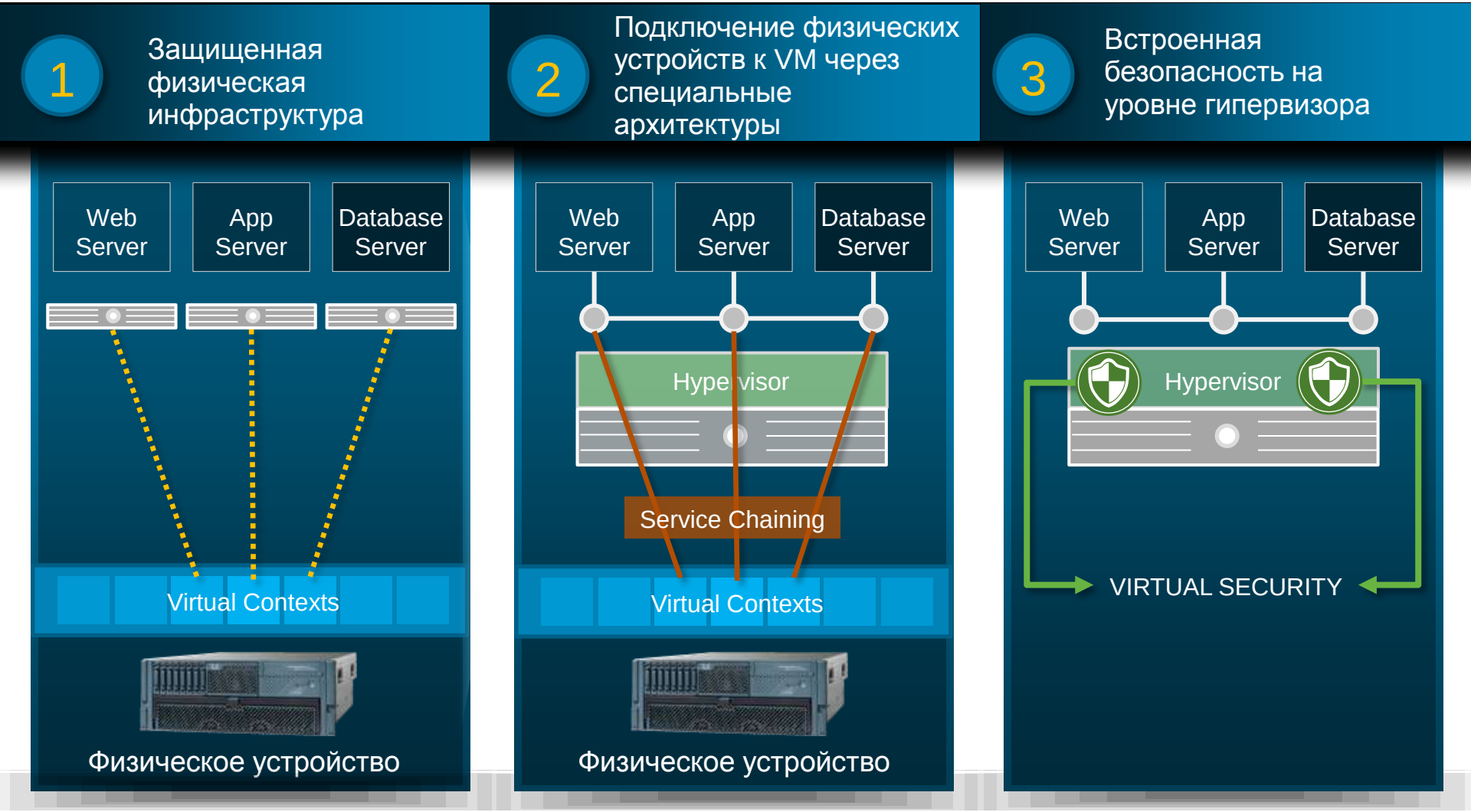
- Виртуализация
- Сети хранения
- Приложения
- Утечки данных
- Доступность
- Соответствие требованиям



Архитектура современного ЦОД

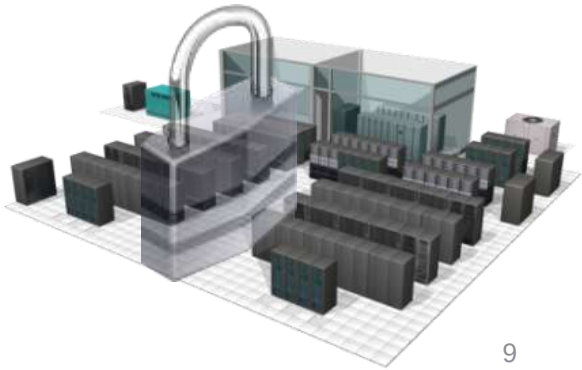


Виртуализация, ЦОД и ИБ



Особенности безопасности в ЦОД

- Сетевые сервисы безопасности внедряются централизованно
- Нужно учитывать функции виртуализации в ЦОД: VDC, vPC, VSS
- Зональный дизайн на основе доверия для контроля доступа и применения политик
- Возможность сопоставления политик безопасности между физической и виртуальной средой
- Предсказуемость пути трафика для обеспечения доступности
- На политику могут влиять – бизнес-модель, соответствие регуляторам, приложения
- Единого решения нет, но есть практические рекомендации…



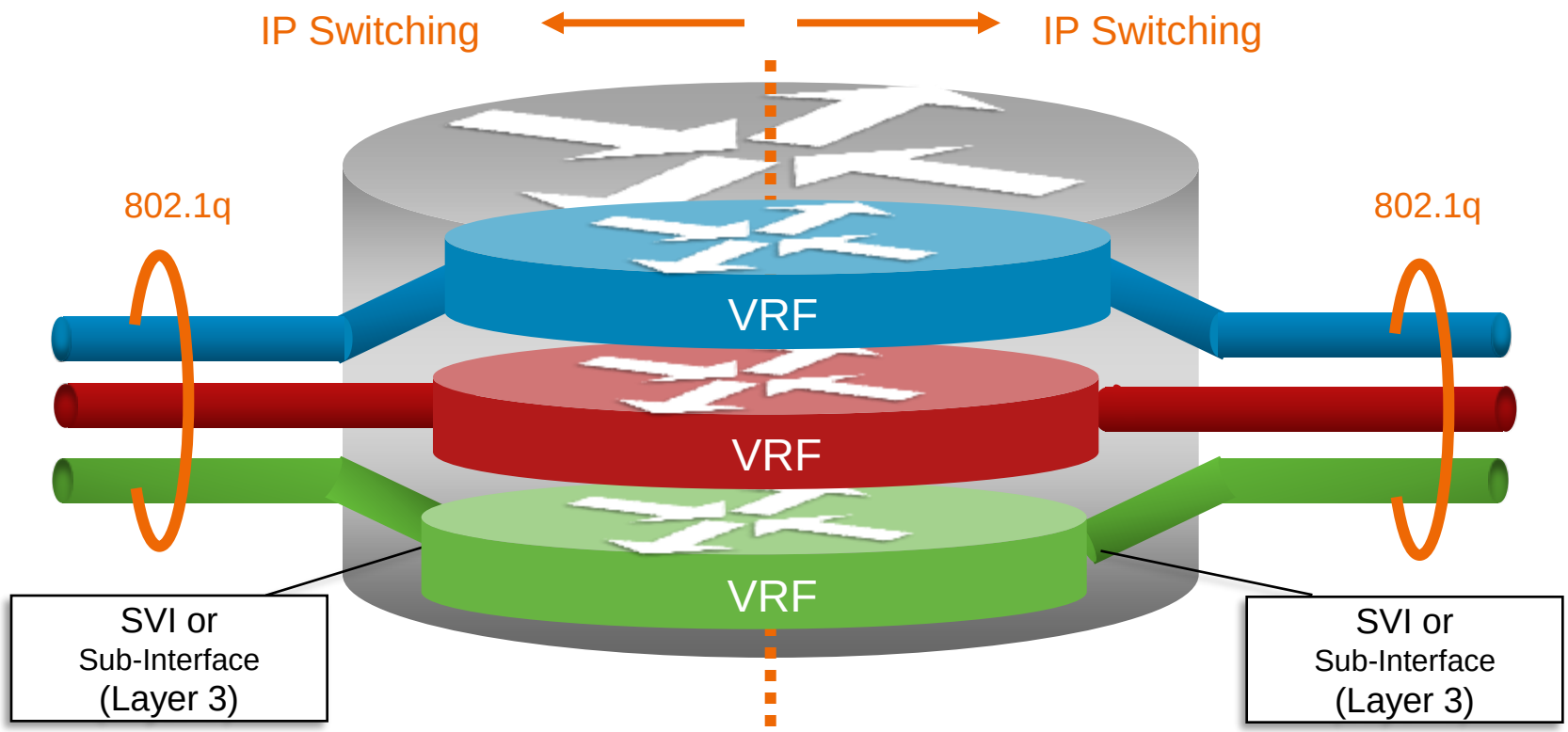
Технологии виртуализации инфраструктуры

Виртуализация устройств: VRF

Ключевая функция

Virtual Routing and Forwarding (VRF)

› VRF позволяет сосуществовать на одном маршрутизаторе нескольким контекстам (таблицам) маршрутизации. Благодаря своей независимости друг от друга, VRF играют важную роль в разделении трафика между клиентами коммерческого ЦОД.

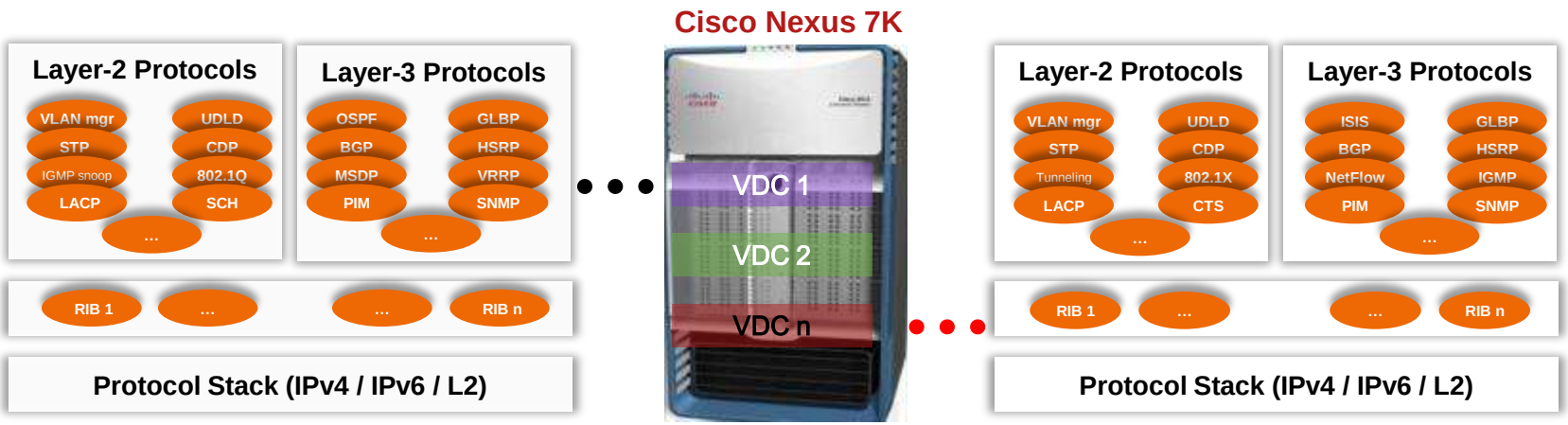


Виртуализация устройств: Контексты с помощью VDC

Ключевая функция

- Virtual Device Context (VDC)

VDC – ключевая функция для максимизации использования ресурсов при одновременном обеспечении безопасности и изоляции благодаря логическому разделению устройств.



Программное разделение

- Полная изоляция программных сбоев
- Домены адресации
- Service differentiation domains
- Контексты управления
- Выделение ресурсов
- Домены безопасности

Общие ресурсы

- Программная инфраструктура
- Ядро
- Блоки питания
- Вентиляторы
- Шасси

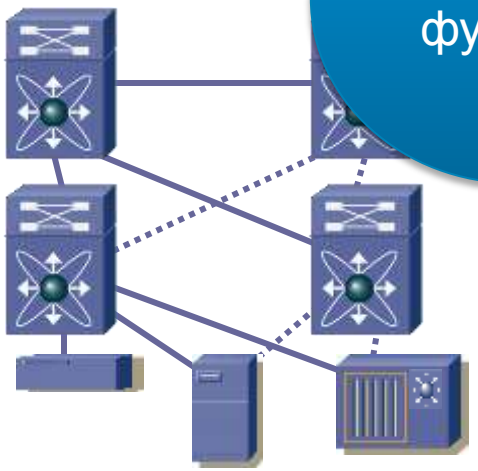
Аппаратное разделение

- Физические порты
  - Layer 2
  - Layer 3
- Port Channels
- Линейные карты

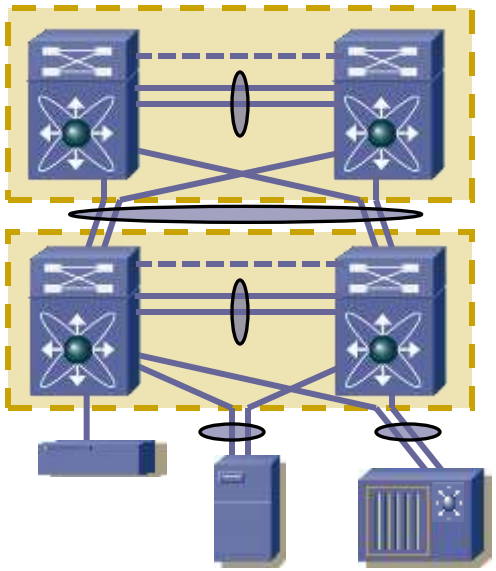
Виртуализация устройств:
Virtual Port Channel

Ключевая функция

- Возможность организации агрегированного канала (port channel), приходящего на два разных коммутатора
- Избавляет от STP
- Использование полосы всех имеющихся соединений
- Быстрая сходимость при отказе устройства или канала
- Обеспечение отказоустойчивости и масштабируемости при подключении серверов
- Сокращение CAPEX и OPEX
- Совместимость со всеми функциями
- Необходима поддержка Etherchannel на сервисных устройствах



Без vPC



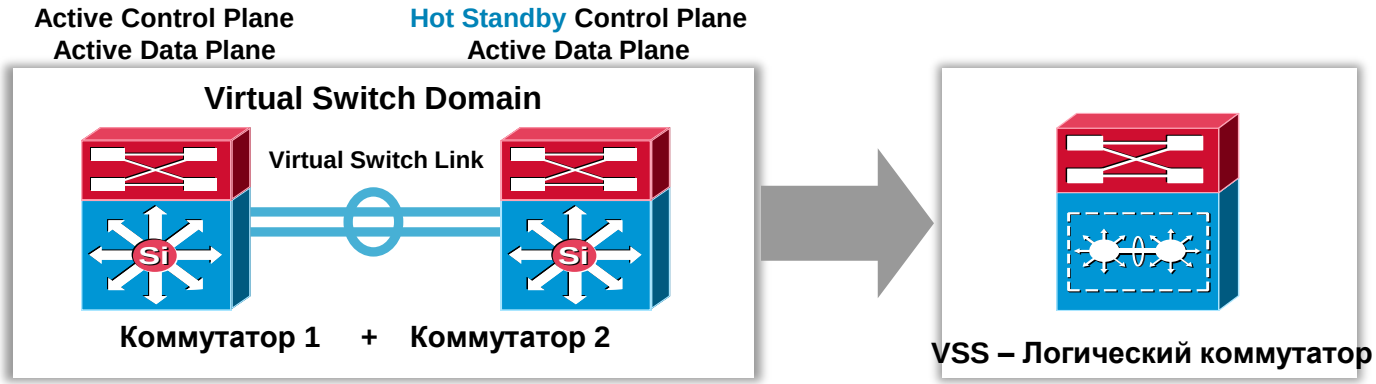
С использованием vPC

Высокая доступность сервисов

Ключевая функция

- Virtual Switch System (VSS)

Два физических коммутатора Catalyst 6500 соединяются специальным соединением Virtual Switch Link (VSL) и работают как единый логический коммутатор для обеспечения высокой доступности сервисов.

