Cisco Expo 2012

Безопасность виртуализации и облачных вычислений

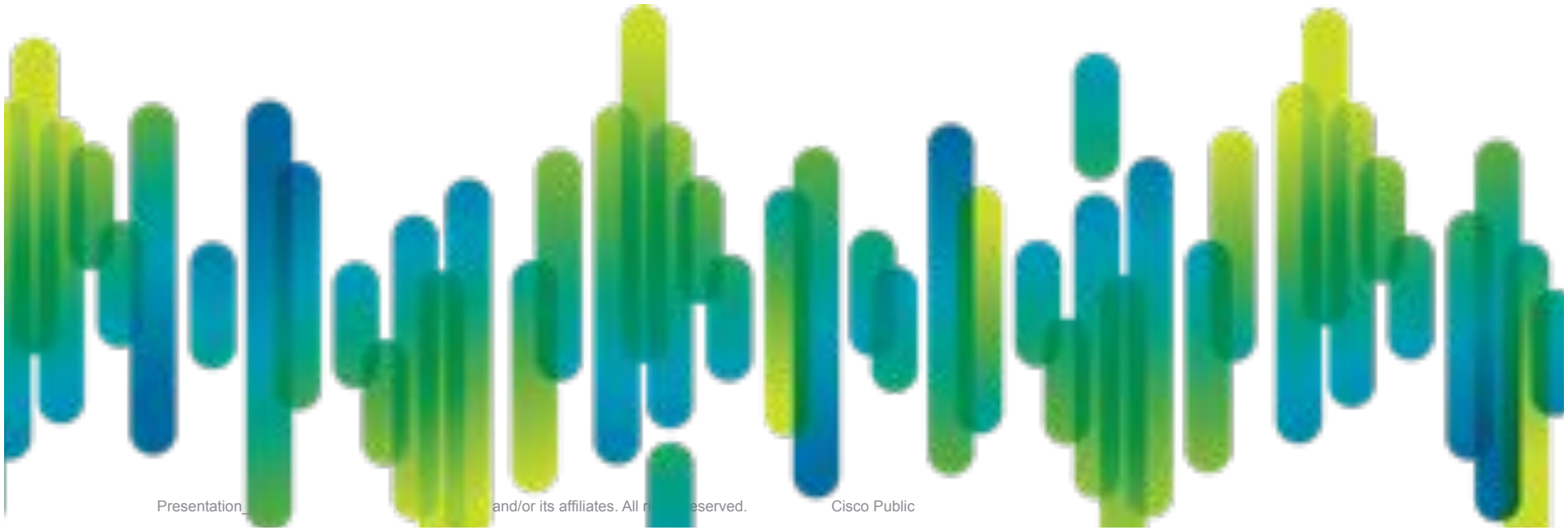
Владимир Илибман
Cisco Systems

О чем пойдет речь:

1. Особенности безопасности виртуальных сред
2. Безопасность сетевой виртуализации
3. Виртуализация сетей хранения данных
4. Безопасность виртуализации вычислений
5. Внедрение политик и сегментация для виртуальных машин
6. Сервисы безопасности для виртуальной среды
7. Безопасность облачных сервисов

Эволюция IT (IT Journey)

Особенности безопасности виртуальных сред

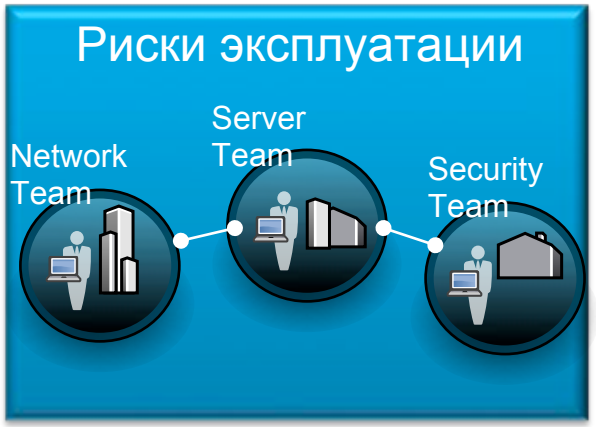


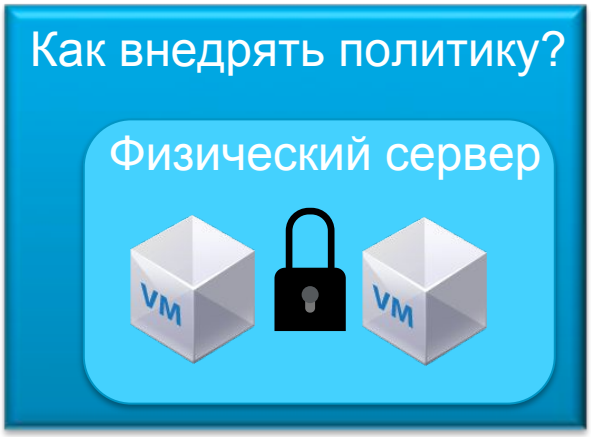
Соблюдение баланса

Риски безопасности виртуализации связаны с высокой консолидацией разнотипных данных, вычислительных и сетевых ресурсов в единой физической системе.

Виртуальный IT-зоопарк

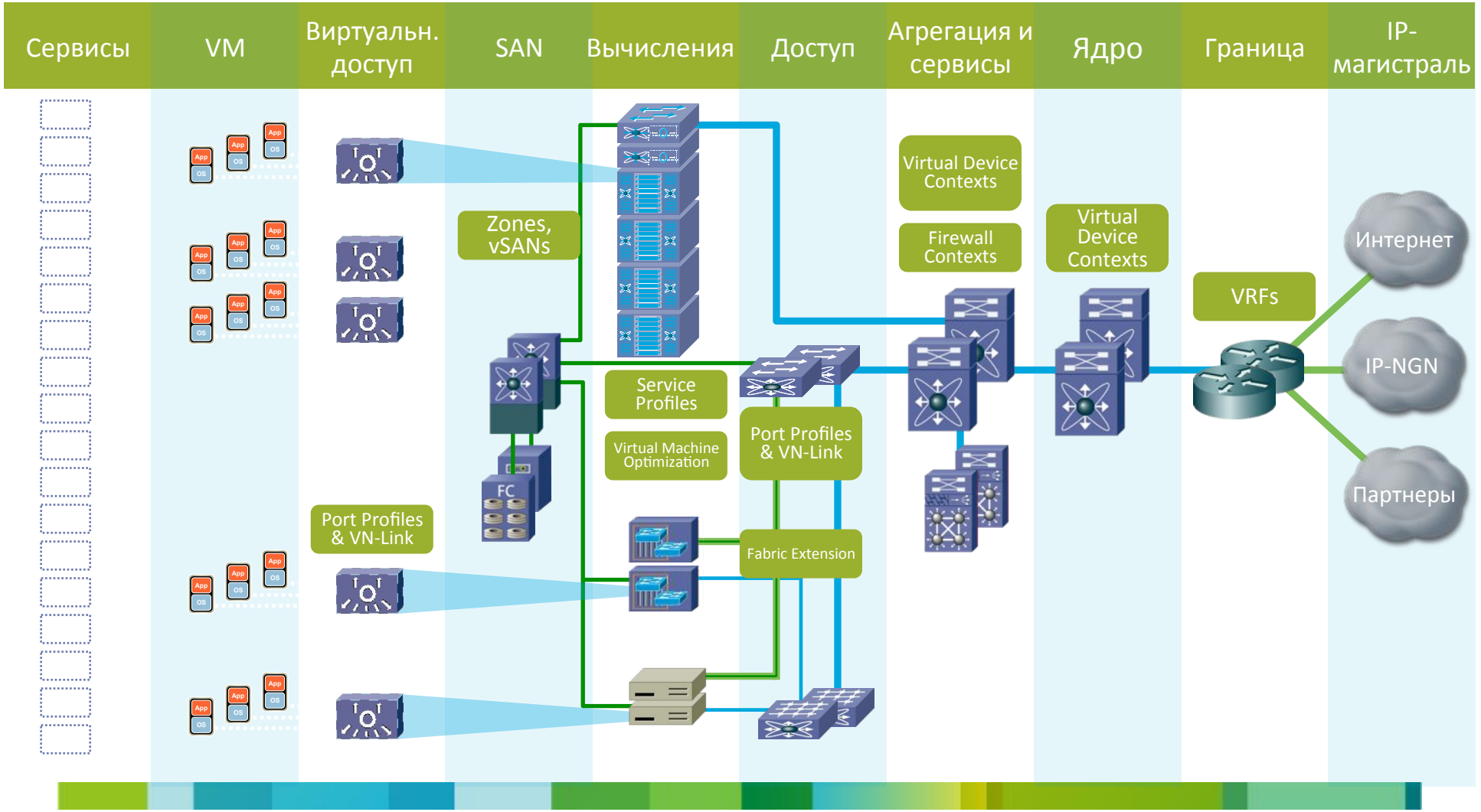
Основные вызовы безопасности в виртуальной среды



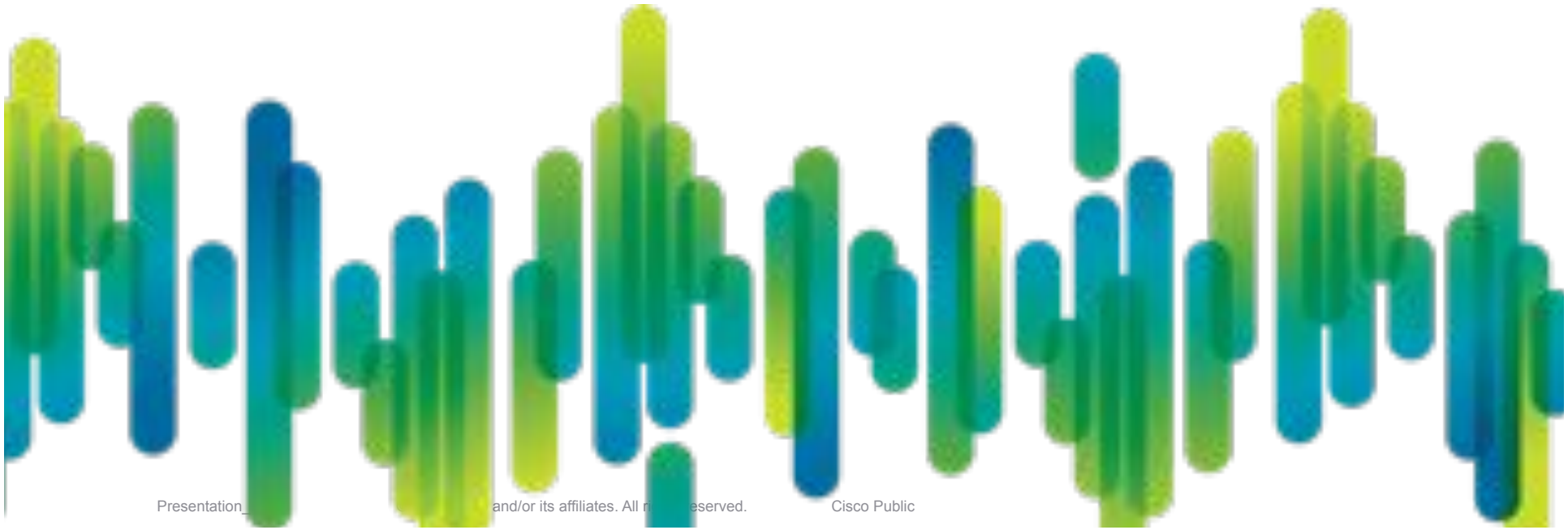


Архитектура Cisco Data Center

Зоны виртуализации



Безопасность сетевой виртуализации



Технологии сетевой виртуализации

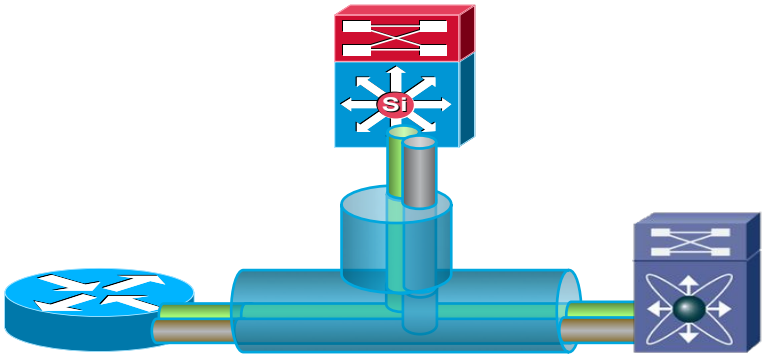
Разделение устройства

VLANs

VRFs

VDC (Virtual Device Context)

Виртуализация подключения

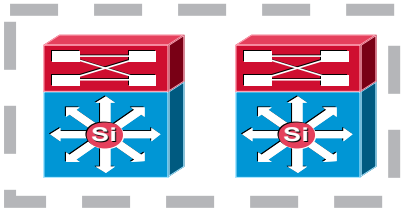


L3 VPNs – MPLS VPNs, GRE, VRF-Lite, MPLS services (L2/L3) over GRE

L2 VPNs - AToM, Unified I/O, VLAN trunks

Evolving – TRILL, 802.1ah, 802.1af

Объединение устройств



VSS

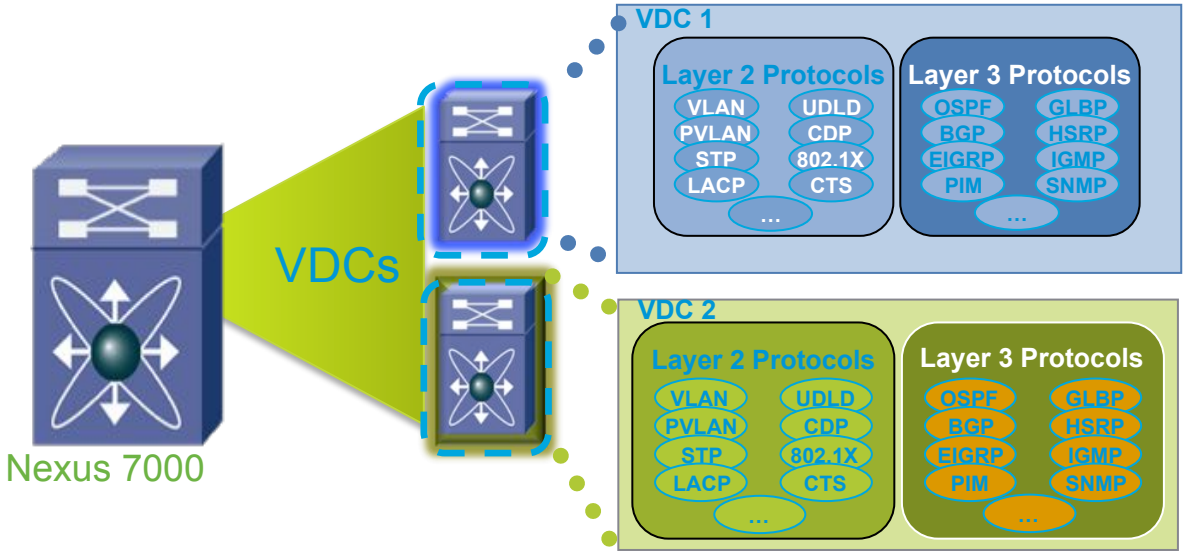
Stackwise

Virtual Port Channel (vPC)

HSRP/GLBP

Контексты коммутатора с помощью VDC

Ключевая функция

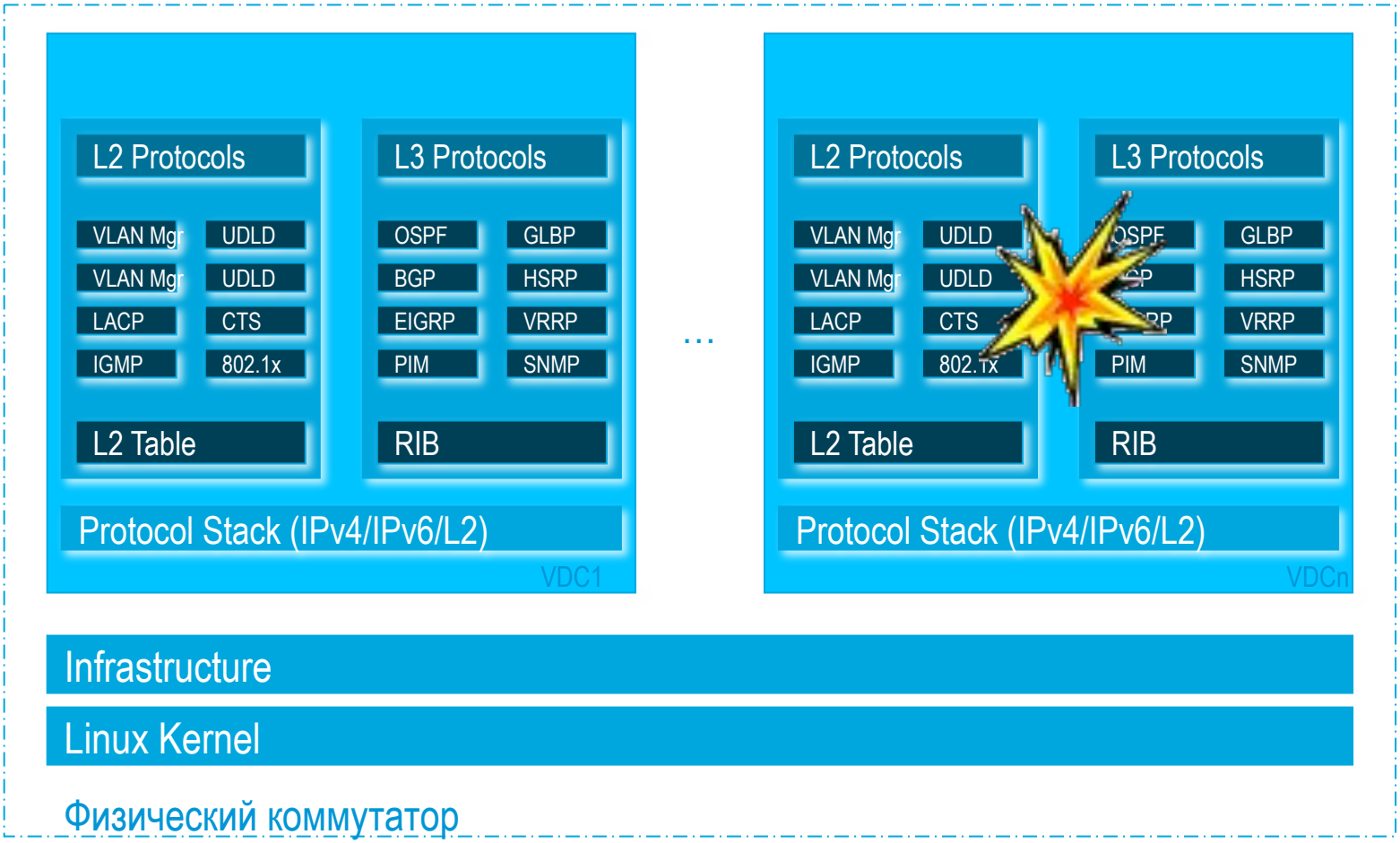


Nexus 7000 VDC – Virtual Device Context

- Разделение **data plane** и **control plane**
- Надежное разделение контекстов управления (**management plane**)
- Гибкое разделение аппаратных и программных ресурсов между контекстами – портов, L2/L3 стеков, VLAN, VRFs, таблиц маршрутизации
- Контроль выделяемых под контекст ресурсов
- **Изоляция процессов и программных сбоев**

Архитектура Virtual Device Contexts

Virtual Device Contexts обеспечивает виртуализацию на уровне устройства, запуская множество виртуальных копий устройства на физическом коммутаторе



Virtual Device Contexts

Управление VDC – модель RBAC

Network Administrator имеет доступ к глобальной конфигурации, может создавать/удалять VDC's и выделять ресурсы для VDC's…

VDC Administrator может изменить любую конфигурацию ресурсов, выделяемых на VDC, а также может создавать пользовательские роли, относящиеся к этому VDC с подмножеством конфигурационных команды ...

VDC User Role ограниченная роль в конкретном VDC, которая может управлять конфигурацией как это определено VDC Администратором…

Сертификация безопасности Virtual Device Context (VDC)

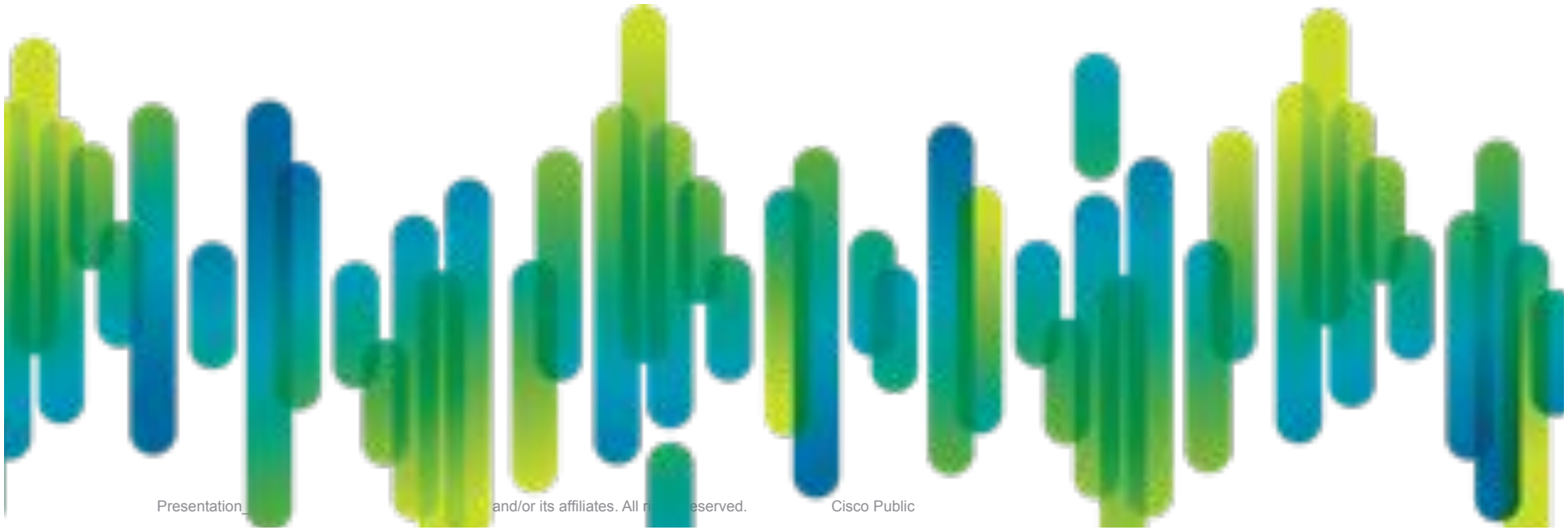
- Разделение VDC индустриально сертифицировано .
- NSS Labs сертифицировал использование Cisco Nexus 7000 VDC функционал для Payment Card Industry (PCI) среды в 2010 году.

  http://www.nsslabs.com/research/network-security/virtualization/cisco-nexus-7000-q2-2010.html
- Federal Information Processing Standards (FIP-140-2) сертификация была получена в 2011году