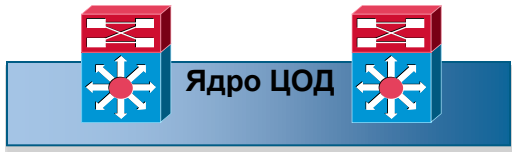


Вместе с vPC технология VSS обеспечивает высокую доступность и пропускную способность на уровне агрегации.
Высокая доступность сервисов для постоянной защиты сети: МСЭ, балансировка нагрузки и система предотвращения вторжений.
Интегрированная безопасность с DHCP Snooping, Dynamic ARP inspection и IP Source Guard

Сервисы безопасности на уровне агрегации

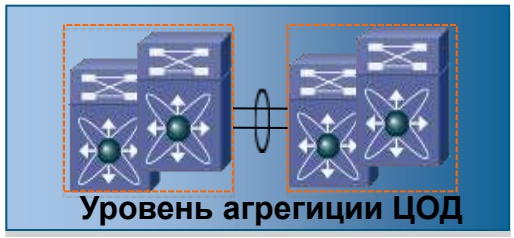
Ключевые области безопасности

Технологии защиты ЦОД



Защита сетевой инфраструктуры
Для защиты устройств, трафика и плоскости управления. Сегментация плоскостей управления и данных с помощью виртуализации

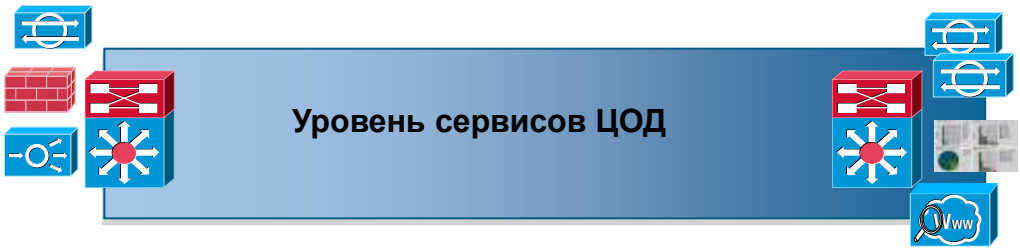
МСЭ - Фильтрация пакетов с учетом состояния
Интеграция с коммутаторами за счет EtherChannel/VDC



МСЭ - Фильтрация пакетов с учетом состояния
Консолидированные виртуальные МСЭ обеспечивают безопасность на основе зон. Интеграция с коммутаторами за счет vPC

Предотвращение вторжений
IPS/IDS: анализ трафика

Балансировка нагрузки серверов
Маскирование серверов и приложений



Flow Based Traffic Analysis
Мониторинг и анализ данных

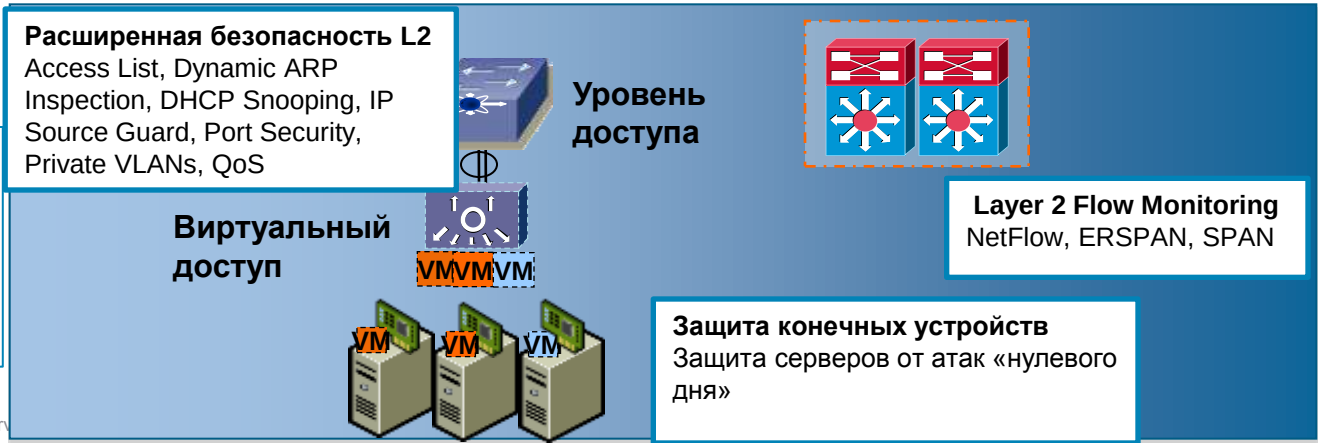
Контроль и защита web-приложений с помощью WSA

Управление безопасностью

- **Прозрачность**
- **Корреляция событий**
  HIPS, Firewalls, IPS, Netflow, Syslog
- **Forensics**
- **Детектирование аномалий**
- **Соответствие регуляторам**

SIEM CSM

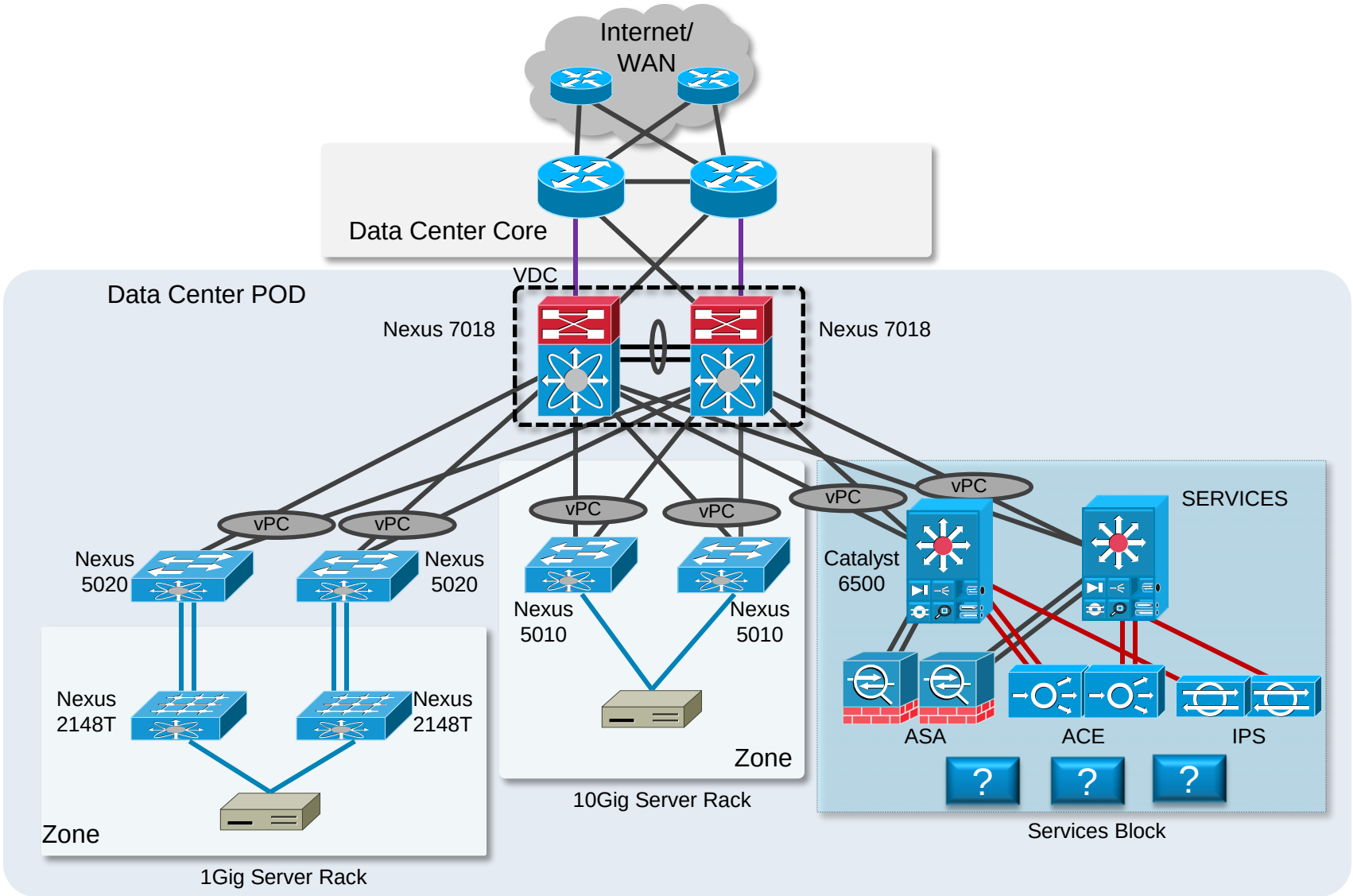
Расширенная безопасность L2
Access List, Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, Port Security, Private VLANs, QoS



Layer 2 Flow Monitoring
NetFlow, ERSPAN, SPAN

Защита конечных устройств
Защита серверов от атак «нулевого дня»

Внедрение безопасности в топологии современного ЦОД



Функции безопасности инфраструктуры на уровне агрегации

- **Защита плоскости управления** – Control Plane Protection

  Защита супервизора от DoS атак для предотвращения перерывов в обслуживании. Предотвращение широковещательного L2 шторма и перенаправления ненужного трафика на CPU

- **Подавление широковещательных пакетов** – Broadcast Suppression

  Защита ЦОД от широковещательного шторма на уровне порта, который влияет на доступность пропускной способности

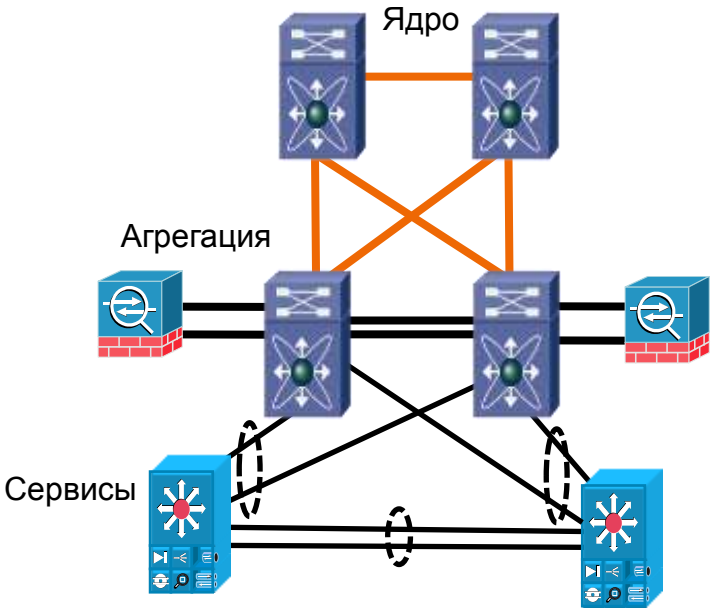
- **Проверка пакетов на соответствие стандартам** – Packet Sanity Checks

  Forwarding engine проверяет заголовки IPv4 и IPv6 пакетов для защиты сети от нелегального трафика

Внедрение функций ИБ:
Уровень агрегации

Важно:

- Переключение при сбое на агрегирующих коммутаторах требует переключения на средствах защиты
- На средствах защиты требуется поддержка EtherChannel для интеграции с vPC



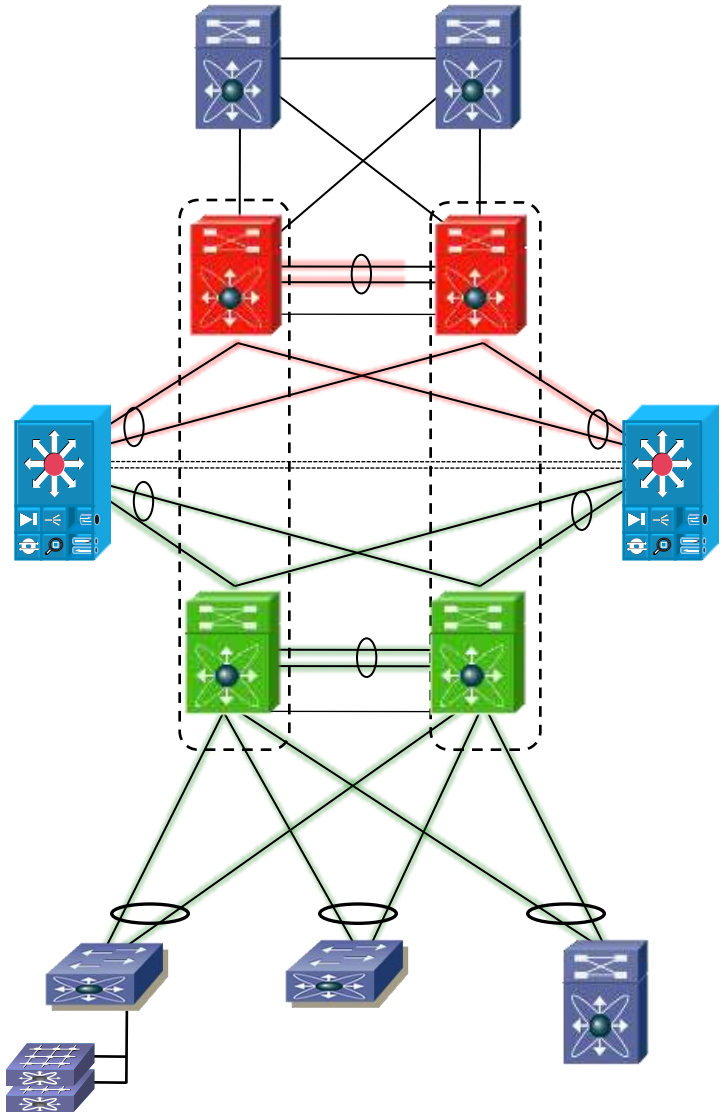
- Прямое подключение к уровню агрегации
- Подключение через коммутаторы уровня сервисов