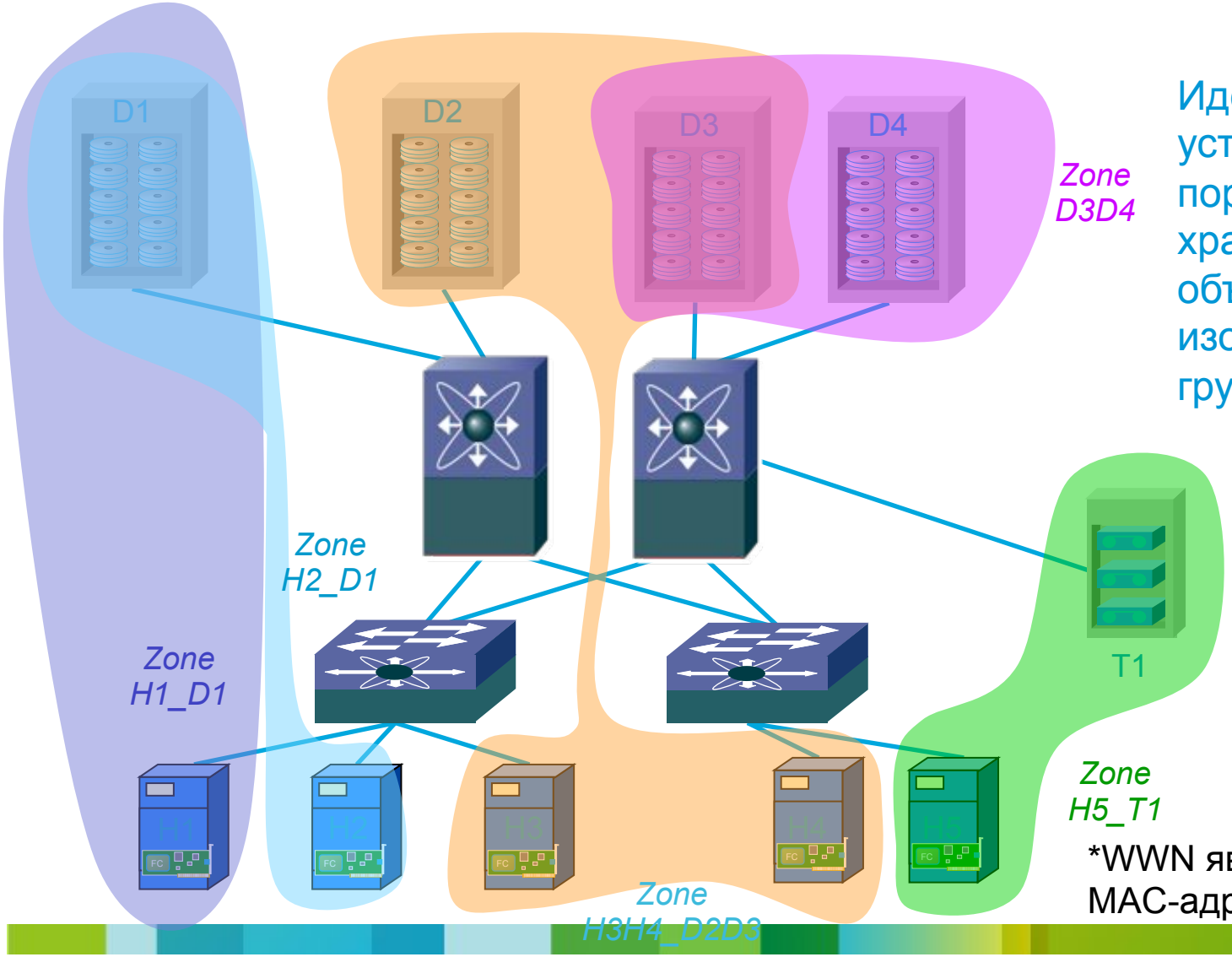
  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1533.pdf
- Cisco Nexus 7000 получил сертификацию по требованиям Common Criteria с уровнем соотствествия EAL4 в 2011 году.

  http://www.niap-ccevs.org/cc-scheme/st/vid10349/

Виртуализация сетей хранения данных



Доступ к SAN: зонирование FC



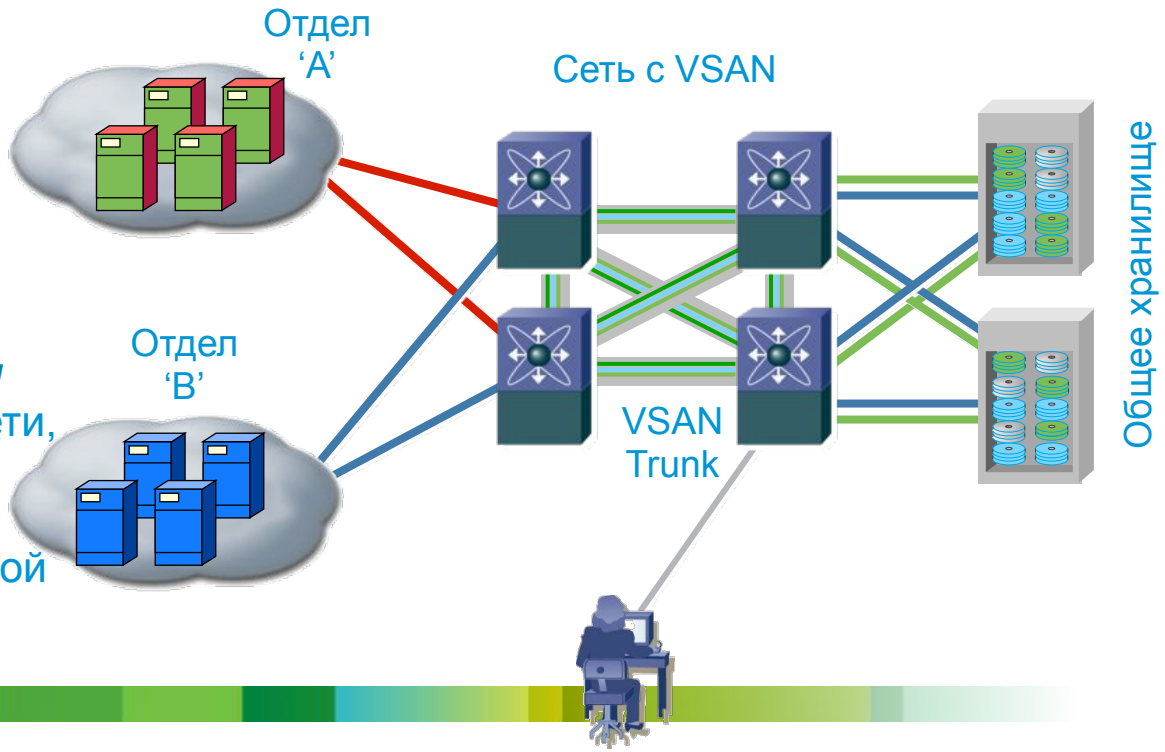
Идентификаторы устройств и портов сети хранения (WWN*) объединяются в изолированную группу.

*WWN является аналогом MAC-адресов в Ethernet

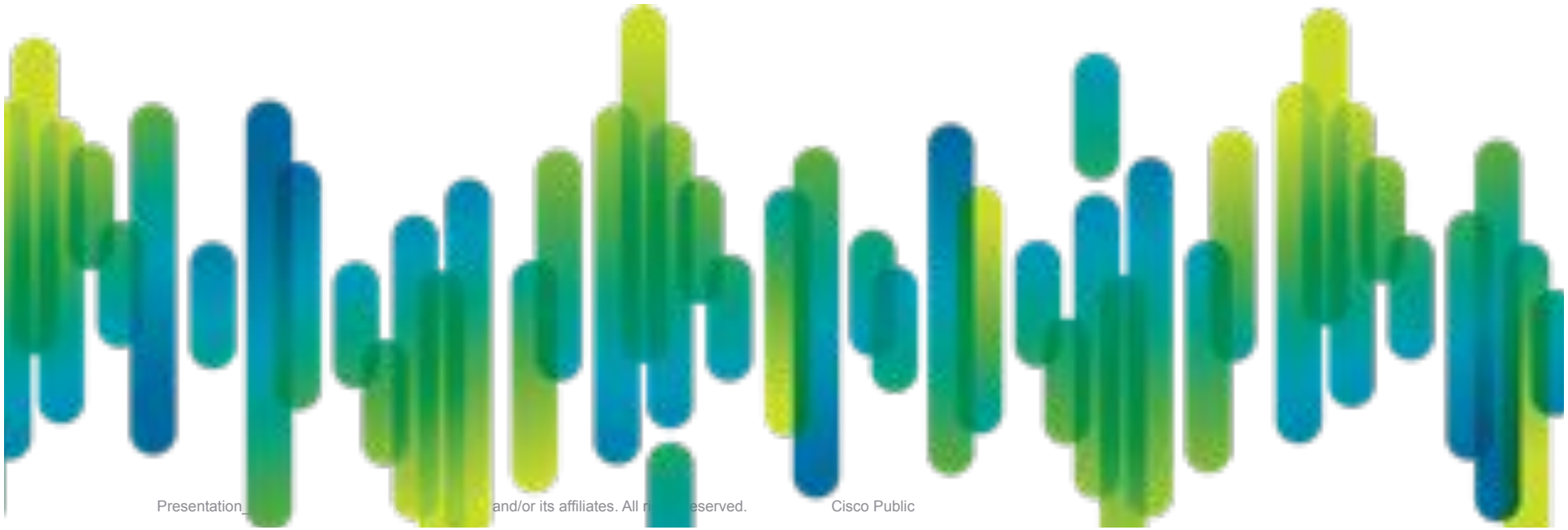
Безопасность уровня доступа: Виртуальные SAN (VSAN)

- Виртуальные SAN (VSAN) помогают достичь более высокой безопасности и стабильности в сетях FC, обеспечивая изоляцию устройств, подключенных к одной физической сети
- VSAN (ANSI T11 FC-FS-2) можно использовать для создания множества логических Сетей Хранения на единой физической инфраструктуре

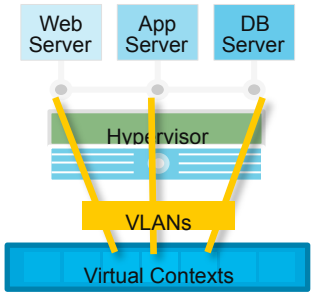
- VSAN обеспечивает:
  - ✓ *Изоляцию трафика* Строгая изоляция между VSAN используя разделение сети и тегирование фреймов)
  - ✓ *Изоляцию сервисов сети* Независимые сервисы сети, включая сервер имен, зонирования, FSPF и менеджер домена в каждой VSAN.



Безопасность виртуализации вычислений (серверная виртуализация)



С чем сталкиваются заказчики ?



- **Внедрение политик информационной безопасности**
  - ✓ Проблемы переноса политики с физических серверов на виртуальные
  - ✓ vMotion и аналоги могут нарушать политику
- **Сегментация и изоляция**
  - ✓ Потеря изоляции VM из-за ошибок конфигурации или атак
  - ✓ Уязвимости гипервизора и систем управления
- **Отсутствие наблюдаемости**
  - ✓ Отсутствие контроля над трафиком между VMs
- **Риски эксплуатации**
  - ✓ Разделение полномочий админов серверов, сети и безоп.
  - ✓ Часто администраторы имеют завышенные полномочия
  - ✓ Несвоевременная установка обновления на VMs и гипервизор
  - ✓ “Забытые” виртуальные машины

Безопасность гипервизора - ключ к безопасности среды виртуализации

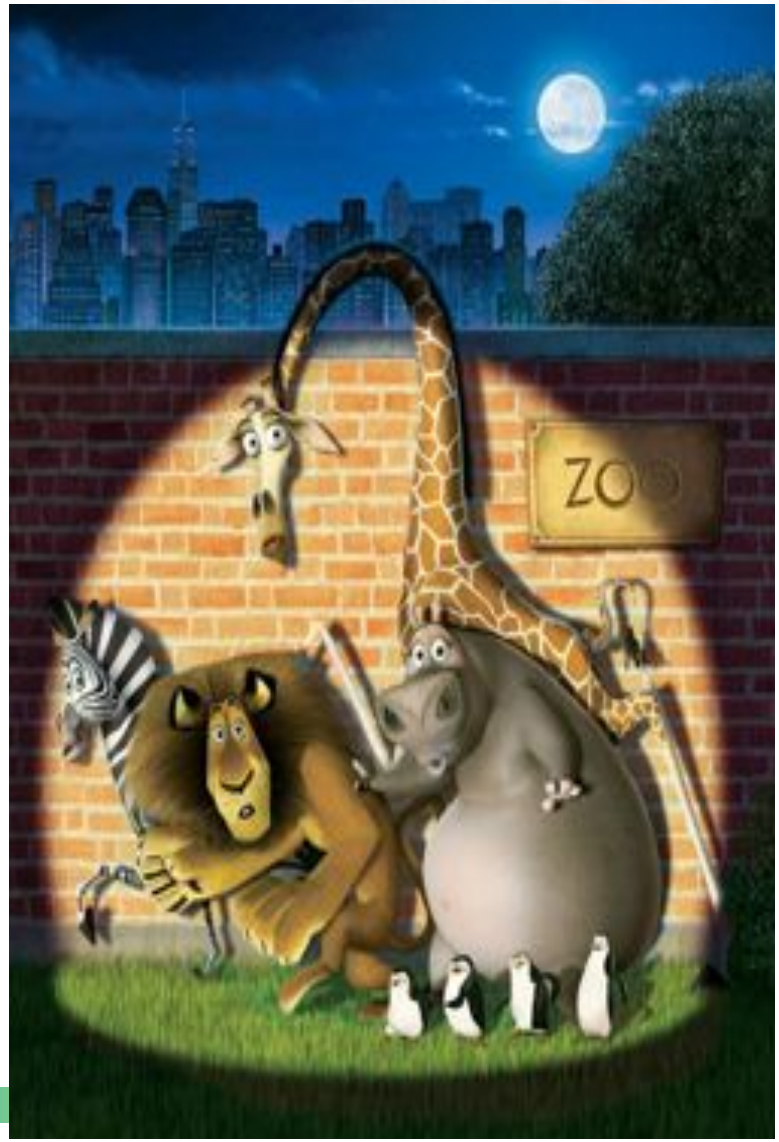
VMSA-2009-0006
- Уязвимость в ESX 3.5, Workstation, etc.
- Исполнение кода из VM Guest на хосте
- Переполнение буфера в графическом драйвере

Експлойт Blue Pill разработанный Йоанной Рутковской для процессоров AMD переносил хостовую ОС в виртуальную среду (2006)

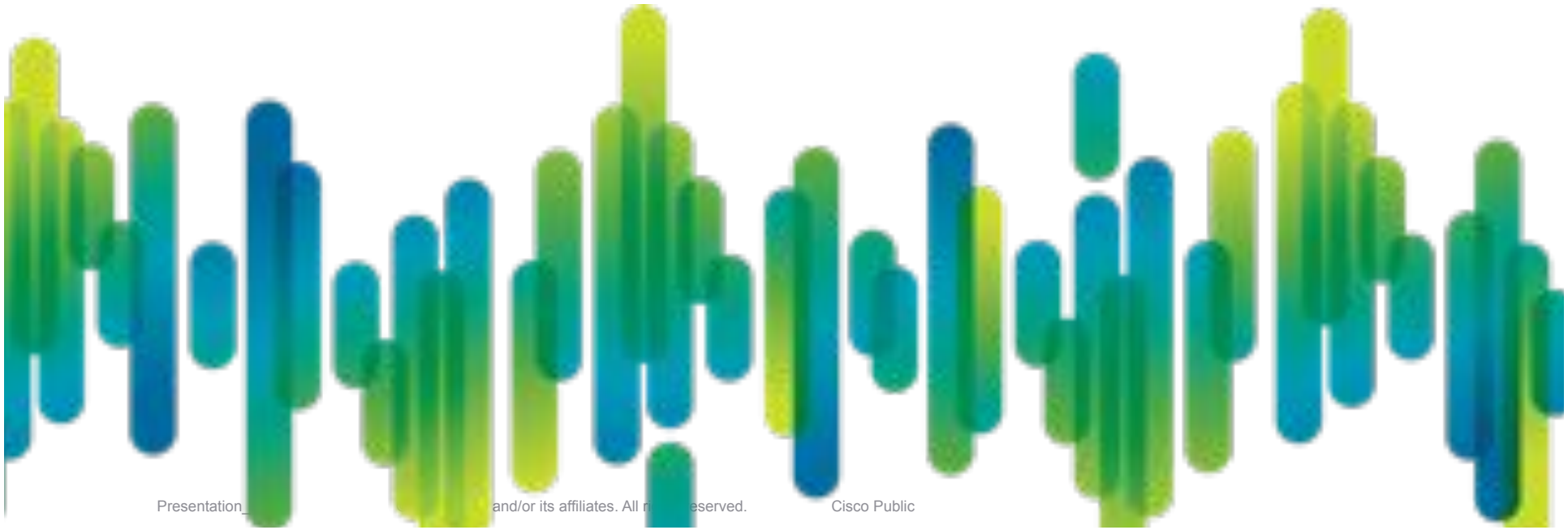
Классические уязвимости среды виртуализации

Время не стоит на месте

- Уязвимость в реализации инструкции SYSRET всех выпущенных x86-64 процессоров Intel позволяет выходить за пределы виртуальной машины - http://www.xakep.ru/post/58862/ 19.06.2012 http://www.xakep.ru/post/58862/
- Как взломать Vmware vCenter за 60 секунда http://2012.confidence.org.pl/materials - Май 2012
- VASTO (Virtualization ASsessment Toolkit) – Первый модуль поиска уязвимостей виртуализации для Metasploit доступен для широкой публики http://vasto.nibblesec.org/



Внедрение политик и сегментация для виртуальных машин

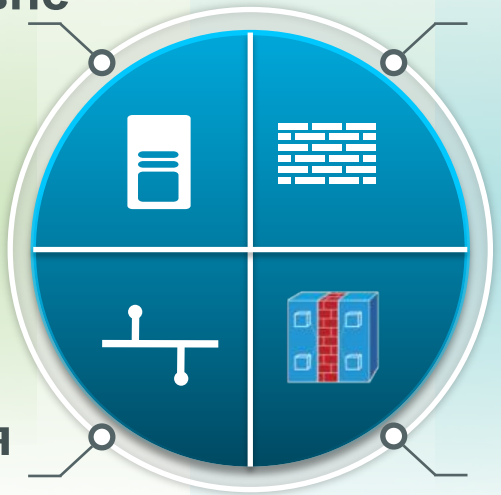


Сегментация и изоляция VM

Обеспечение согласованной политики в пределах физических и виртуальных границ сети

1. Сегментация на уровне фабрики

UCS Fabric Interconnect



2. Сетевая сегментация на коммутаторе

Nexus 1000V или физический коммутатор ЦОД

3. Сегментация на физических устройствах безопасности

ASA 5585-X, IPS

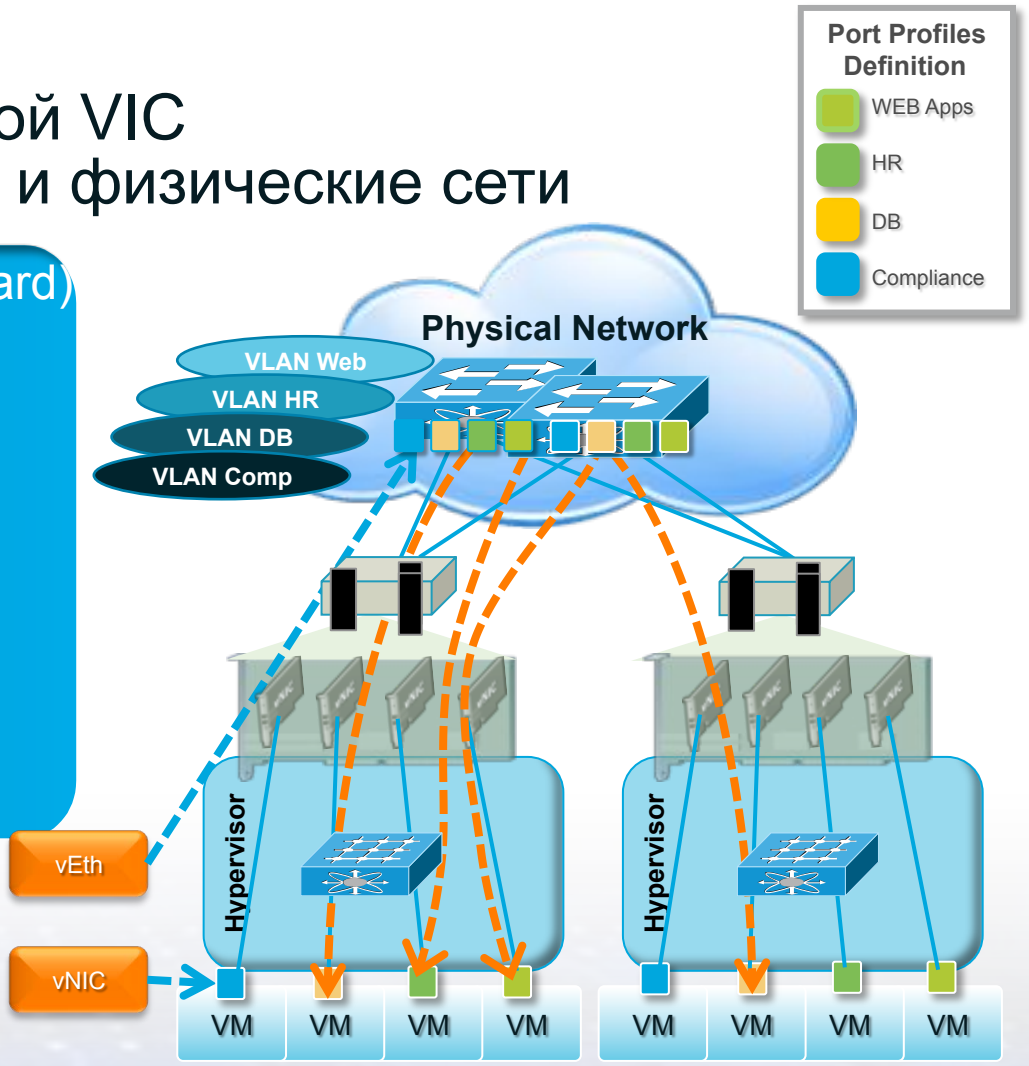
4. Сегментация на виртуальных устройствах безопасности