Внедрение функций ИБ: Сервисный блок

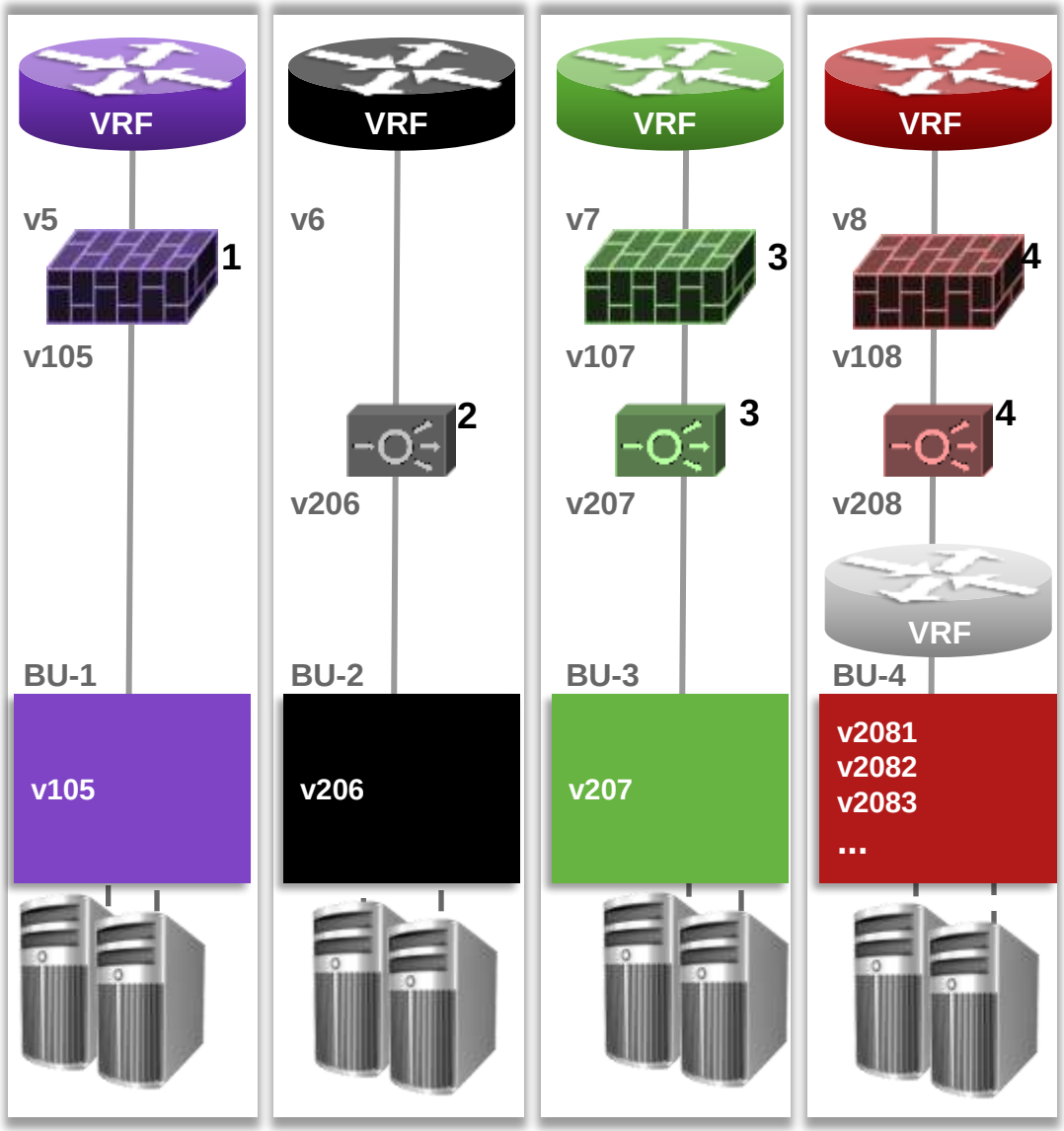
- Два виртуальных контекста на Nexus 7000 используются для вставки сервисов между виртуальными уровнями коммутации
- L2 коммутация в сервисных шасси с прозрачными сервисами
- Сервисные шасси поддерживают Etherchannel для взаимодействия с vPC
- vPC работает между обеими парами контекстов VDC для поддержки Etherchannel между внутренними и внешними интерфейсами сервисных шасси

Особенности дизайна:

- Поддержка нескольких виртуальных сервисных контекстов за счет использования нескольких VRF во внутренних контекстах VDC



Пример:
Виртуализованные сервисы



“Front-End” VRFы (MSFC)

Контексты МСЭ

Контексты ACE

“Back-End” VRFы (MSFC)

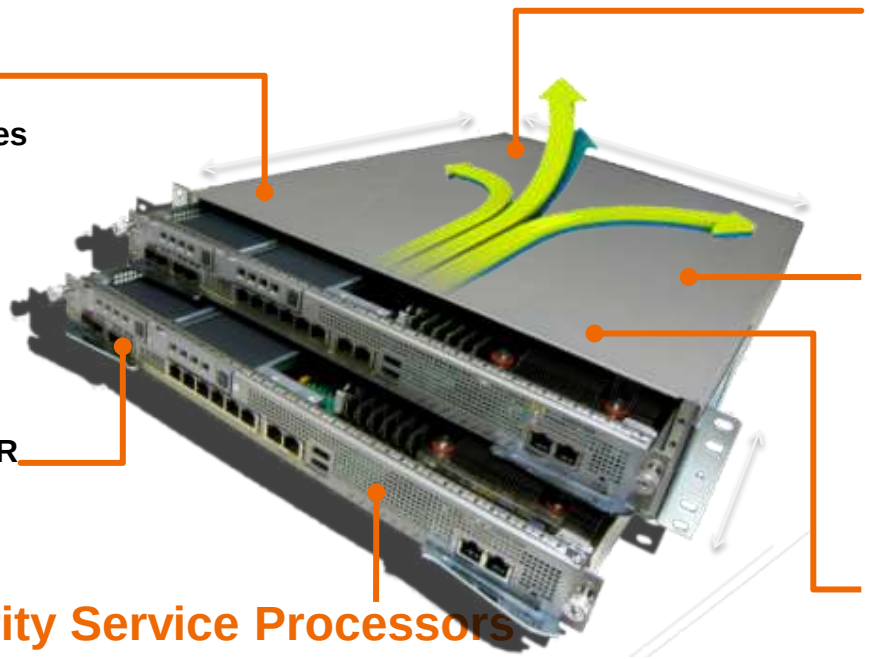
Серверные VLANы

Последние разработки: Cisco ASA 5585-X

Оптимизировано для использования в ЦОД

2 RU Шасси
- 2 x full-slot modules
- 1 x full-slot + 2 x half-slot modules
- Поддержка OIR

GE Порты
- До 8 x 10G SFP+ с поддержкой OIR
- До 16 x 1GbE Cu
- Слоты SFP/SFP+



Резервируемые блоки питания с горячей заменой
- Обдув спереди назад
- 320W (1 модуль) / 670W (2 модуля)

Multi Gigabit Fabric
- Пассивная шина
- Прямое взаимодействие модулей
- Приоритезация и шейпинг пакетов

eUSB
- 2 GB внутри
- Удобное хранилище
- Идентификационные данные безопасности

Security Service Processors
- Мультисервисная поддержка
- Специализированные многоядерные 64-битовые процессоры
- Платформа с расширяемой производительностью

Защита уровня доступа

Используйте функции безопасности коммутатора

- **Функции безопасности L2:**
  - Access Lists
  - Dynamic ARP Inspection
  - DHCP Snooping
  - IP Source Guard
  - Port Security
  - Private VLANs
  - STP Extensions (BPDU Guard)
  - Layer 2 Storm Control
- **Мониторинг на L2:**
  - NetFlow
  - SPAN
  - ERSPAN
  - ACL Logs

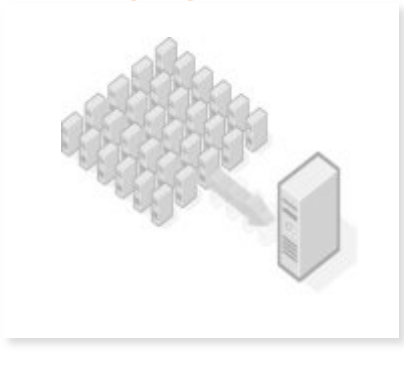
Виртуальный доступ и безопасность

X86 виртуализация сегодня

Одно приложение на сервер

Много приложений на сервер

Консолидация серверов в ЦОД



До виртуализации

- Один образ ОС на машину
- ПО и аппаратная платформа тесно связаны
- Несколько приложений, работающих под одной ОС, часто конфликтуют
- Негибкая и дорогая инфраструктура

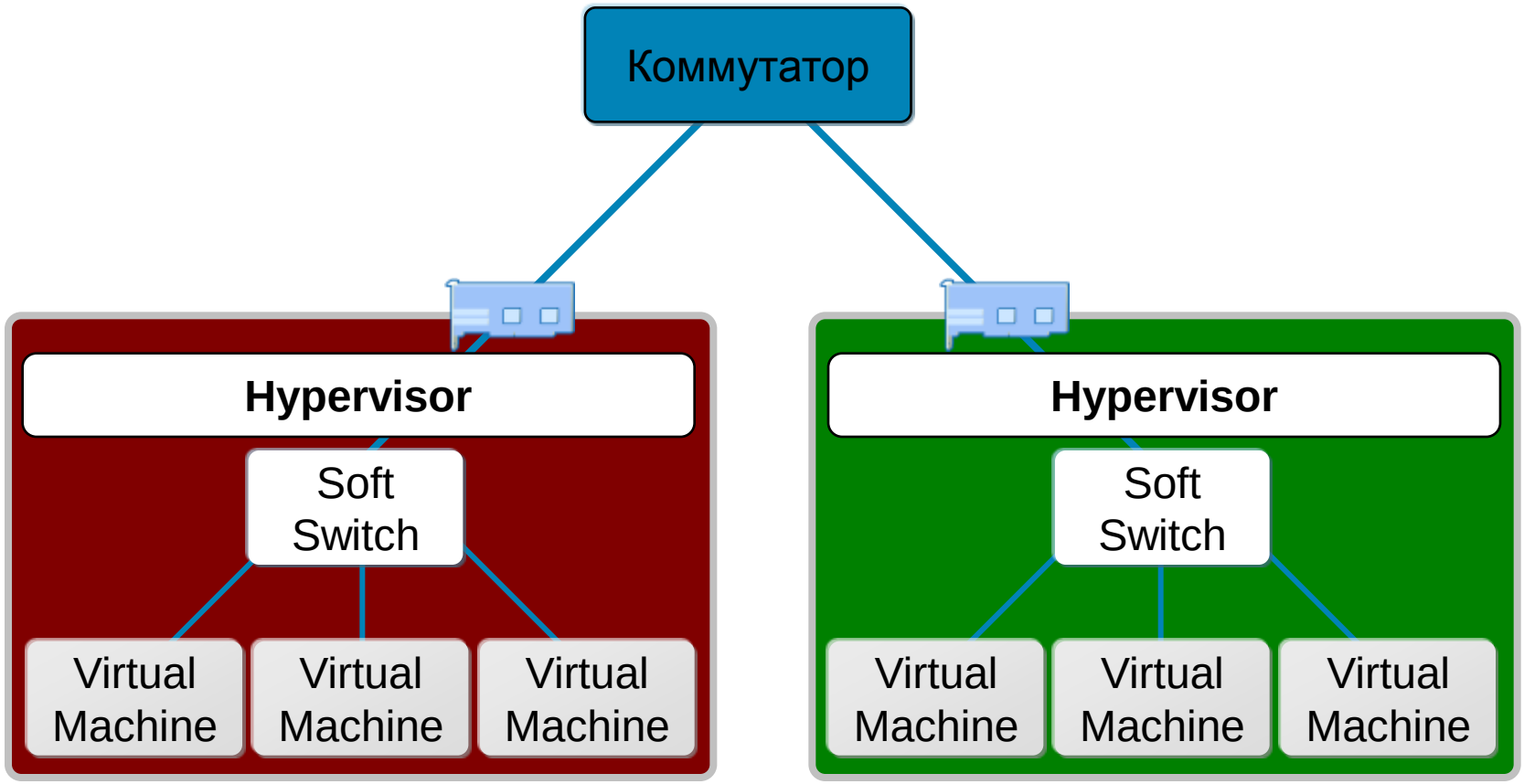
После виртуализации

- Аппаратная независимость ОС и приложений
- Виртуальные машины могут запускаться на любой системе
- Управление ОС и приложениями как единым элементом за счет инкапсуляции в ВМ

Преимущества

- Экономия на электропитании и охлаждении
- Проще управление
- Быстрое развертывание
- Высокая доступность
- Меньше места в стойках
- Уменьшение CAPEX и OPEX

X86 виртуализация сегодня



Безопасность виртуальной среды

- Защита Гипервизора

  Атакующий может получить неавторизованный доступ к гипервизору и контроль над физическим сервером и виртуальными машинами

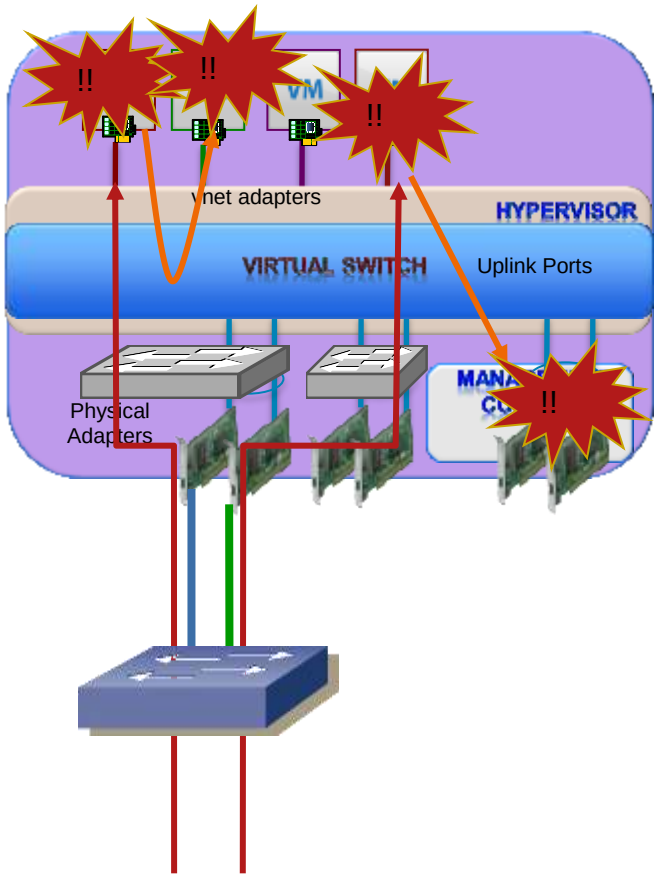
- Чужеродные VM

  Была ли гостевая ОС скомпрометирована?