Cisco Virtual Security Gateway,
Cisco ASA 1000V

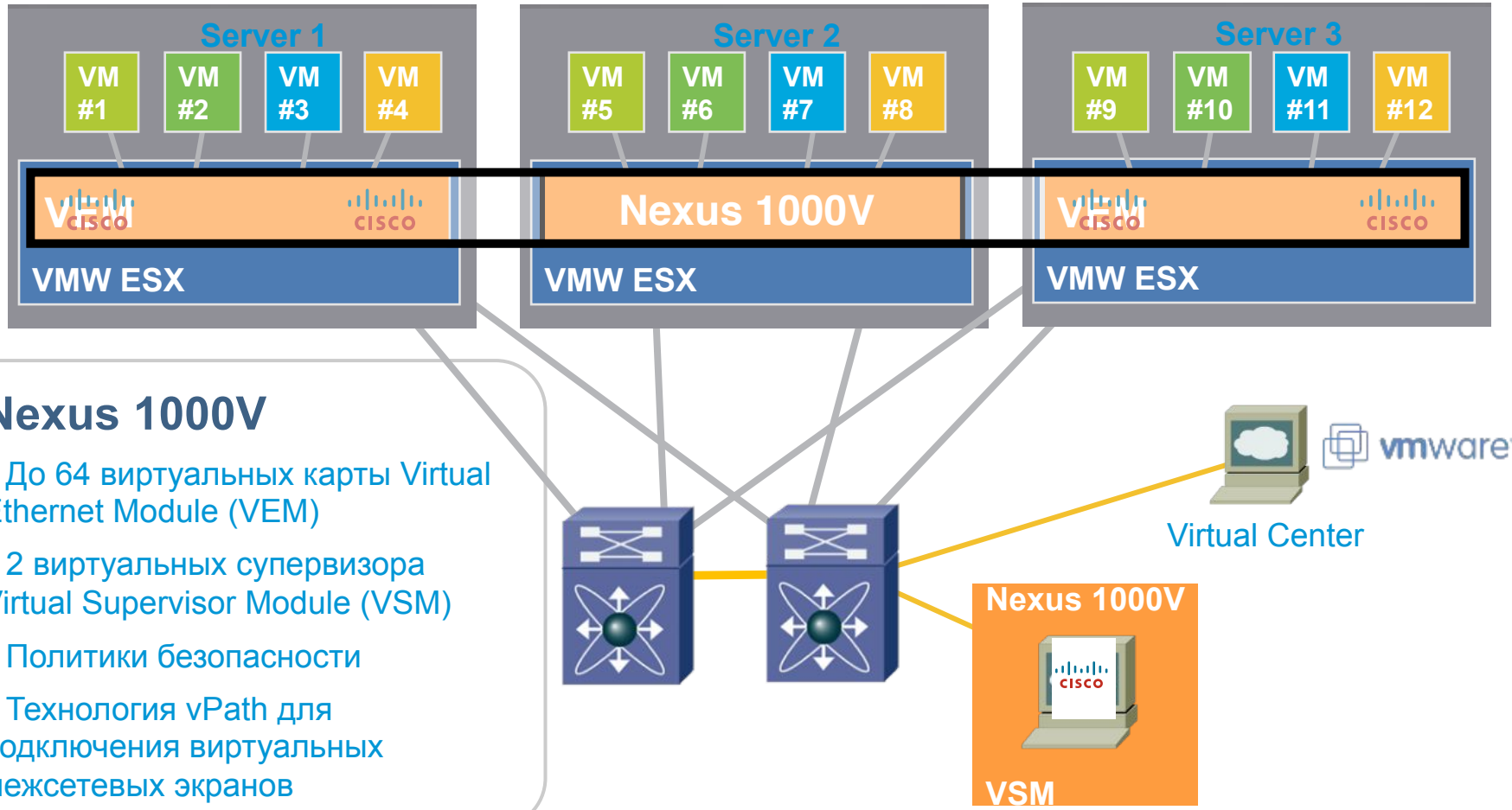
1 Сегментация на Унифицированной фабрики

Cisco® UCS с сетевой картой VIC унифицирует виртуальные и физические сети

- Cisco UCS VIC (Virtual Interface Card) поддерживает VM-FEX (VN-Link)
- С VM-FEX, каждой виртуальной машине (VM) предоставляется выделенный порт коммутатора доступа в ЦОД (Nexus 5500 или Fabric Interconnect)
- Весь трафик VM отсылается непосредственно на порт коммутатора



2 Сегментация на виртуальном коммутаторе Cisco Nexus 1000V



Nexus 1000V

- До 64 виртуальных карты Virtual Ethernet Module (VEM)
- 2 виртуальных супервизора Virtual Supervisor Module (VSM)
- Политики безопасности
- Технология vPath для подключения виртуальных межсетевых экранов

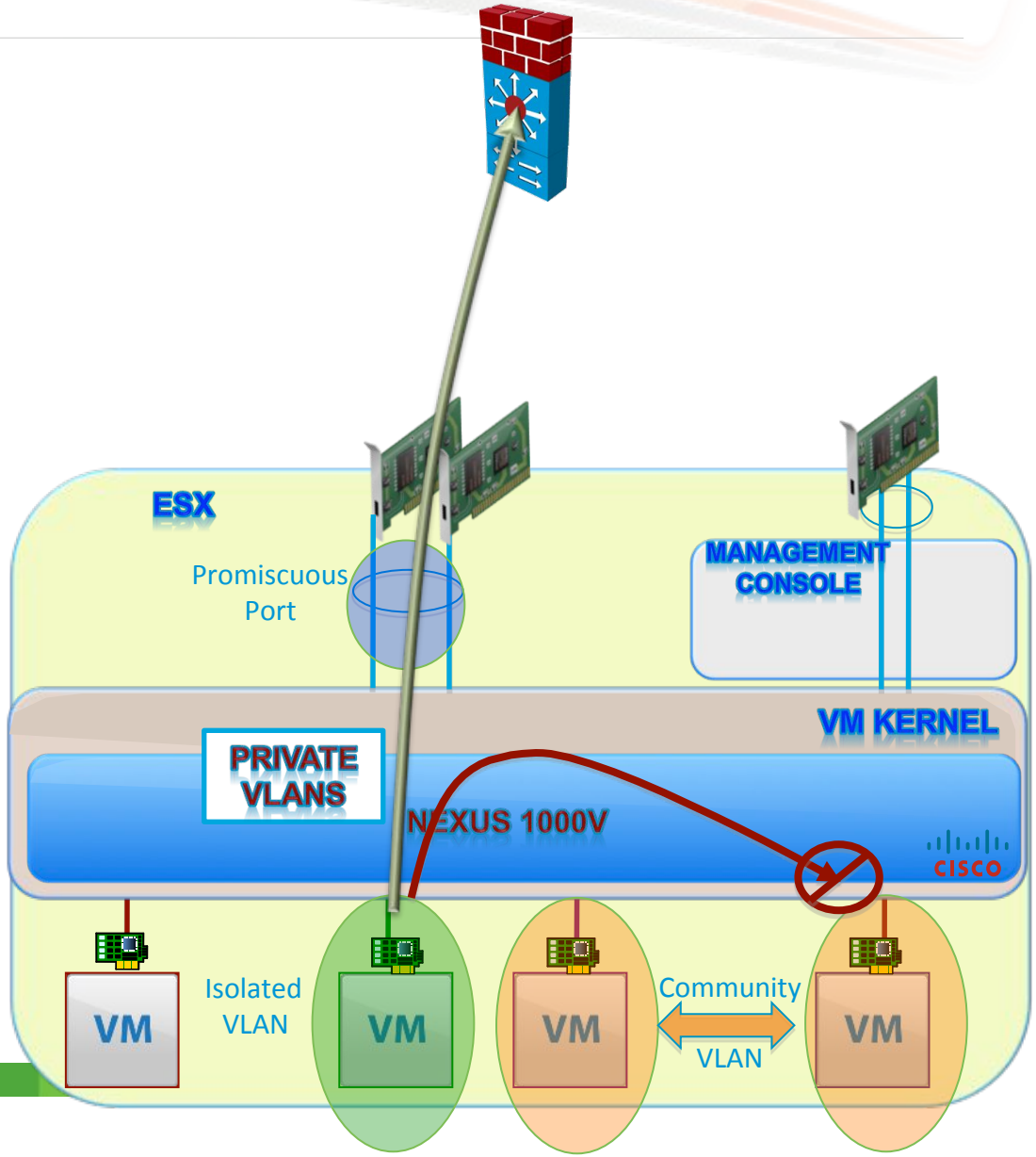
Поддержка гипервизоров : vSphere ; анонс для Win8/Hyper-V/KVM/Xen

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 ▪ Dynamic ARP inspection, IP Source Guard, DHCP Snooping
Внедрение	▪ Automated vSwitch Config, Port Profiles, Virtual Center Integration ▪ Optimized NIC Teaming with Virtual Port Channel – Host Mode
Наблюдаемость	▪ VMotion Tracking, ERSPAN, NetFlow v.9 w/ NDE, CDP v.2 ▪ VM-Level Interface Statistics
Управление	▪ Virtual Center VM Provisioning, Cisco Network Provisioning, CiscoWorks ▪ Cisco CLI, Radius, TACACs, Syslog, SNMP (v.1, 2, 3)

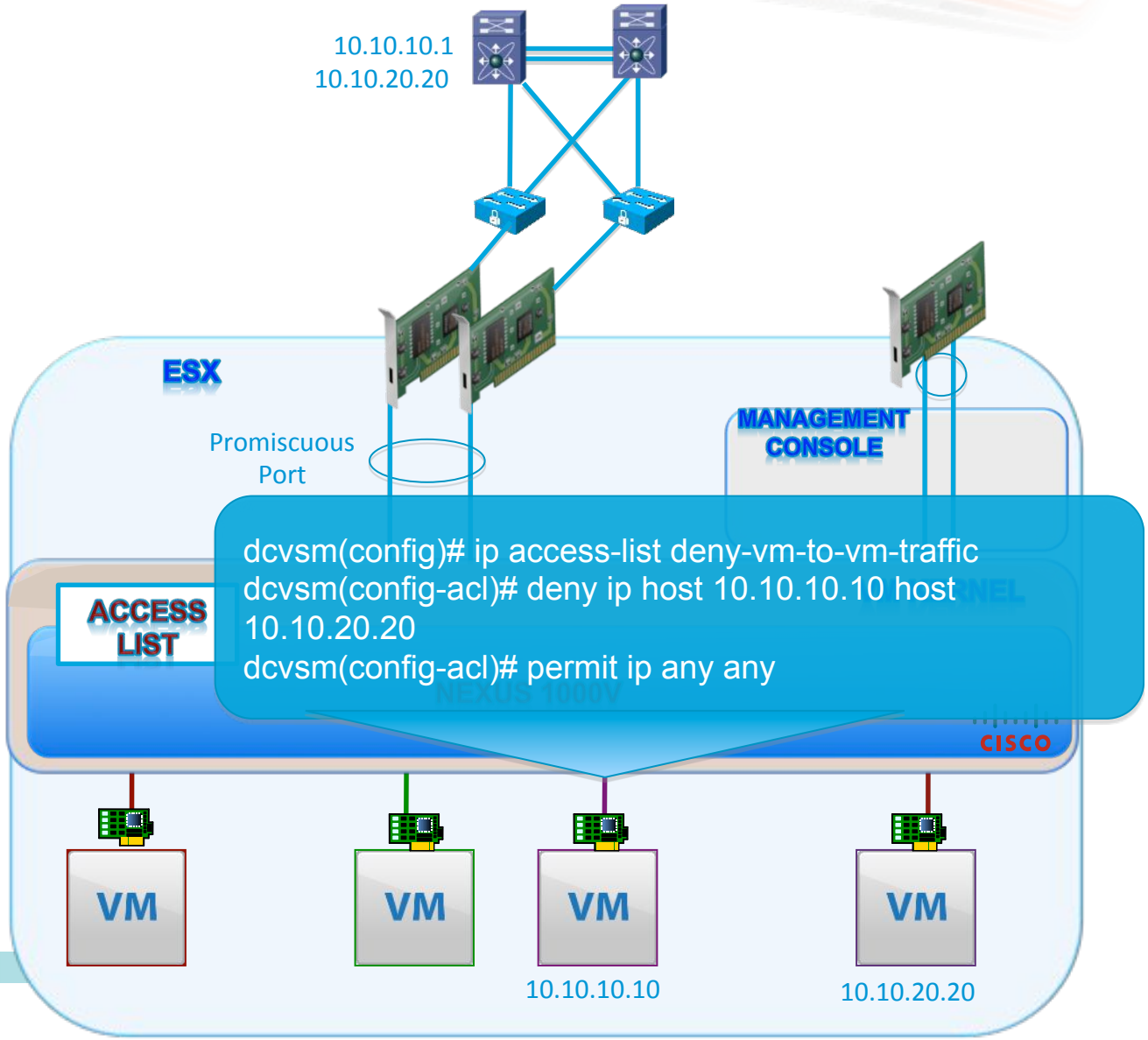
Изоляция VM: Cisco Private VLAN

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

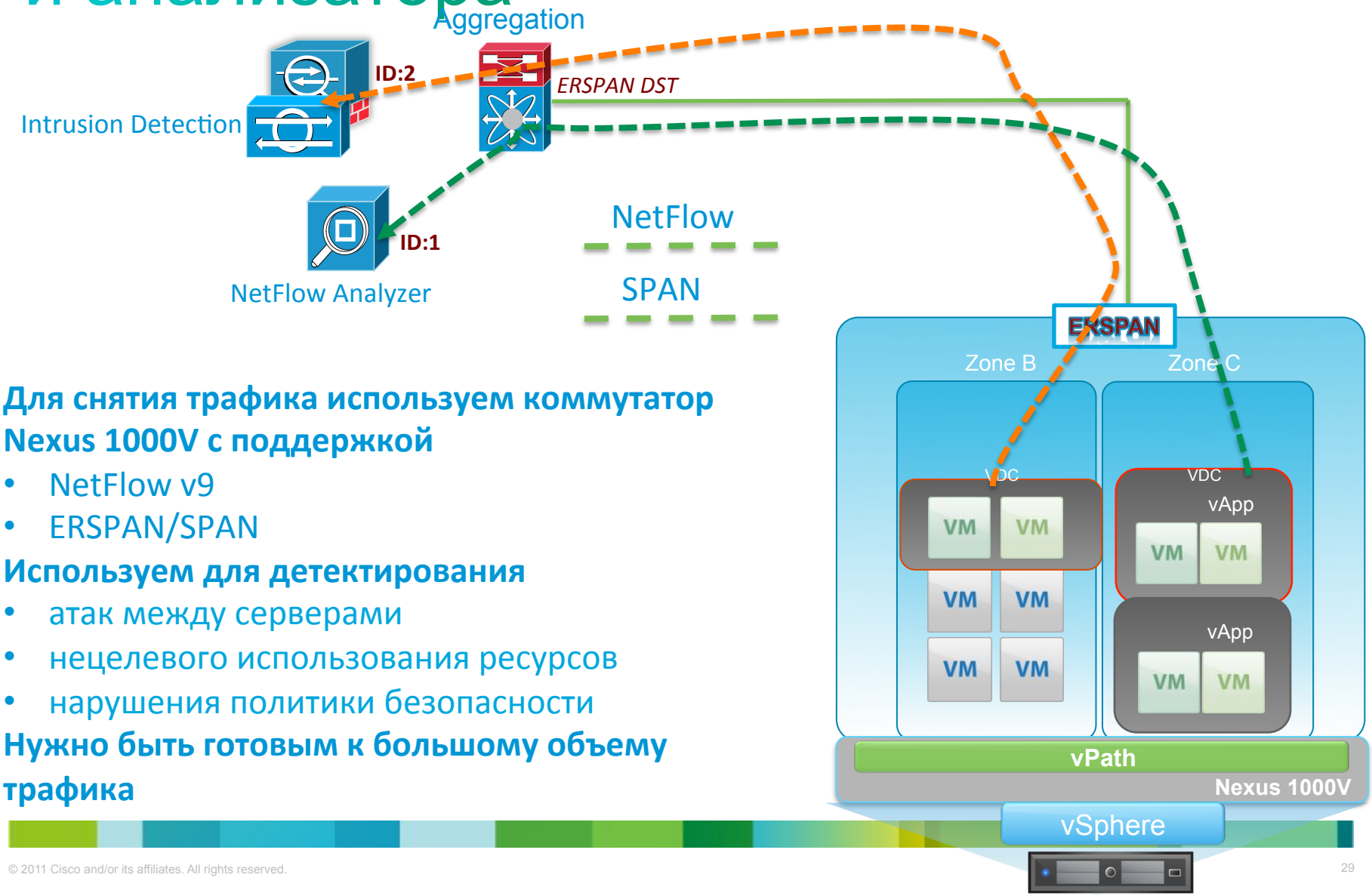


Изоляция VM и контроль трафика

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



Наблюдаемость: мониторим трафик между VMs с помощью физических IDS и анализатора



Для снятия трафика используем коммутатор Nexus 1000V с поддержкой

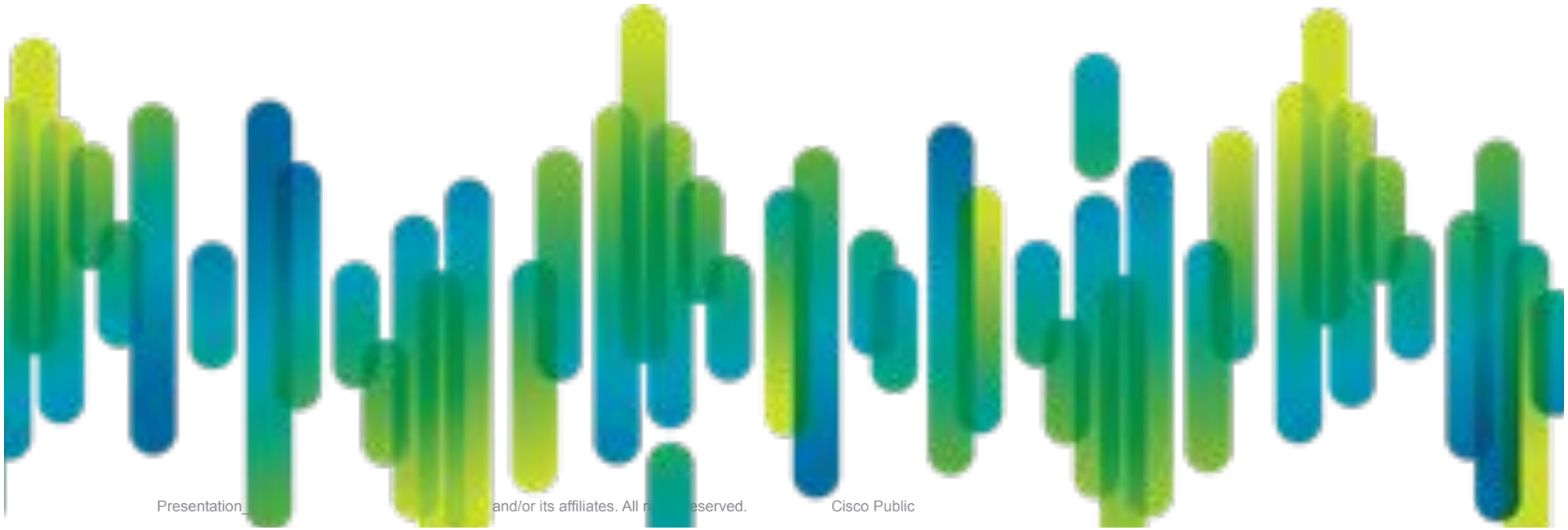
- NetFlow v9
- ERSPAN/SPAN

Используем для детектирования

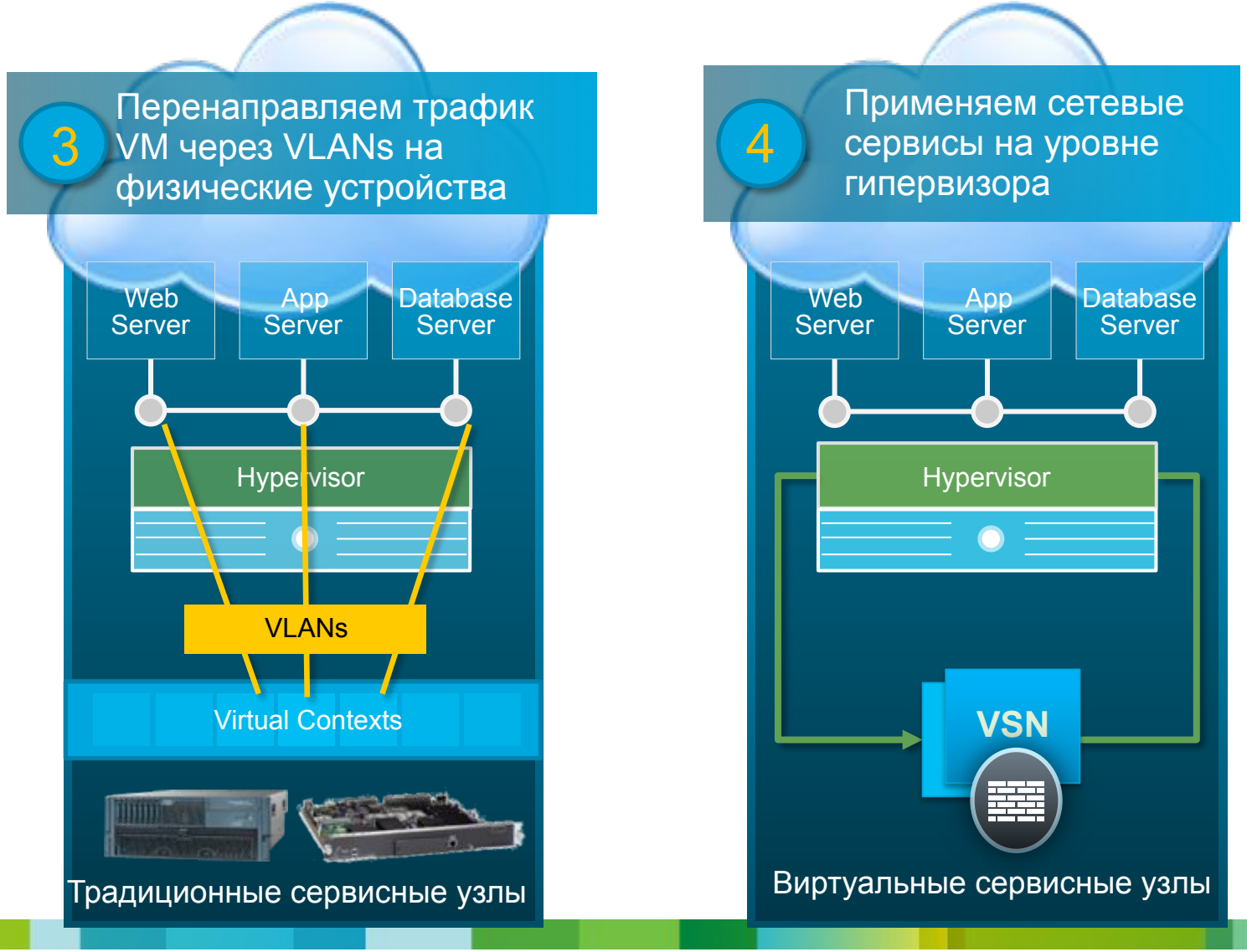
- атак между серверами
- нецелевого использования ресурсов
- нарушения политики безопасности

Нужно быть готовым к большому объему трафика

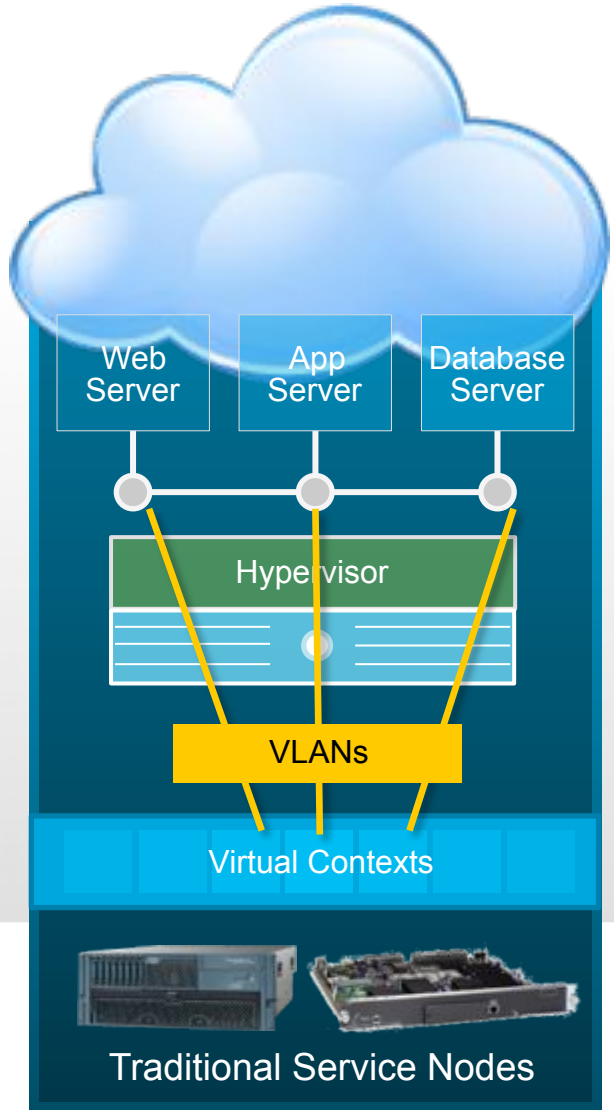
Сервисы безопасности для виртуальной среды