  Мобильность виртуальных серверов

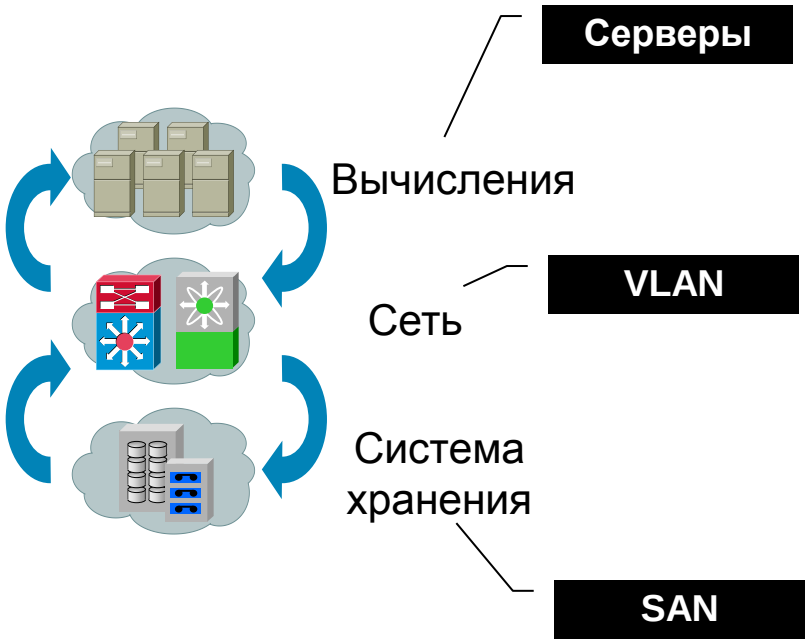
- Прозрачность и безопасность трафика между VM

  Трафик между 2-мя виртуальными машинами может путешествовать по внутренней шине физического сервера не выходя во внешнюю сеть, где применяются традиционные меры безопасности

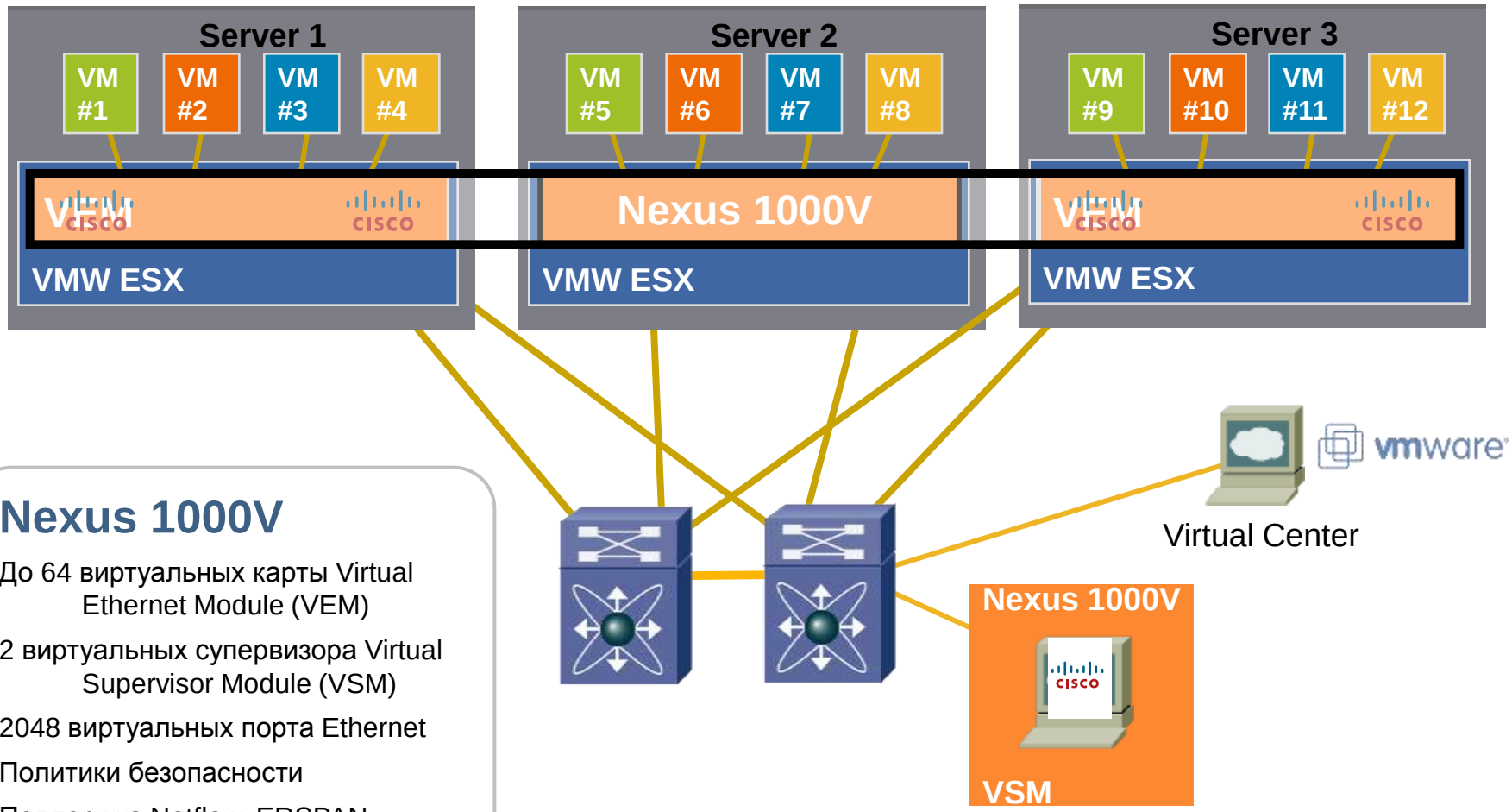


Сегментация и идентификация
Физические и виртуальные ресурсы

- При переходе на виртуальные машины, политики безопасности должны сохраняться
  - Те же приложения и ОС выполняются в VM
- Гипервизор
  - Разделяйте интерфейсы серверов, VLANы для VMotion, интерфейсы управления и интерфейсы VM
  - Раздельные политики безопасности и управления трафиком
- LAN
  - Используйте Группы портов (Port groups) для сегментирования VLAN в гипервизоре



Cisco Nexus 1000V и VN-Link



Nexus 1000V

- До 64 виртуальных карты Virtual Ethernet Module (VEM)
- 2 виртуальных супервизора Virtual Supervisor Module (VSM)
- 2048 виртуальных порта Ethernet
- Политики безопасности
- Поддержка Netflow, ERSPAN, мультикаста, etherchannel

Cisco NX-OS

Data Center Network Manager (DCNM), CiscoWorks, VMWare vCenter

Возможности Nexus 1000V

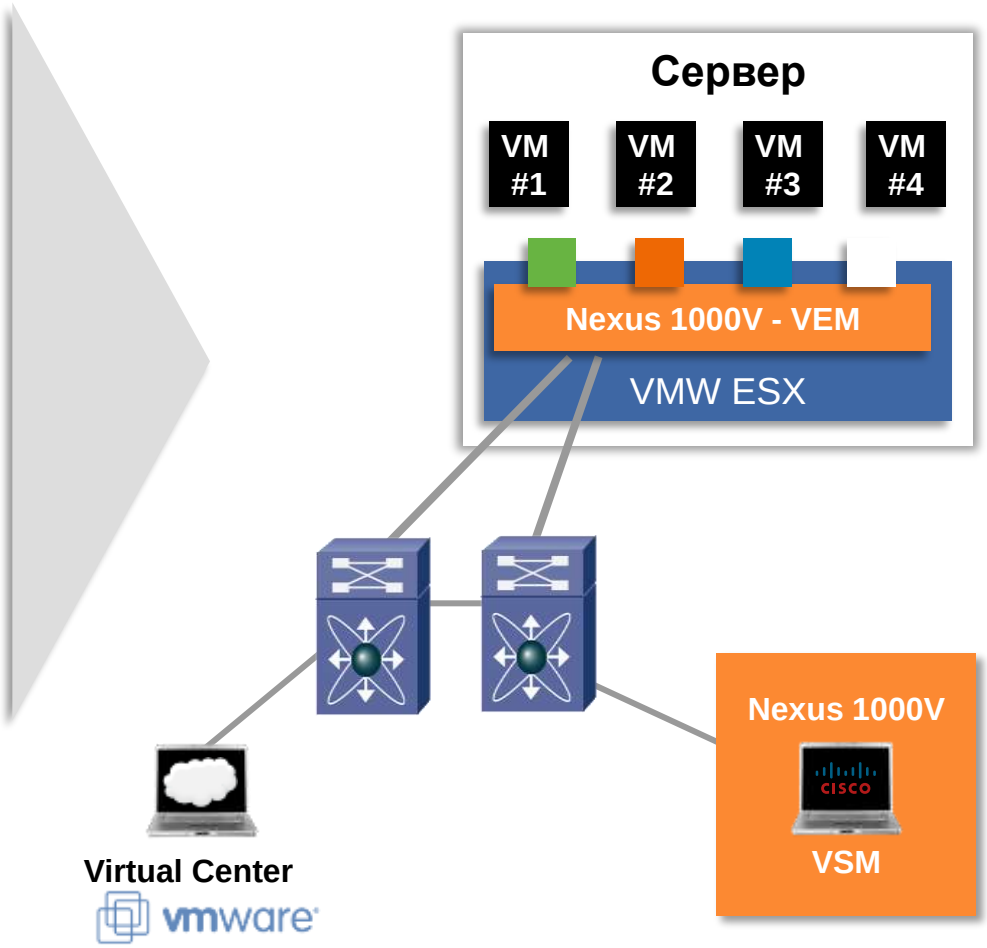
Коммутация	▪ L2 Switching, 802.1Q Tagging, **VLAN Segmentation**, Rate Limiting (TX) ▪ IGMP Snooping, QoS Marking (COS & DSCP)
Безопасность	▪ **Policy Mobility, Private VLANs w/ local PVLAN Enforcement** ▪ **Access Control Lists (L2–4 w/ Redirect), Port Security, SGT, 802.1x** ▪ **Dynamic ARP inspection, IP Source Guard, DHCP Snooping**
Provisioning	▪ Automated vSwitch Config, **Port Profiles**, Virtual Center Integration ▪ Optimized NIC Teaming with Virtual Port Channel – Host Mode
Прозрачность	▪ VMotion Tracking, **ERSPAN, NetFlow v.9 w/ NDE**, CDP v.2 ▪ VM-Level Interface Statistics
Управление	▪ **Virtual Center VM Provisioning**, Cisco Network Provisioning, CiscoWork ▪ Cisco CLI, Radius, TACACs, Syslog, SNMP (v.1, 2, 3)

Функции	ESX 4.0: vNetwork Standard Switch	ESX 4.0: vNetwork Distributed Switch	Cisco Nexus 1000V
IGMP Snooping v3	-	-	Да
Network Policy VMotion	-	Да	Да
Asynchronous Port Channels	-	-	Да
VPC-Host Mode	-	-	Да
Link Aggregation Control Protocol (LACP)	-	-	Да
Quality of Service Marking (DSCP, ToS, CoS)	-	-	Да
Private VLANs	-	Да	Да
Local PVLAN Enforcement	-	-	Да
Access Control Lists	-	-	Да
DHCP Snooping	-	-	Да
IP Source Guard	-	-	Да
Dynamic ARP Inspection	-	-	Да
Multi-Tier Policy Groups	-	-	Да
SPAN	-	-	Да
ERSPAN	-	-	Да
Netflow v5, v9	-	-	Да
SNMP v3 Read/Write	-	-	Да
Syslog	**	**	Да
Radius/TACACS+	-	-	Да
Configuration & Management Console/Interface	VI Client	VI Client to vCenter Server	vCenter & Cisco CLI

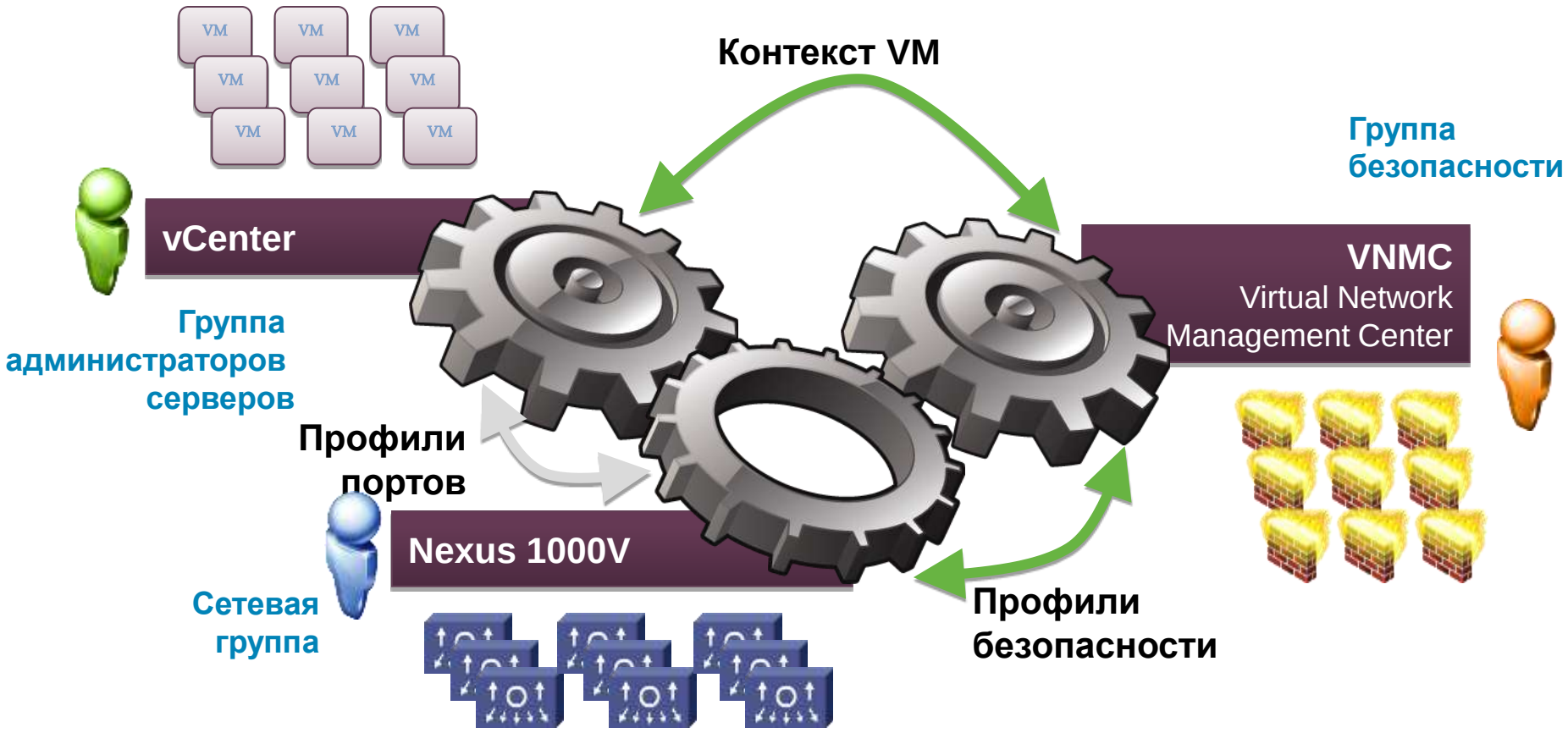
** Syslog сетевых событий объединяется и экспортируется вместе с остальной, не сетевой, информацией об событиях в vCenter.