Физические и Виртуальные сервисные узлы безопасности



3 Физические устройства защиты



Модули межсетевых экранов ASA

Устройства ASA 5585

Устройства защиты от атак Cisco IPS

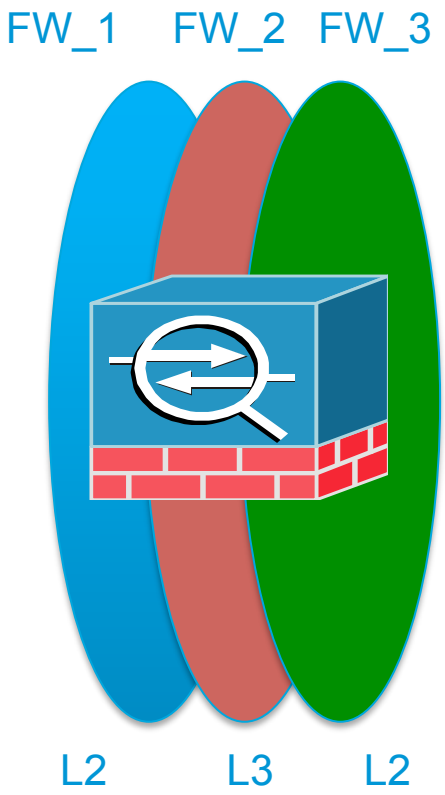
Поддержка виртуализации в ASA

Виртуальные контексты на семействе ASA

- до 256 виртуальных контекстов на ASA 5585 и ASA SM (до 1000 контекстов на кластер с ASA 9.0)
- до 1024 VLAN, которые могут разделяться между контекстами (до 4000 VLAN на кластер с ASA 9.0)
- контексты в режиме L2 или L3
- контекст – это полнофункциональный файервол
- контроль ресурсов для контекстов (MAC-адреса, соединения, инспекции, трансляции…)

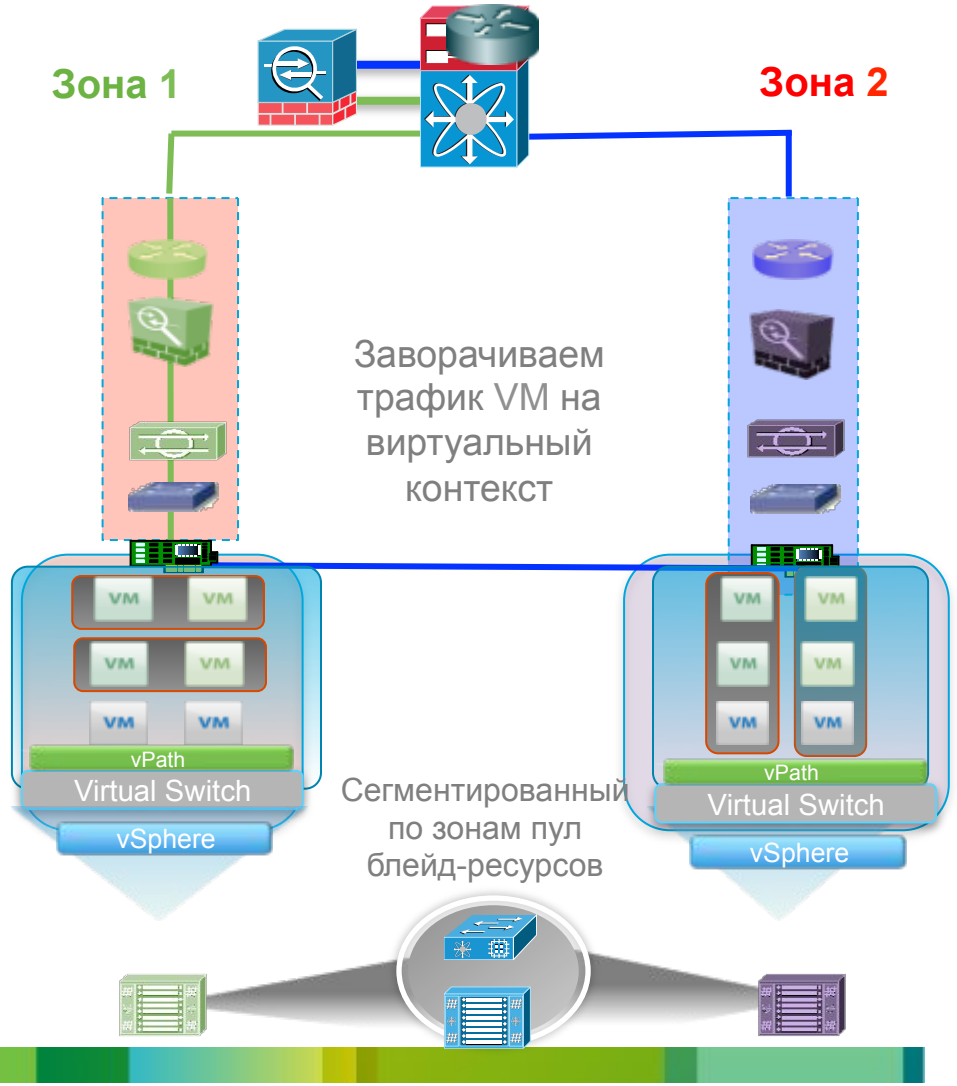
До 32 интерфейсов в L2-контекстах

- 4 интерфейса в бридж-группе. 8 бридж-групп на виртуальный контекст

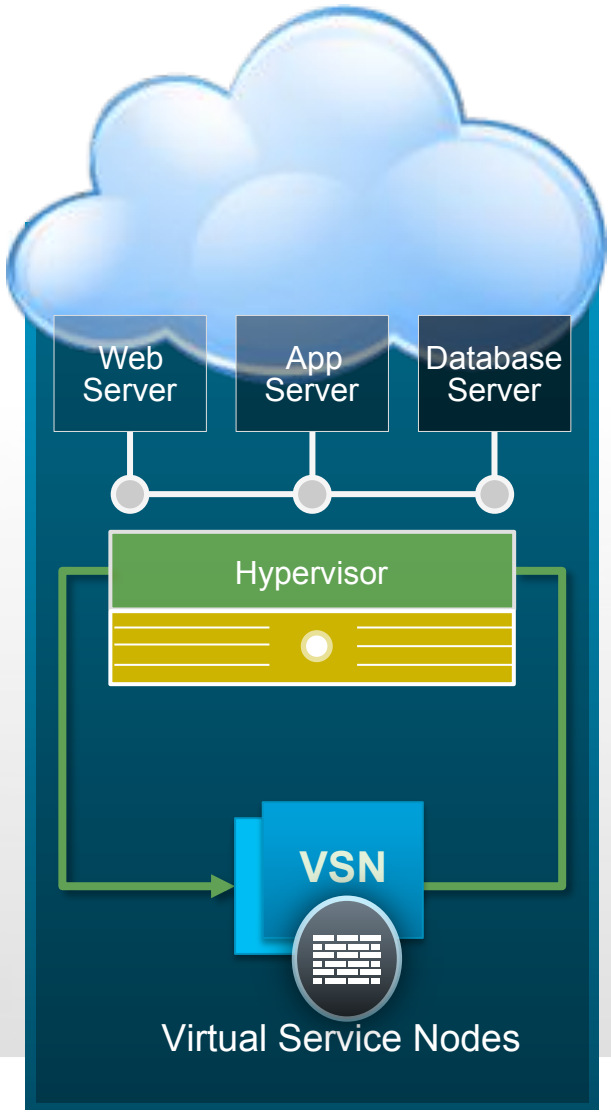


Сценарий 1.
Сервисы безопасности путем виртуализации физических устройств

- Для применения политик используются зоны безопасности
- Политики безопасности применяются на входе/выходе в зону
- Для привязки к физической инфраструктуре используются:
  - Технологии VLAN//VRF на коммутаторах
  - Виртуальные контексты на ASA