Nexus 1000v
Профили портов

- Настройки безопасности в профилях портов:
  - ACL
  - Port Security
  - VLAN, PVLAN
  - SPAN, RSPAN и ERSPAN
  - NetFlow Collection
  - Rate Limiting
  - QoS Marking (COS/DSCP)

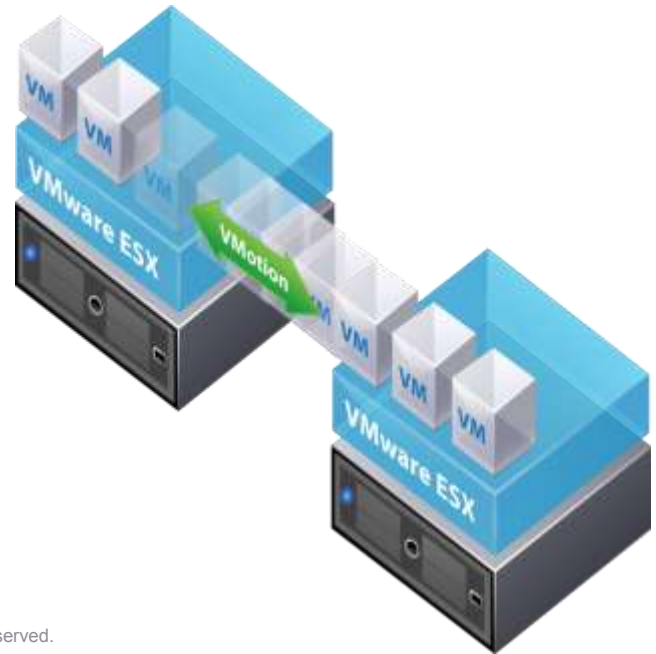


Разделение обязанностей



Мобильность политик с VMotion, включая безопасность

1. Virtual Center запускает VMotion (ручной/DRS) и сообщает Nexus 1000V
2. Во время репликации VM, Nexus 1000V копирует состояние порта VM на новый сервер
3. После окончания VMotion порт на новом ESX сервере поднимается и MAC-адрес виртуальной машины анонсируется в сеть

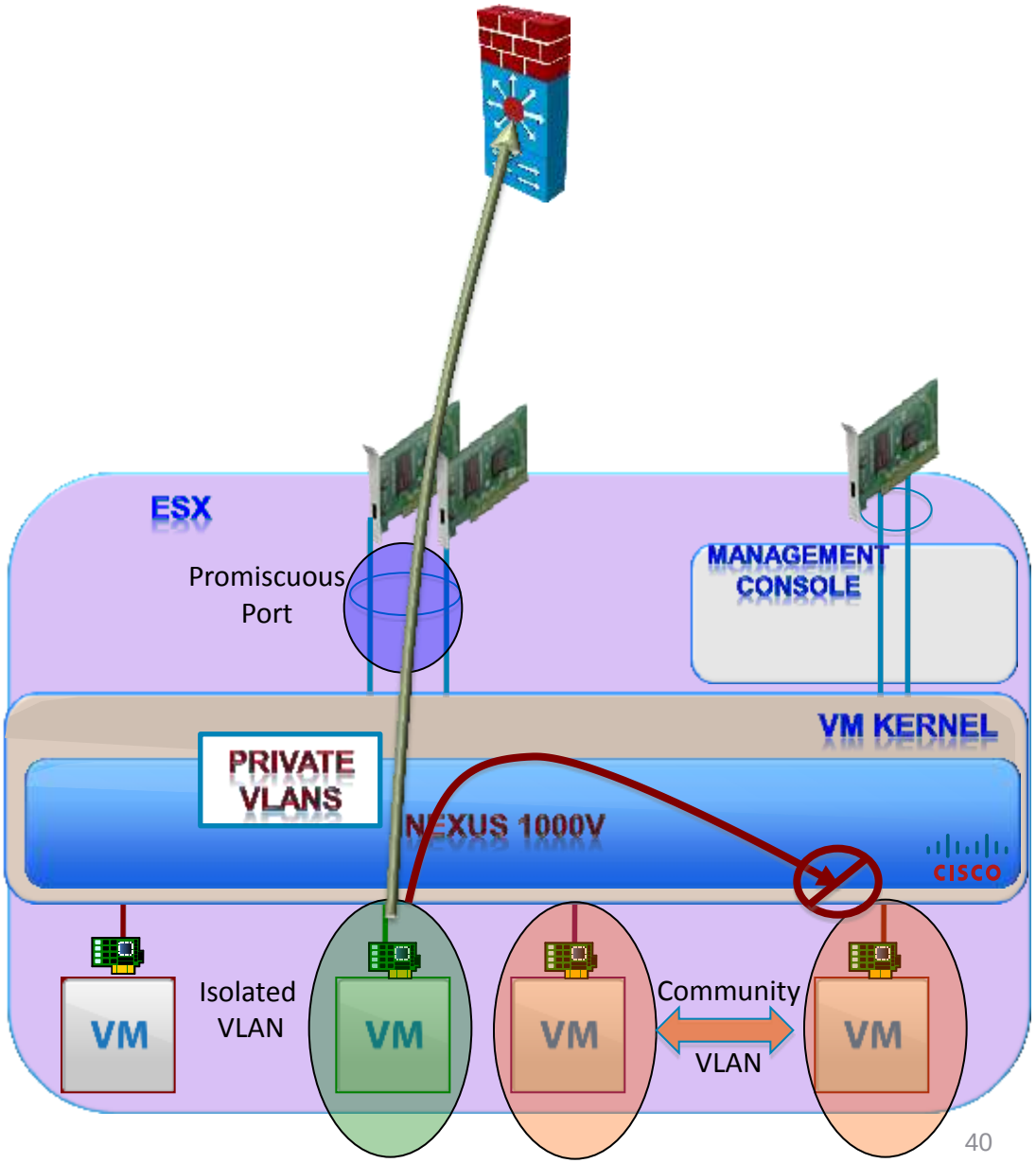


Мобильные настройки:

- Политики портов
- Состояние интерфейсов и счетчики
- Статистика

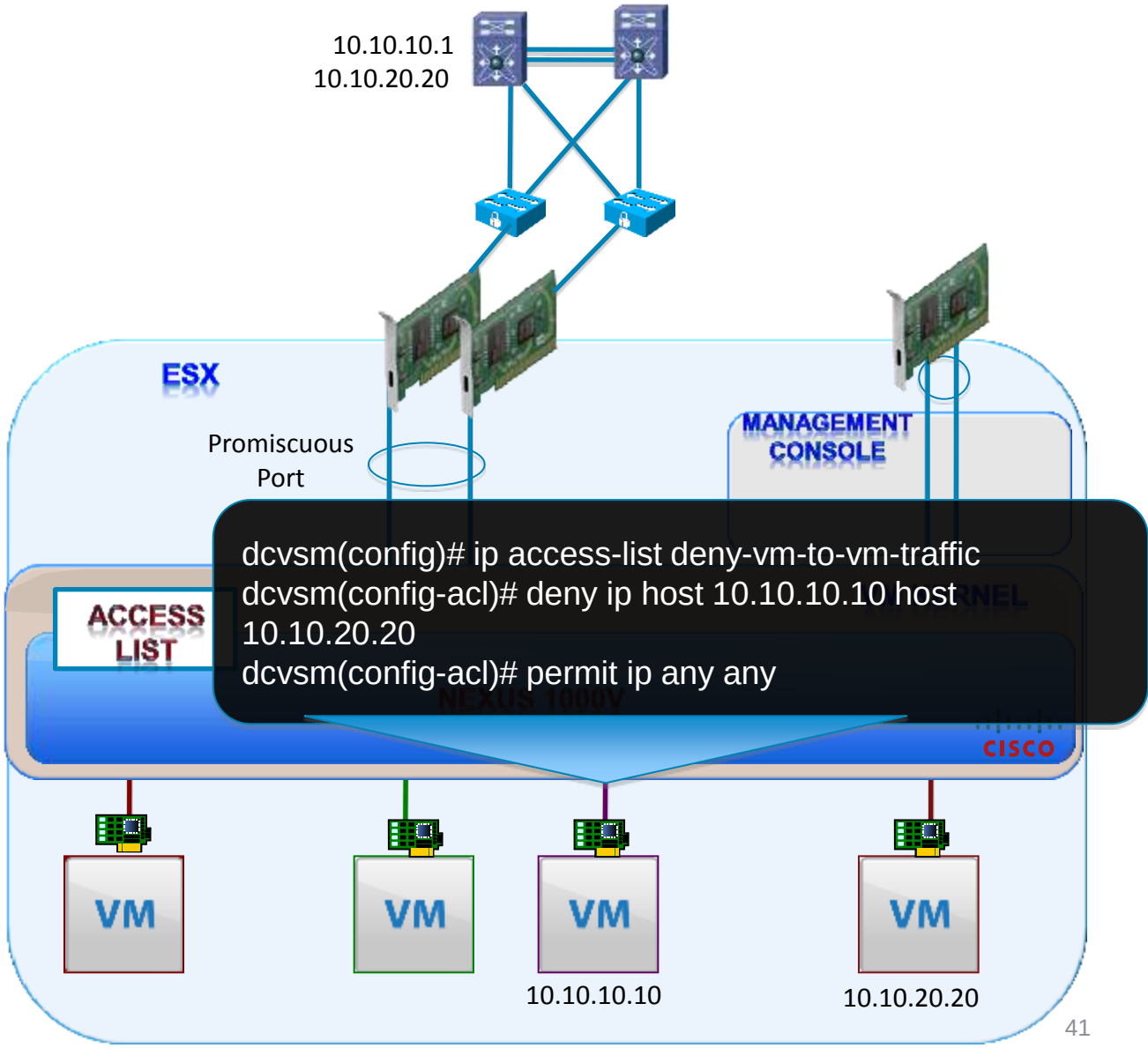
Изоляция VM: Cisco Private VLAN

- Private VLAN изоляция хостов из одной подсети на L2
- Поддержка традиционных Cisco PVLAN: порты Isolated и Community
- Физическая инфраструктура понимает PVLAN



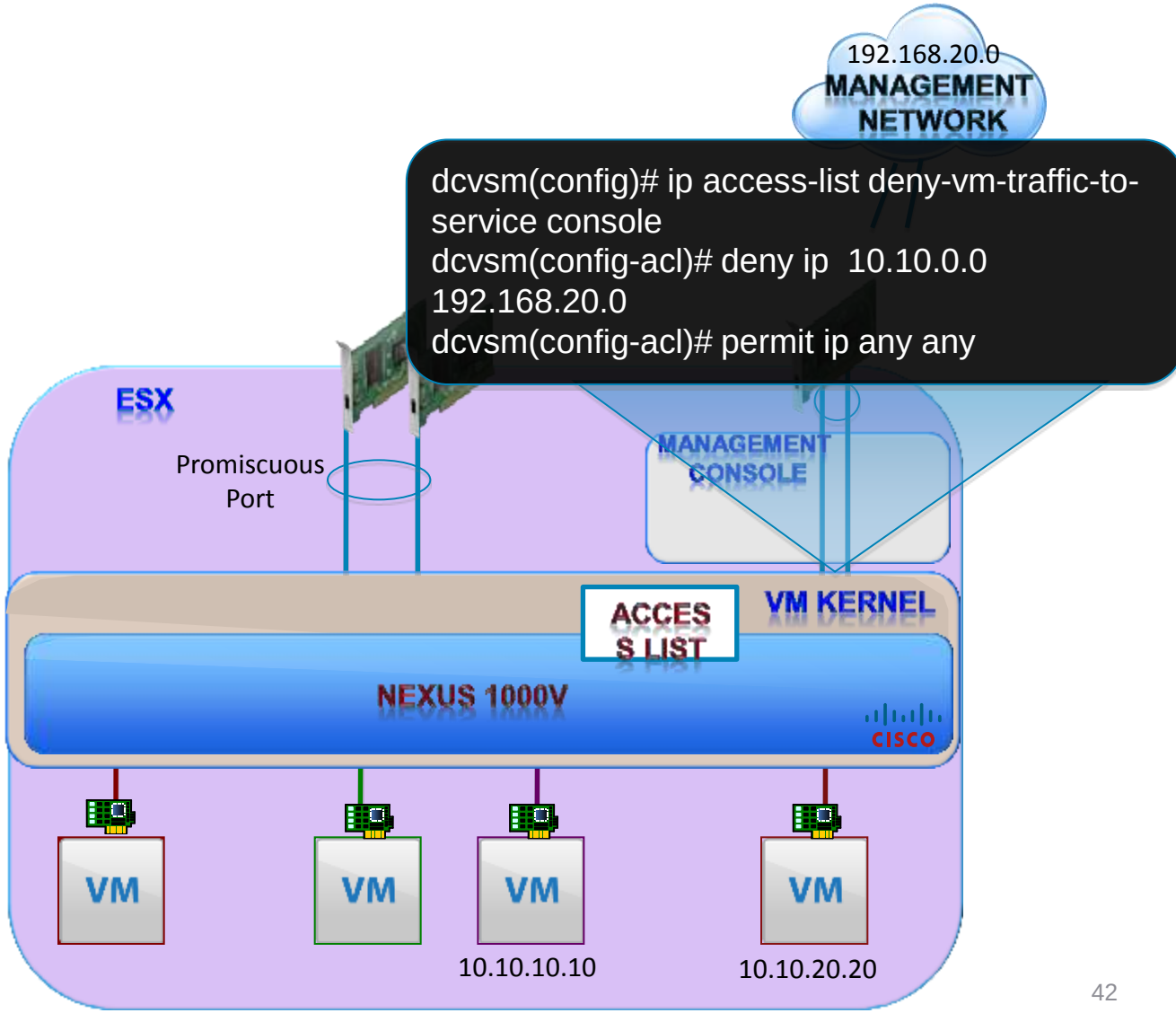
Изоляция VM и контроль трафика

- ACL на портах
- Ограничение трафика между VM
- Настройки как между физическими серверами
- Использовать вместе с VLANs, PVLAN



Разделение данных и трафика управления

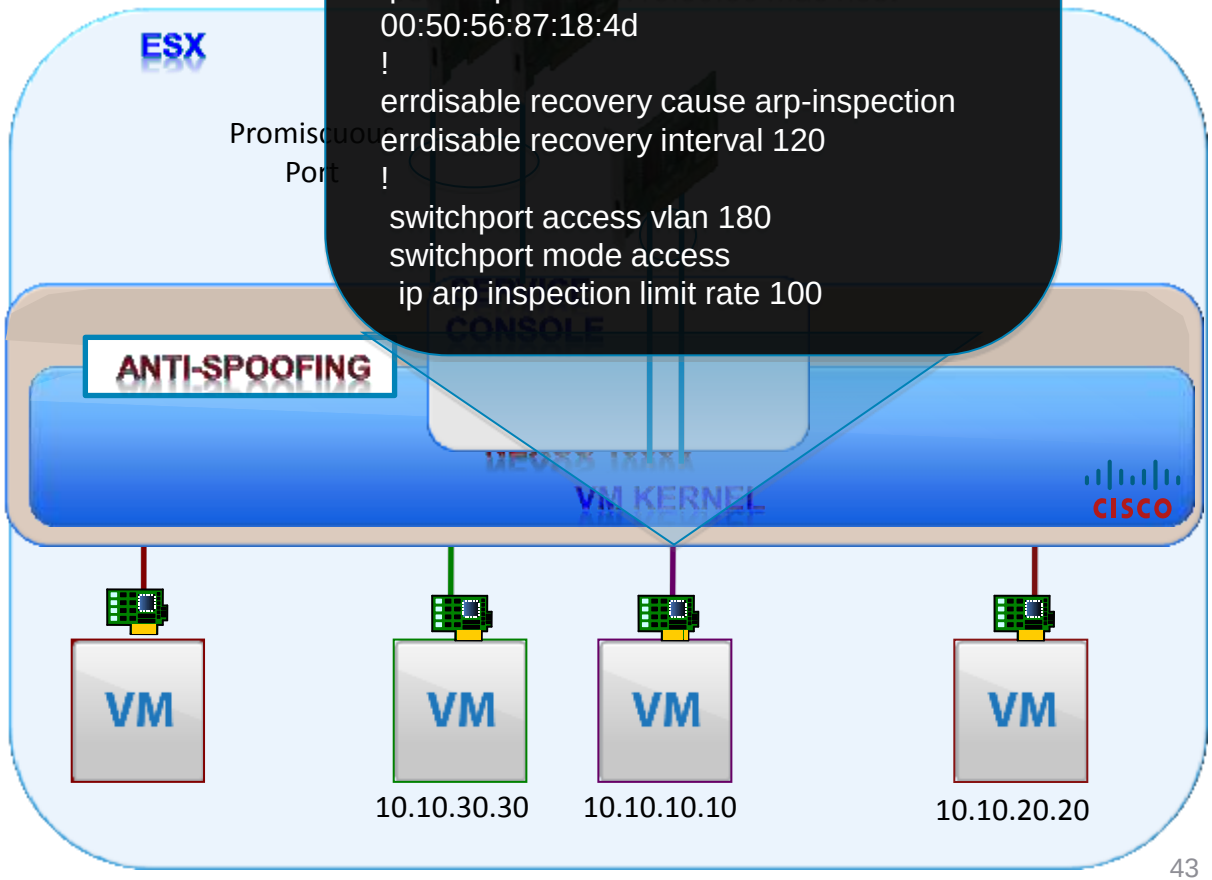
- Изолировать трафик управления от данных
- Физическое и виртуальное разделение



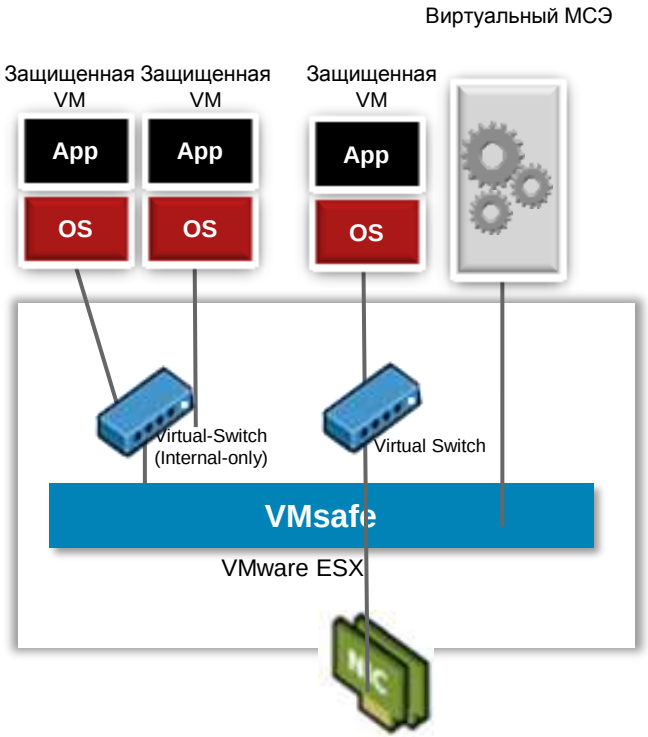
Anti-Spoofing

- Защита от атак man-in-the middle
- Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, Port Security

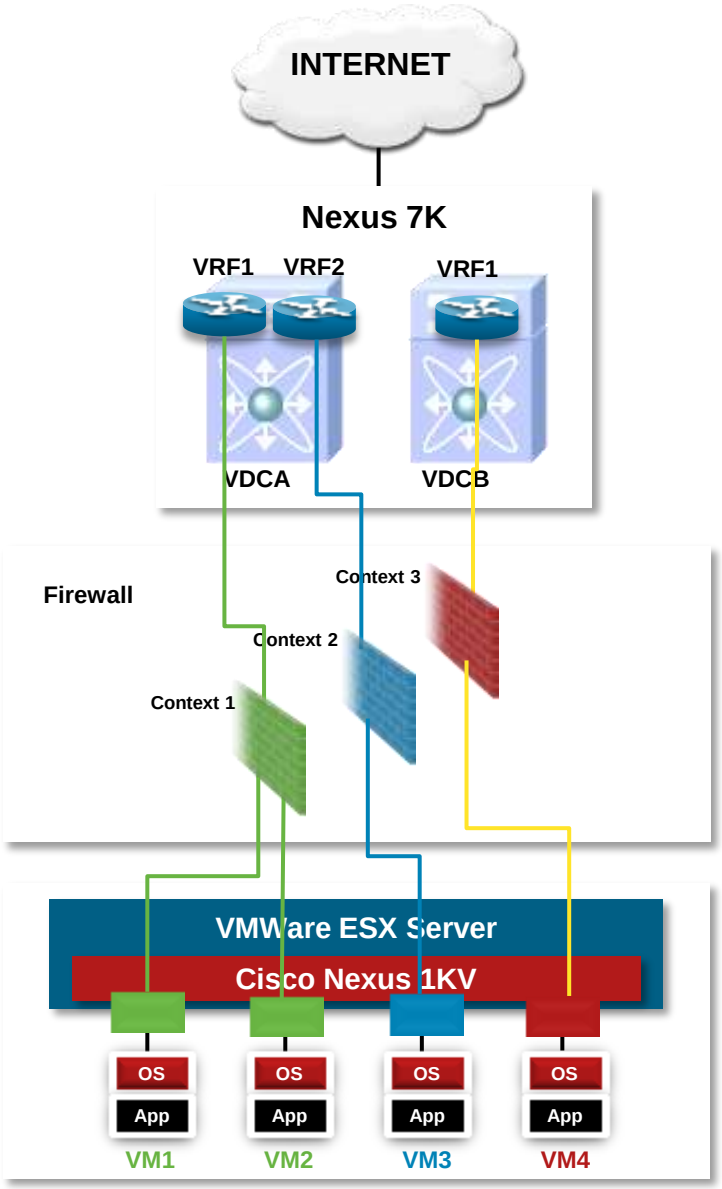
```
ip arp inspection vlan 180
!
ip arp inspection filter staticIP vlan  180
arp access-list staticIP
 permit ip host 10.10.10.10 mac host
00:50:56:87:18:2d
 permit ip host 10.10.20.20 mac host
00:50:56:87:18:3d
 permit ip host 10.10.30.30 mac host
00:50:56:87:18:4d
!
errdisable recovery cause arp-inspection
errdisable recovery interval 120
!
 switchport access vlan 180
 switchport mode access
  ip arp inspection limit rate 100
```



Сервисы безопасности
Варианты дизайна

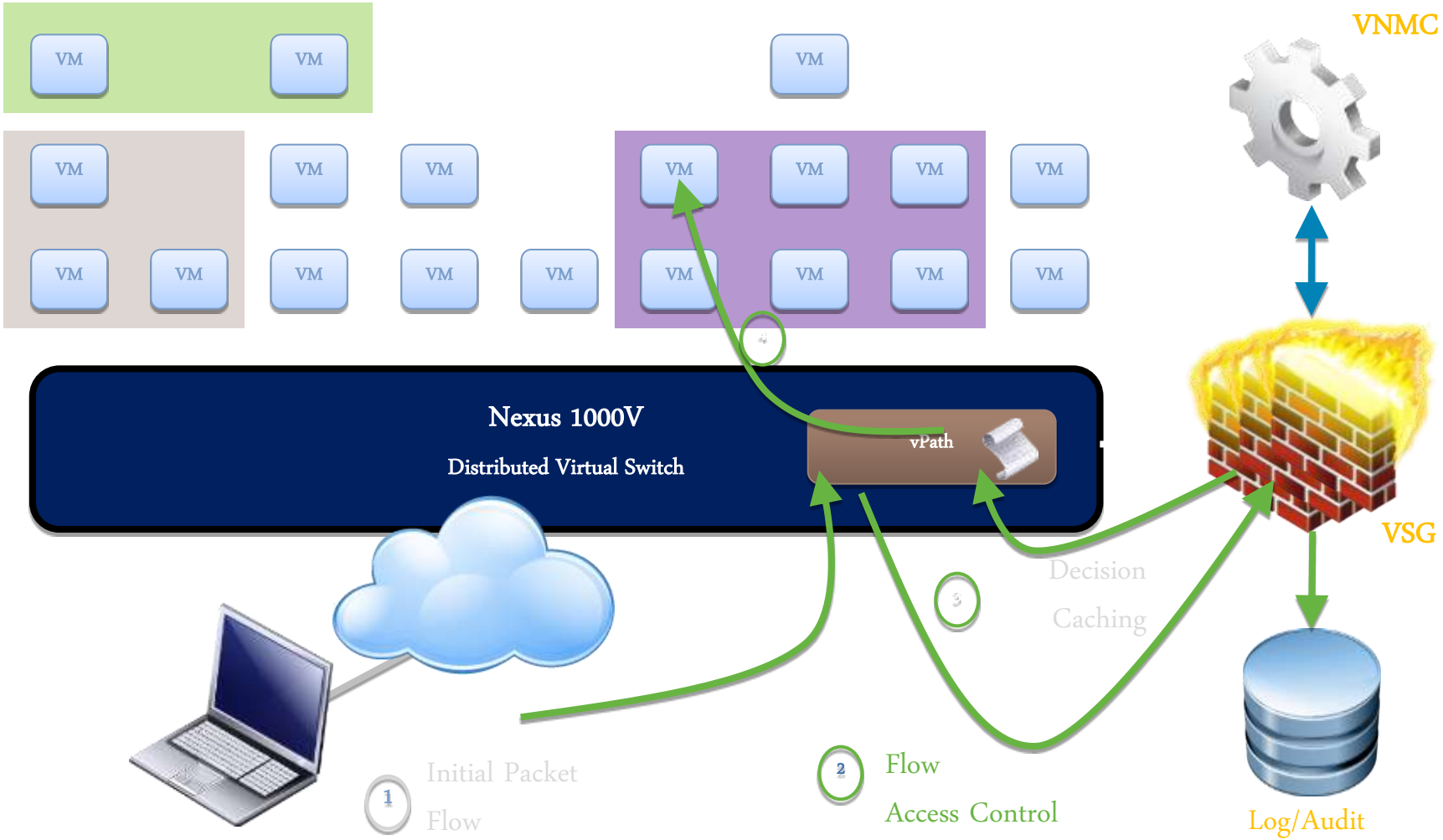


VMware VMsafe дает возможность разработки виртуальных устройств для мониторинга и контроля сетевой активности между всеми виртуальными машинами.

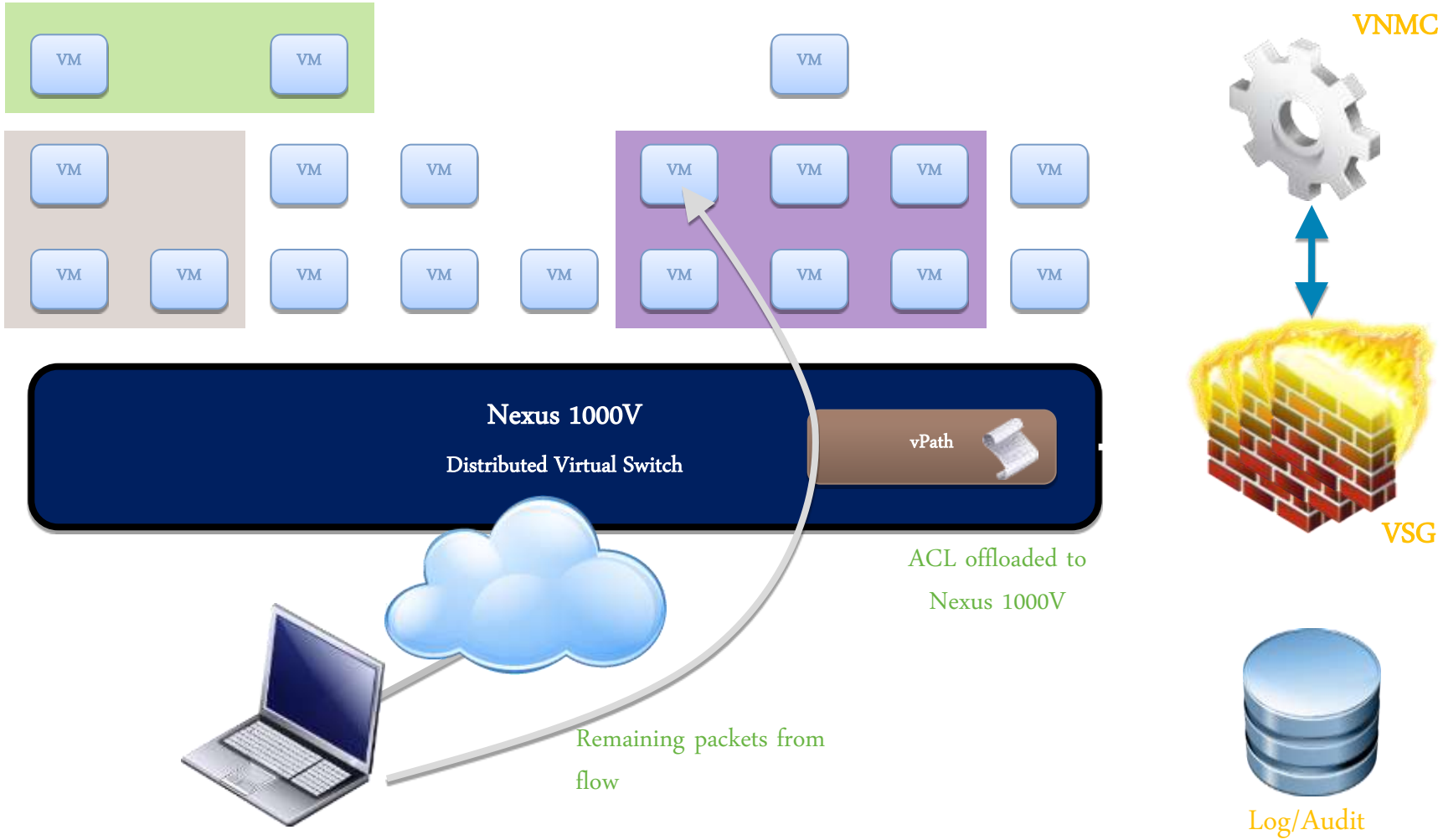


Virtual Security Gateway

Интеллектуальная защита с vPath



Virtual Security Gateway
Ускорение работы с vPath

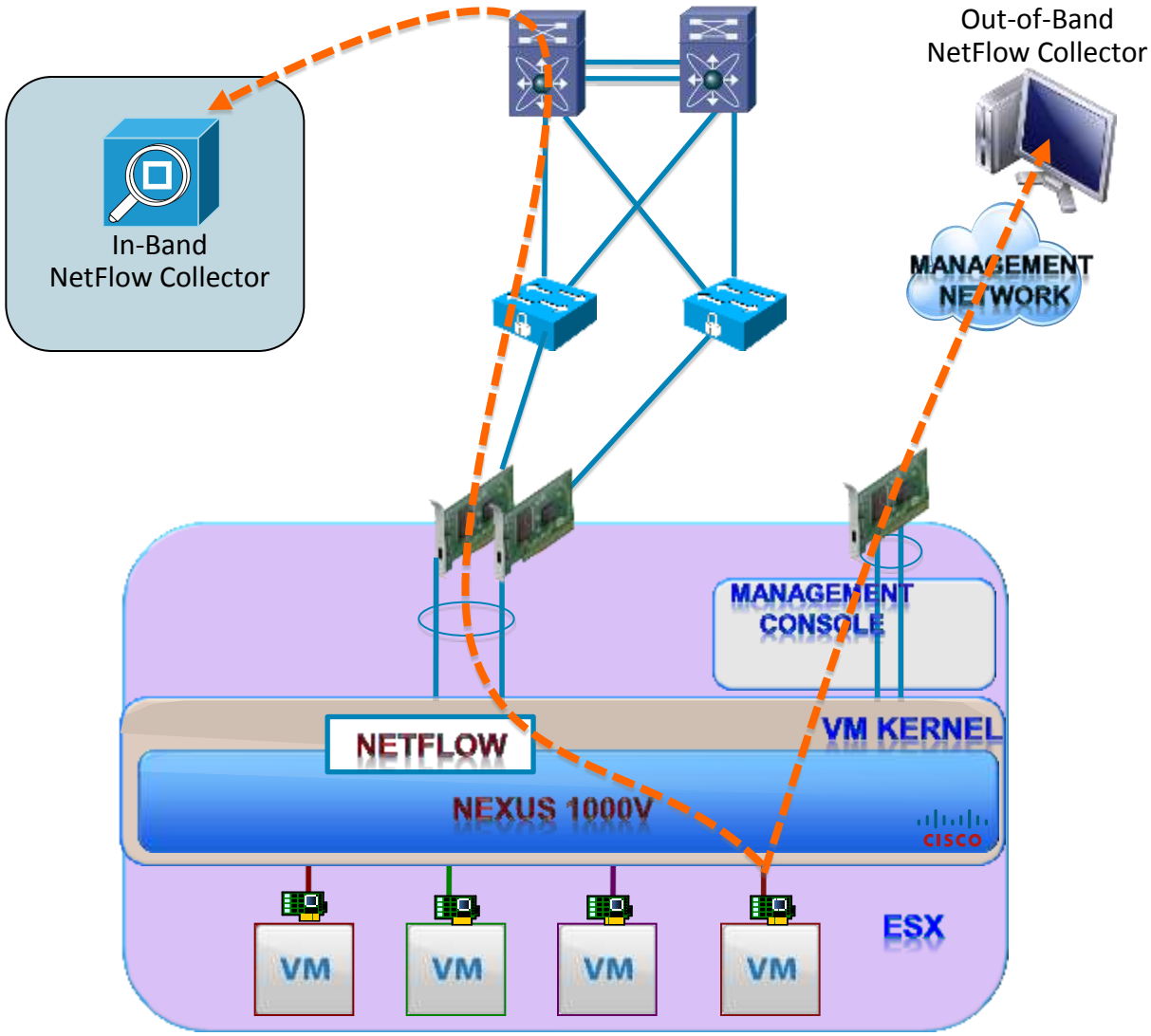


Анализ Netflow
Это нормально или нет?

Видимость трафика между VM

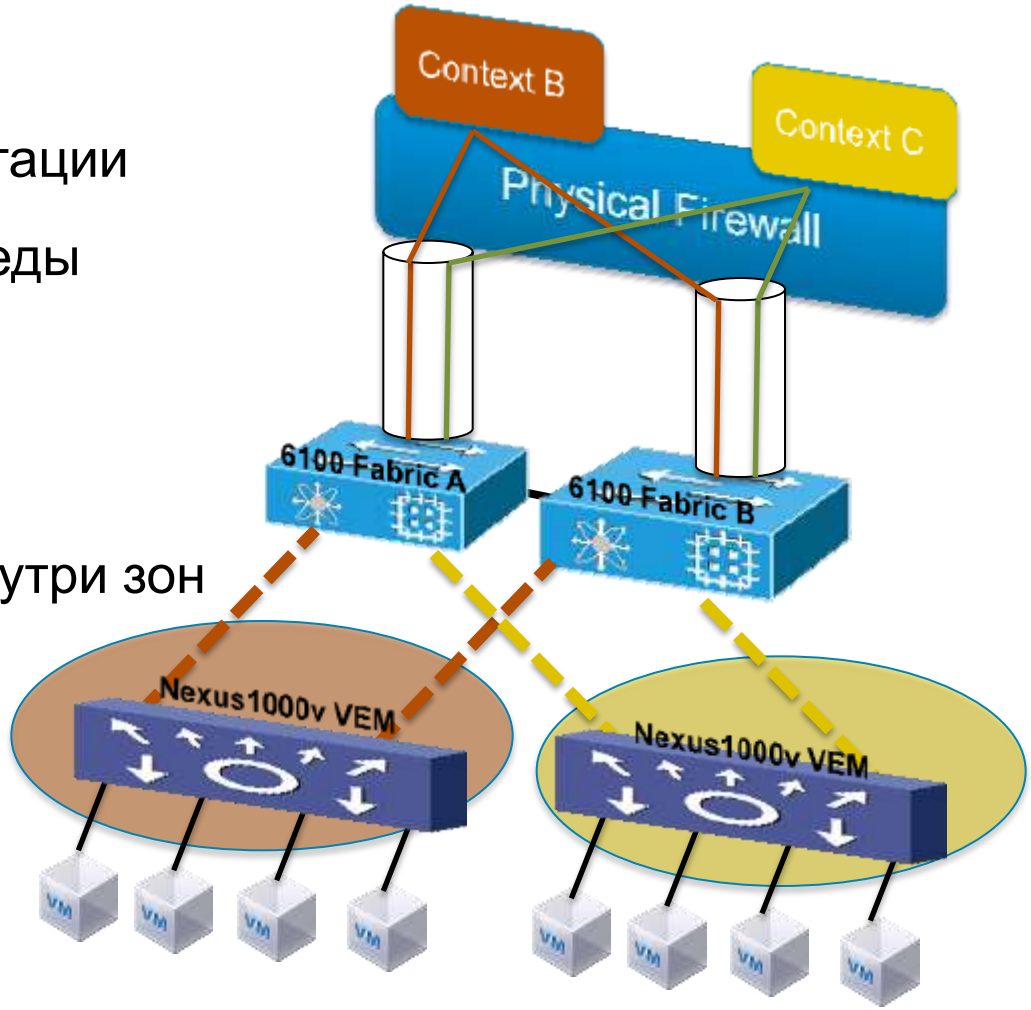
NetFlow

- N1000V требуется Netflow source interface
  - По умолчанию - Mgmt0
  - Поддержка формата v9

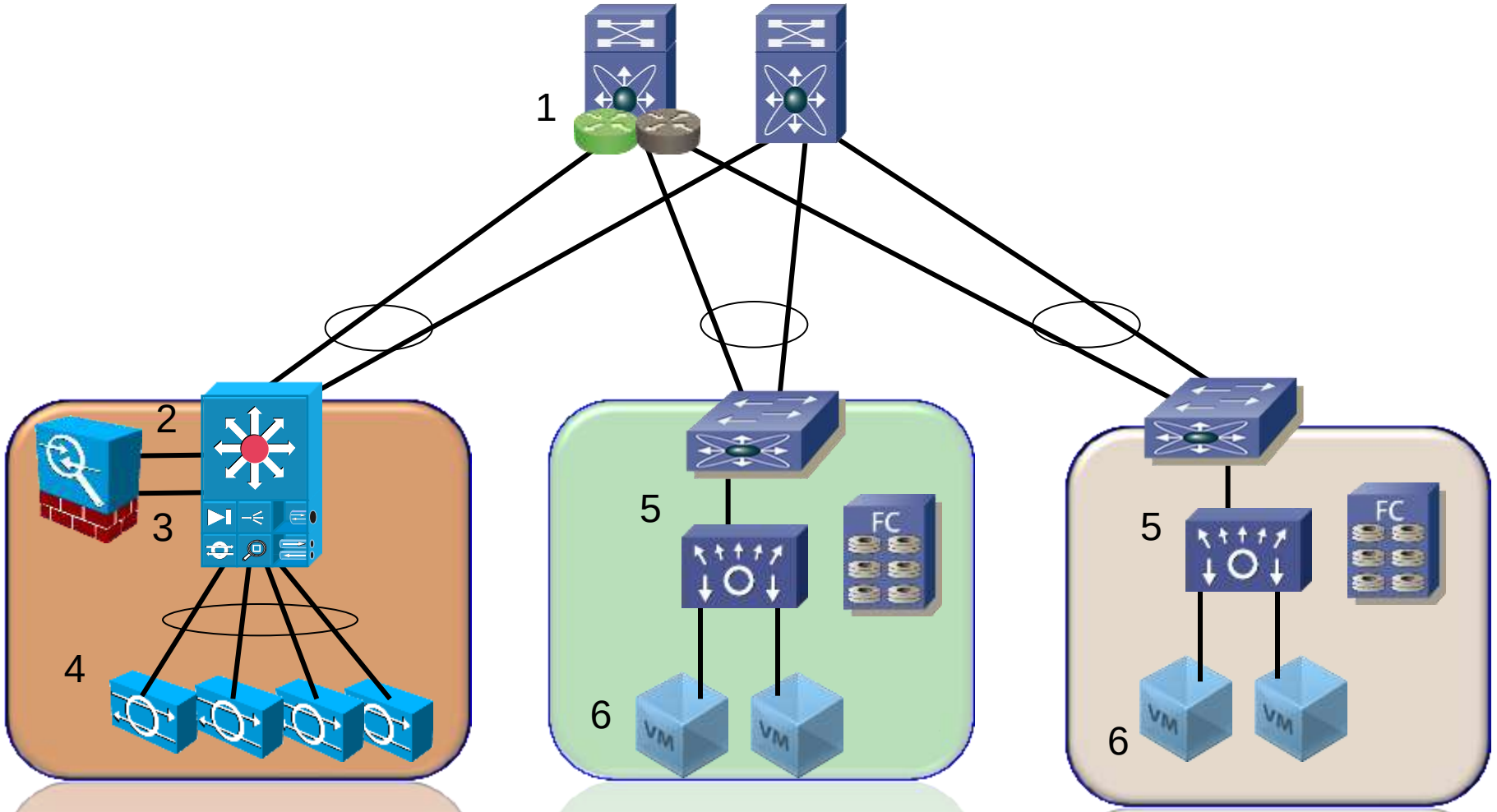


Зональный дизайн с использованием физических устройств

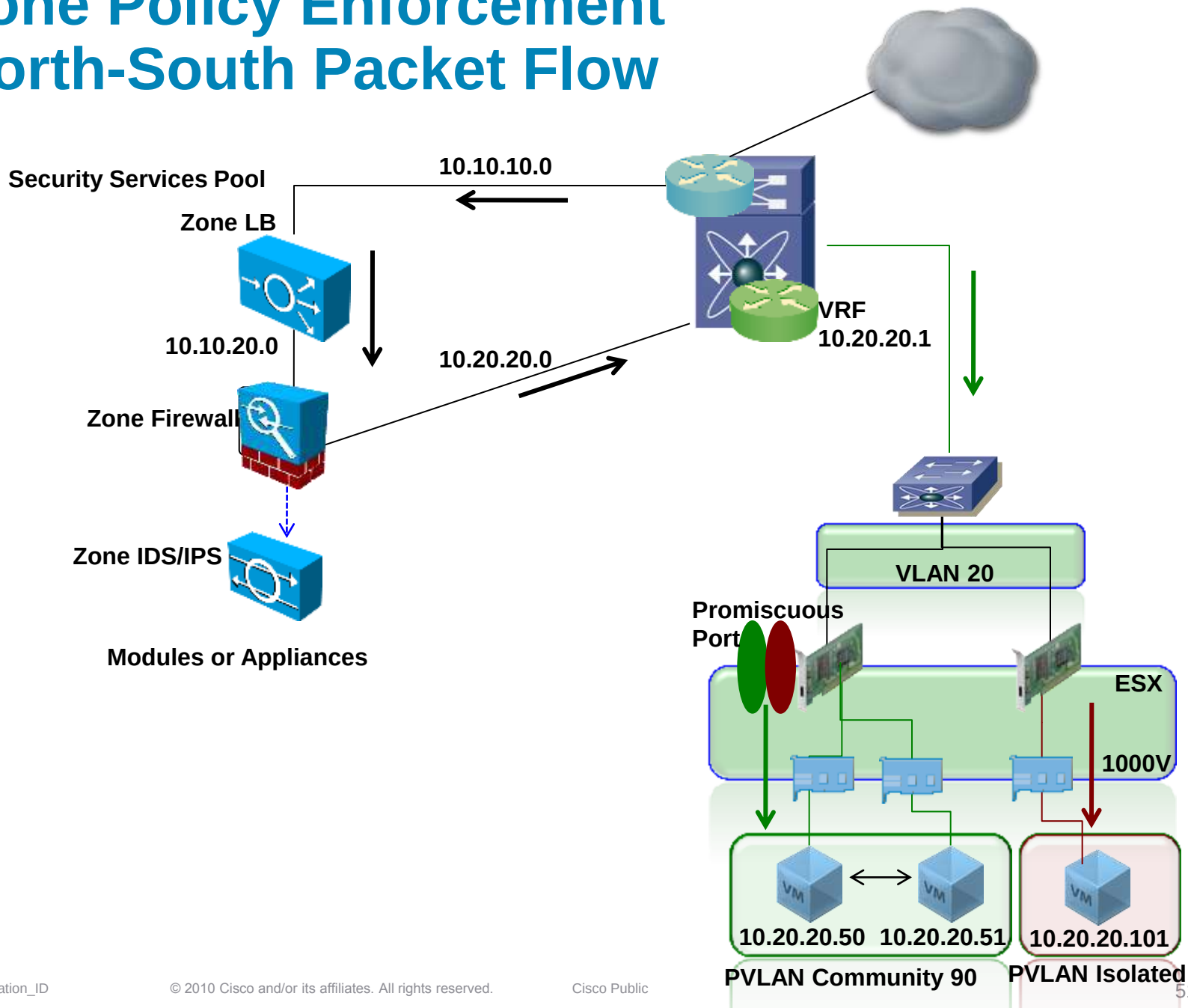
- Контексты используются для поддержки зональной сегментации
- Сегментация виртуальной среды (Nexus 1000V)
- Направление VM трафика к контекстам МЭ
- Сегментирование трафика внутри зон
  - VM трафик
  - Трафик управления
- Защиту L2/L3 на уровне зоны



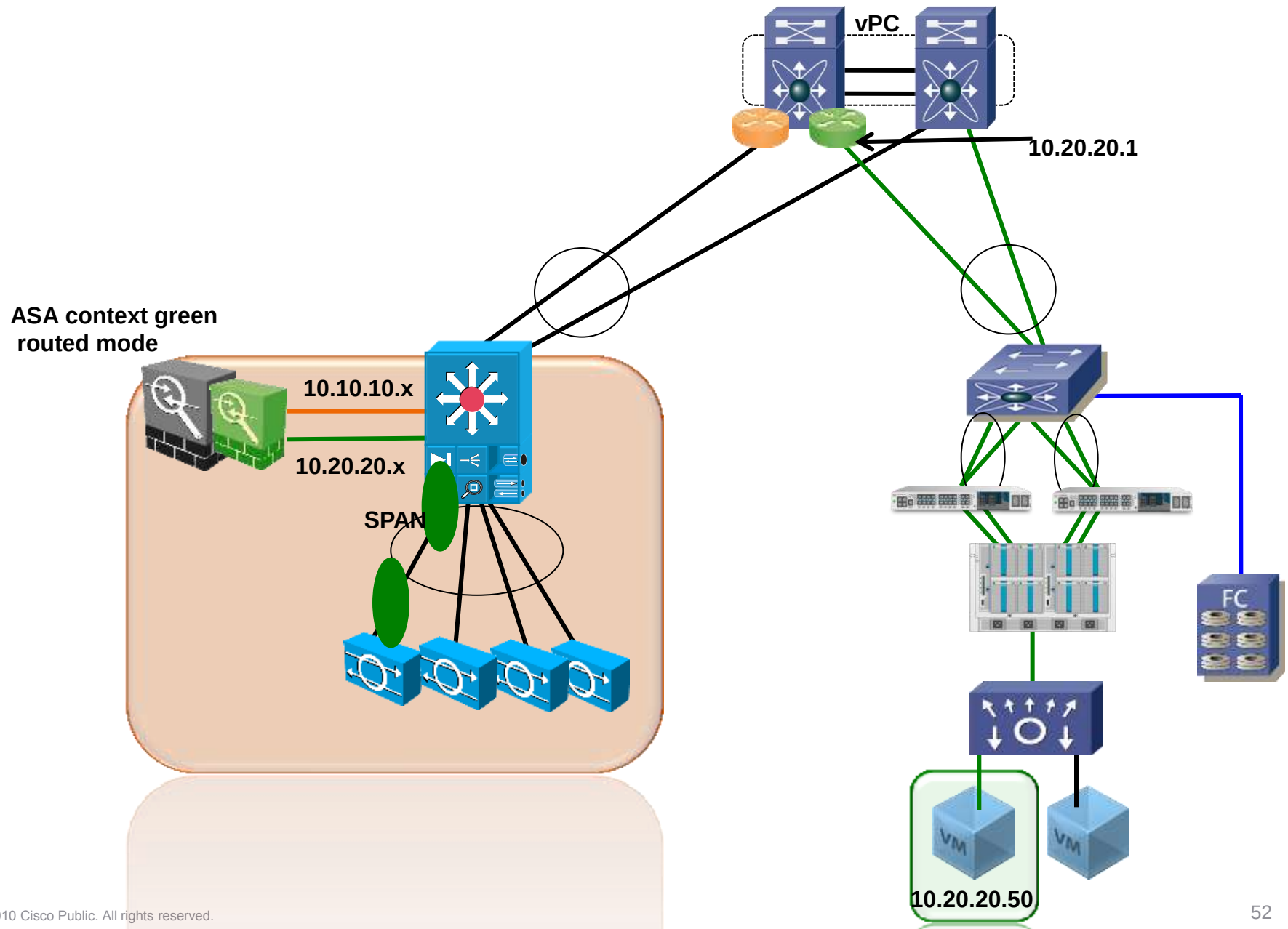
Пример для входящего трафика



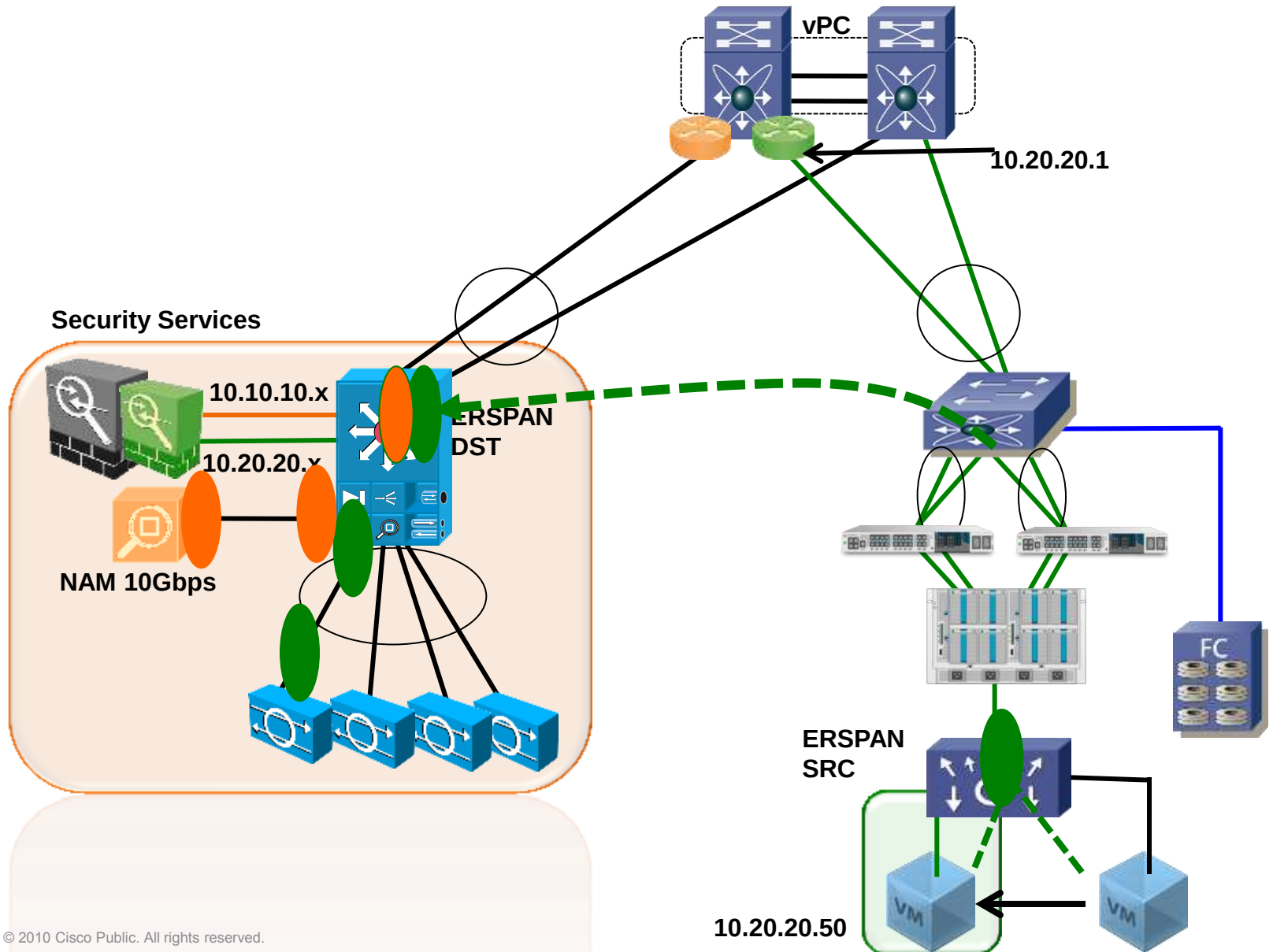
Zone Policy Enforcement North-South Packet Flow



Межсетевой экран и IDS на зону



Мониторинг трафика VM



Заключение

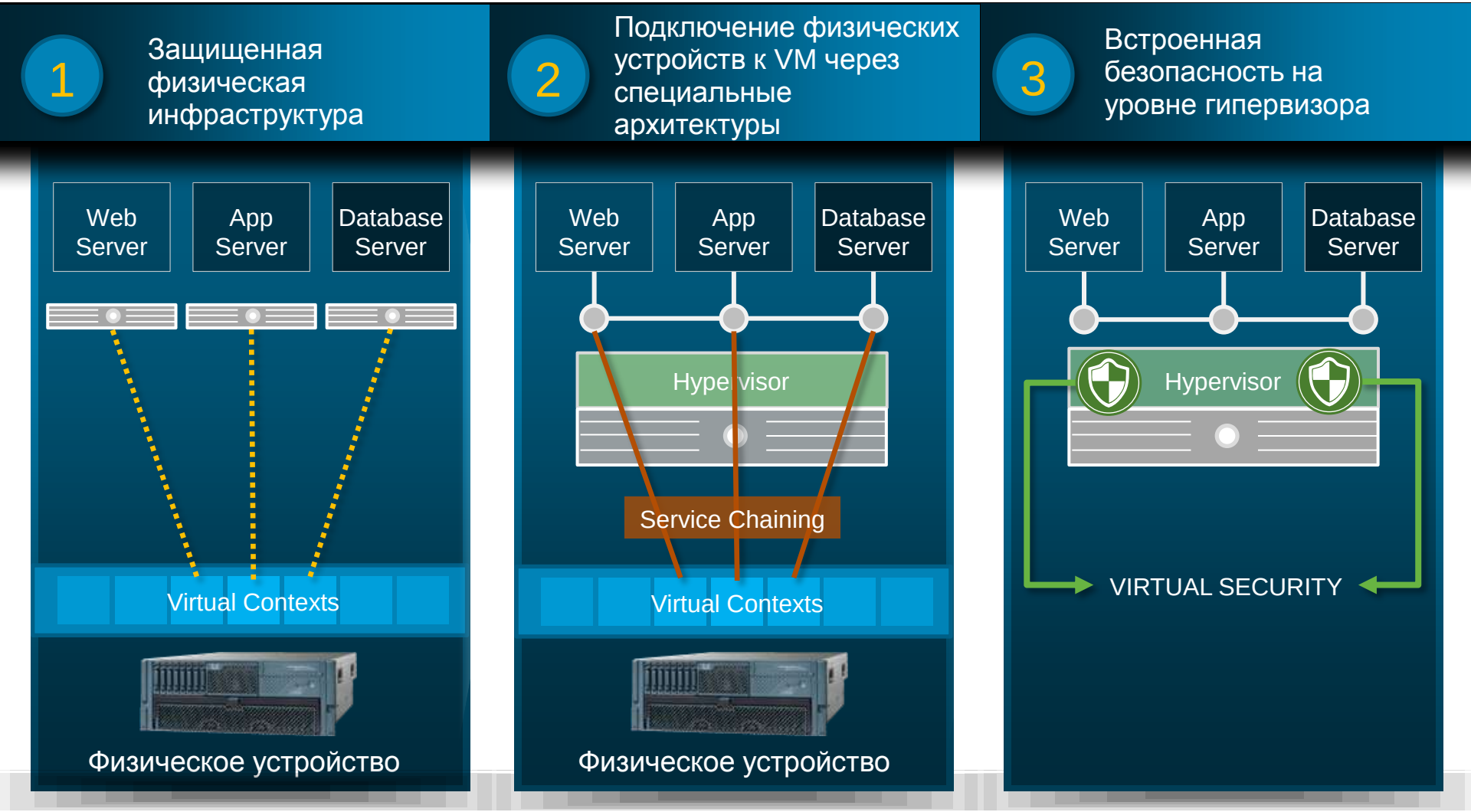
Помните…

- Общепринятые практики безопасности все еще актуальны
- Ограничивайте взаимодействие между серверами и ресурсами
- Защищайте ОС физического сервера, гипервизор и гостевые ОС
- Используйте антивирус, применяйте заплатки и обновления

Заключение

- Виртуализация устройств
  - Масштабирование сетевых компонентов и устройств безопасности
  - Гибкие варианты интеграции
  - Аккуратность планирования – залог отсутствия сложностей
- Виртуализация серверов
  - Защита виртуальных машин
  - Обеспечение прозрачности работы виртуальных машин
  - Разделение обязанностей
  - Не делайте то, что не будете делать на физических серверах

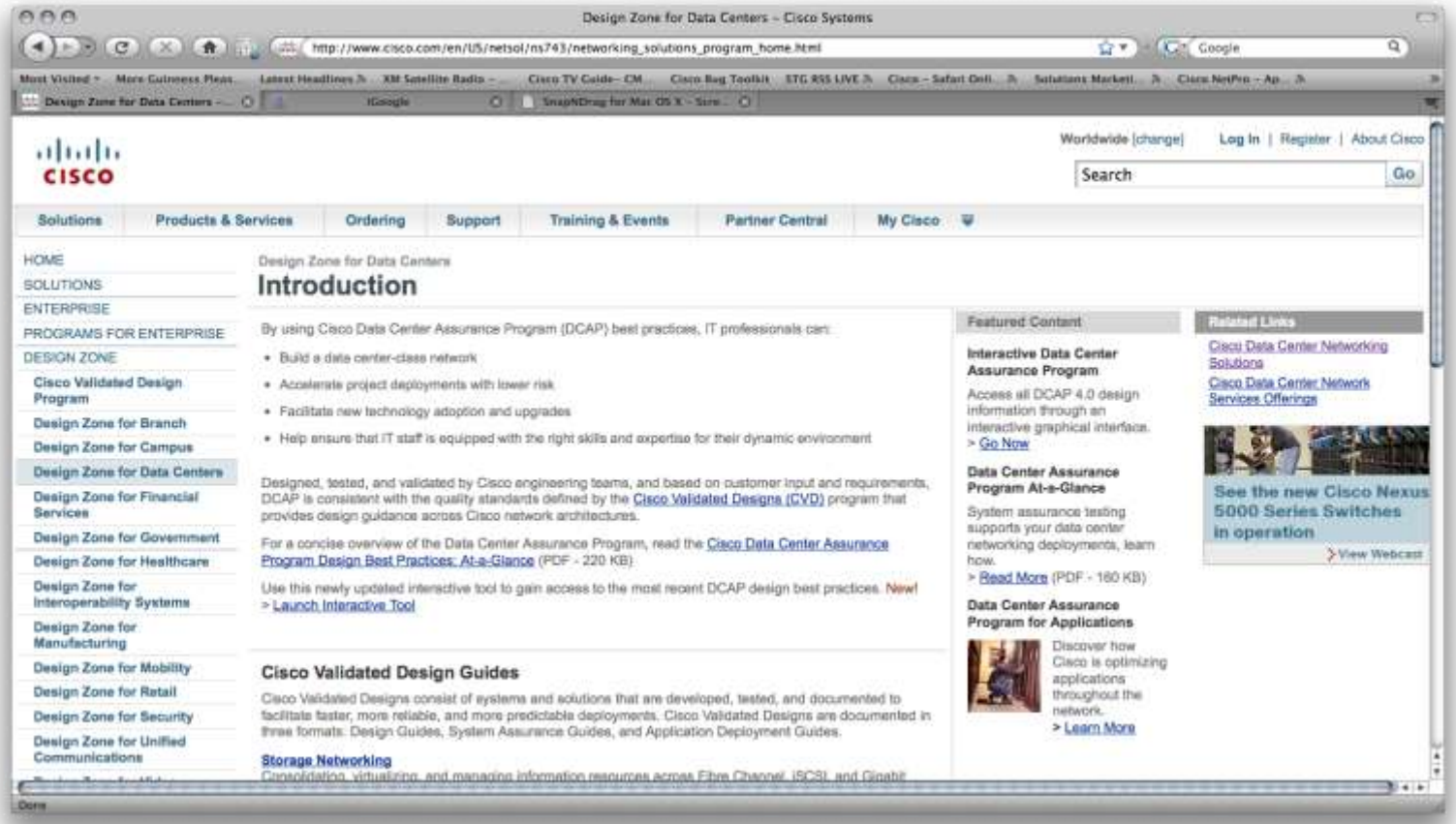
Над чем работает Cisco



Дополнительная информация

- Data Center Design Zone

  http://www.cisco.com/go/designzone



Вопросы и Ответы

Мы хотели бы узнать Ваше мнение

Пожалуйста,
заполните анкету


CISCO