4 Виртуальные сервисные узлы



Nexus 1000V

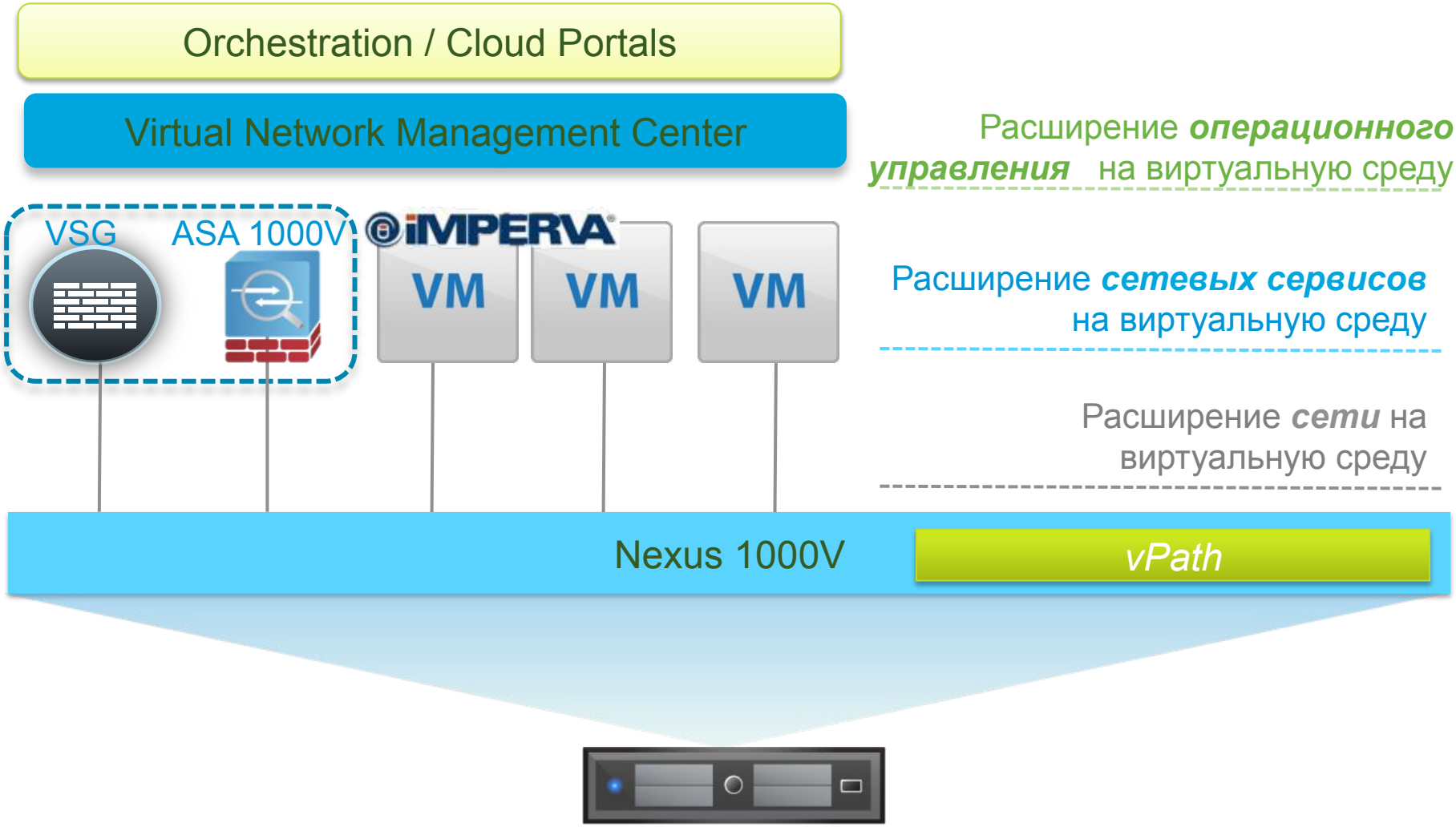
Virtual Security Gateway

Сегментация VMs на основе зон внутри виртуального ЦОД

ASA 1000V

Внедрение на границе виртуального ЦОД

Архитектура виртуальных сервисов безопасности



Расширение ***операционного управления*** на виртуальную среду

Расширение ***сетевых сервисов*** на виртуальную среду

Расширение ***сети*** на виртуальную среду

Защита виртуальных зон безопасности

Virtual Security Gateway: Зонный межсетевой экран

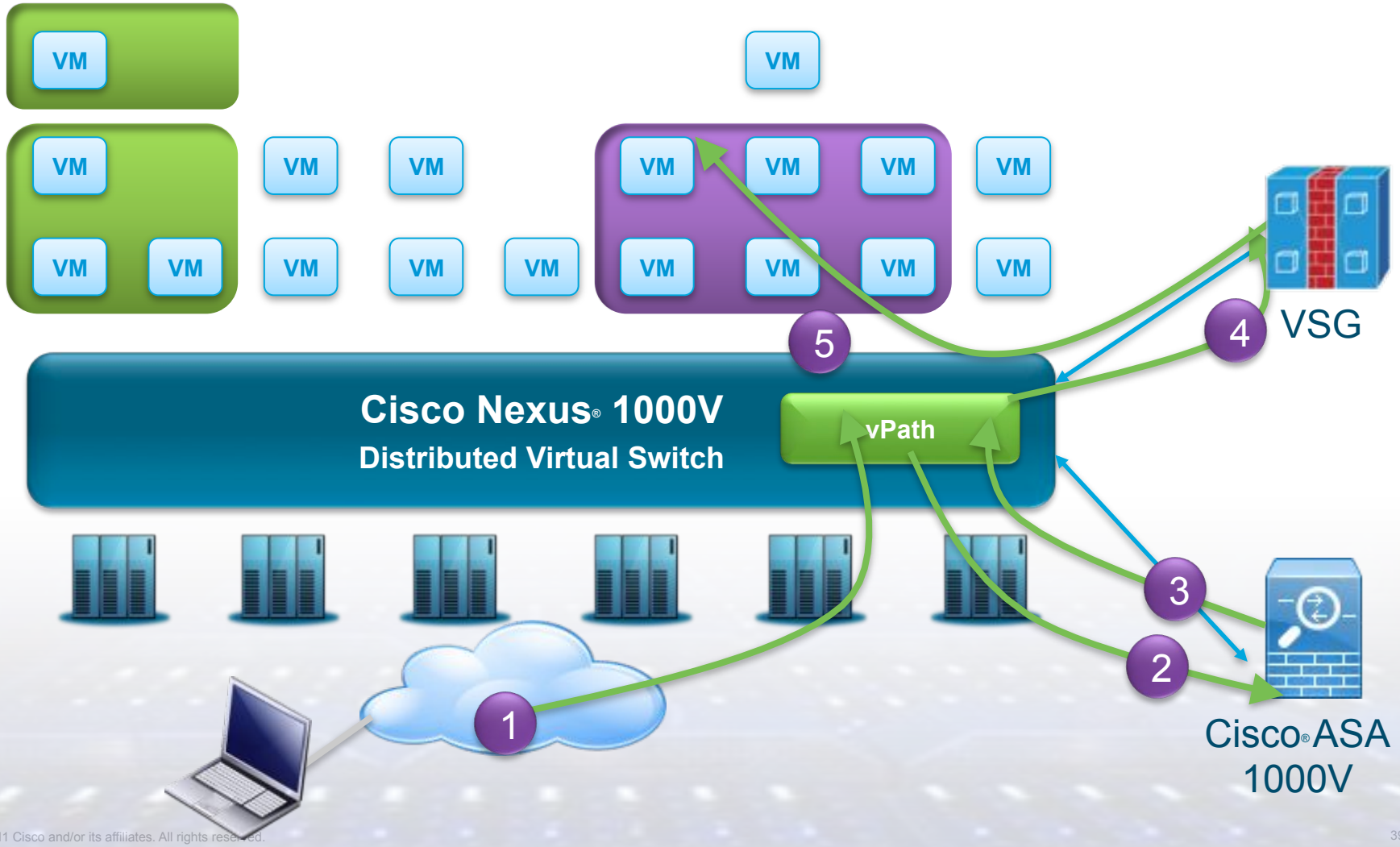
Cisco® ASA 1000V: Функции и особенности

- **Построен на технологиях аппаратной Cisco ASA**
- **Совместимость VSG с помощью service chaining**
- **Поддержка Virtual Extensible LAN (VXLAN) до 16M сегментов**
- **Многопользовательское управление VNMC (Multi Tenant)**

- IPSec VPN (Site-to-Site)
- NAT
- DHCP для VM
- Шлюз по умолчанию для VM
- Статическая маршрутизация
- Инспекция с учетом состояния
- IP Audit

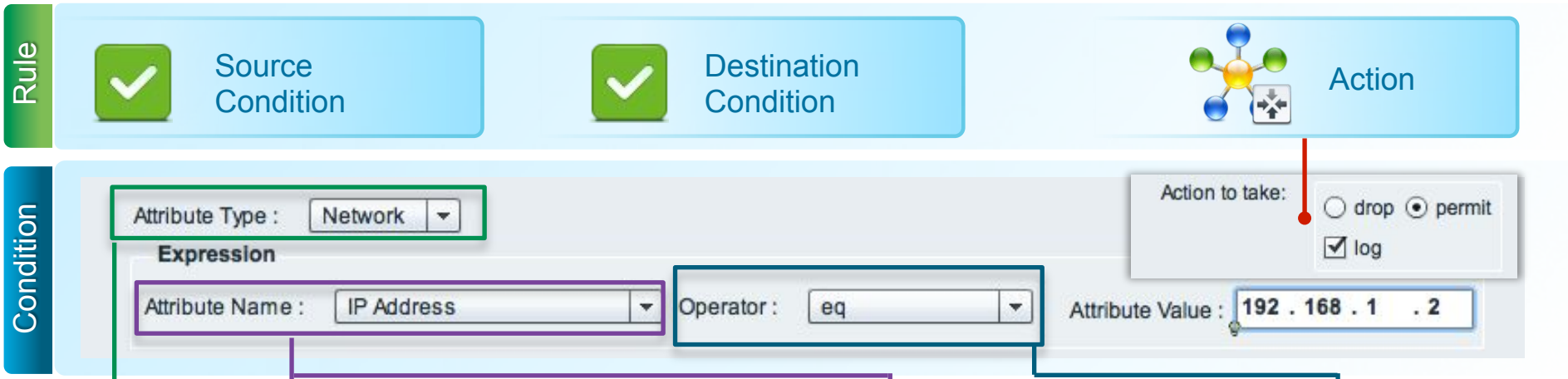
Цепочка сервисов безопасности в технологии vPath

Интеллектуальный отвод трафика с vPath



Cisco® ASA 1000V и атрибуты политик

- Cisco® ASA 1000V поддерживает политики на основе сетевых атрибутов*
- Cisco VSG поддерживает политики на основе сетевых атрибутов и атрибутов VM



Attribute Type
Network
VM
Custom

VM Attributes	VM Attributes	Network Attributes
Instance Name	Port Profile Name	IP Address
Guest OS full name	Cluster Name	Network Port
Zone Name	Hypervisor Name	
Parent App Name		

Operator
eq
neq
gt
lt
range

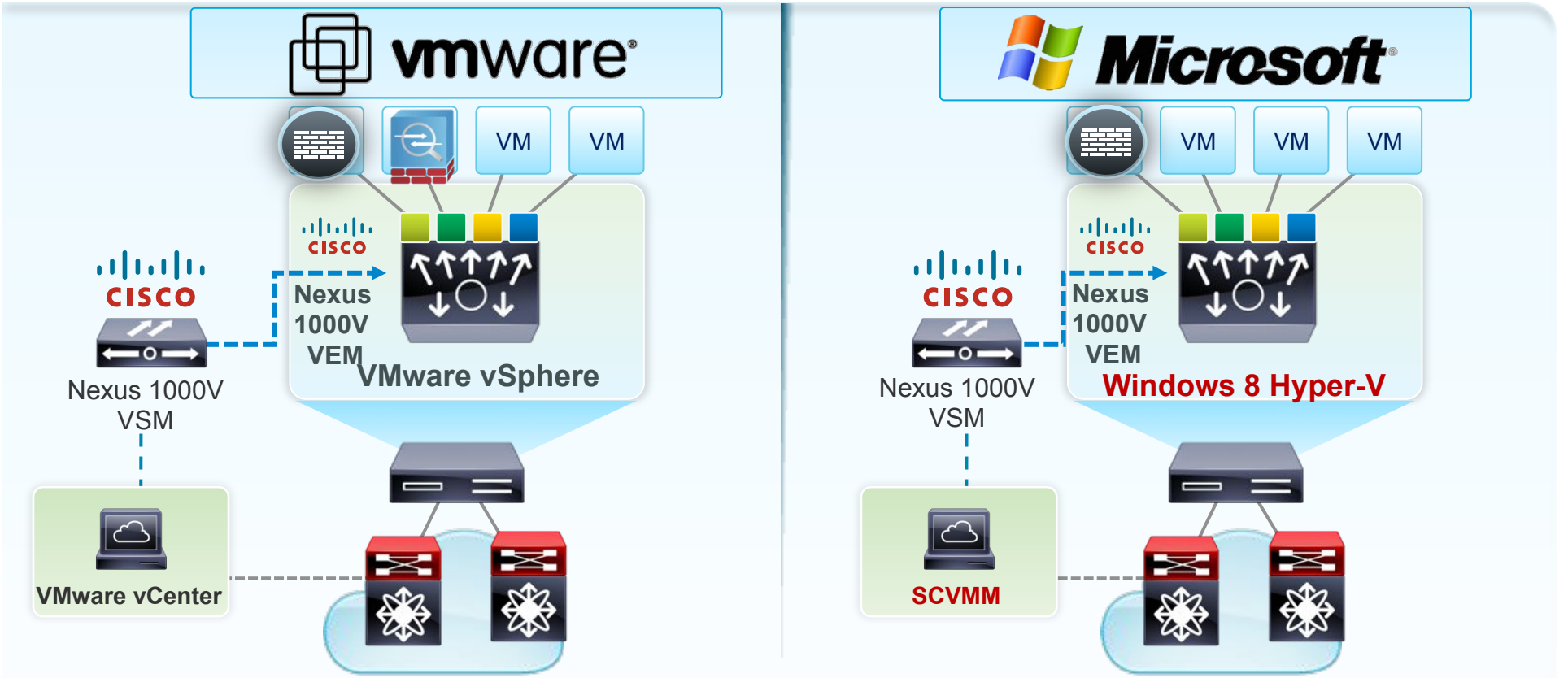
Operator
Not-in-range
Prefix
member
Not-member
Contains

поддержка атрибутов VM для ASA в роадмапе

Разделение обязанностей

- Управление многопользовательскими ЦОД (multitenant)
- Динамическое управление на основе политик
- Гибкость с помощью внешнего XML API

Унифицированное решение безопасности под разные гипервизоры



✓ Решение адаптируется под разных вендоров гипервизоров

✓Унифицированное управление безопасностью через единую консоль VMDC

* Available Q4CY12 on Cisco Nexus 1000V; roadmap item for Cisco® ASA 1000V

Сценарий 2. Модель безопасности ЦОД с виртуальными сервисами

- Глубокая инспекция входящего/исходящего в виртуальный ЦОД трафика на ASA 1000V
- NAT и DHCP на ASA 1000V
- Шифрование трафика между облачным ЦОД и сетями клиентов на ASA 1000V
- Микросегментация на Cisco VSG

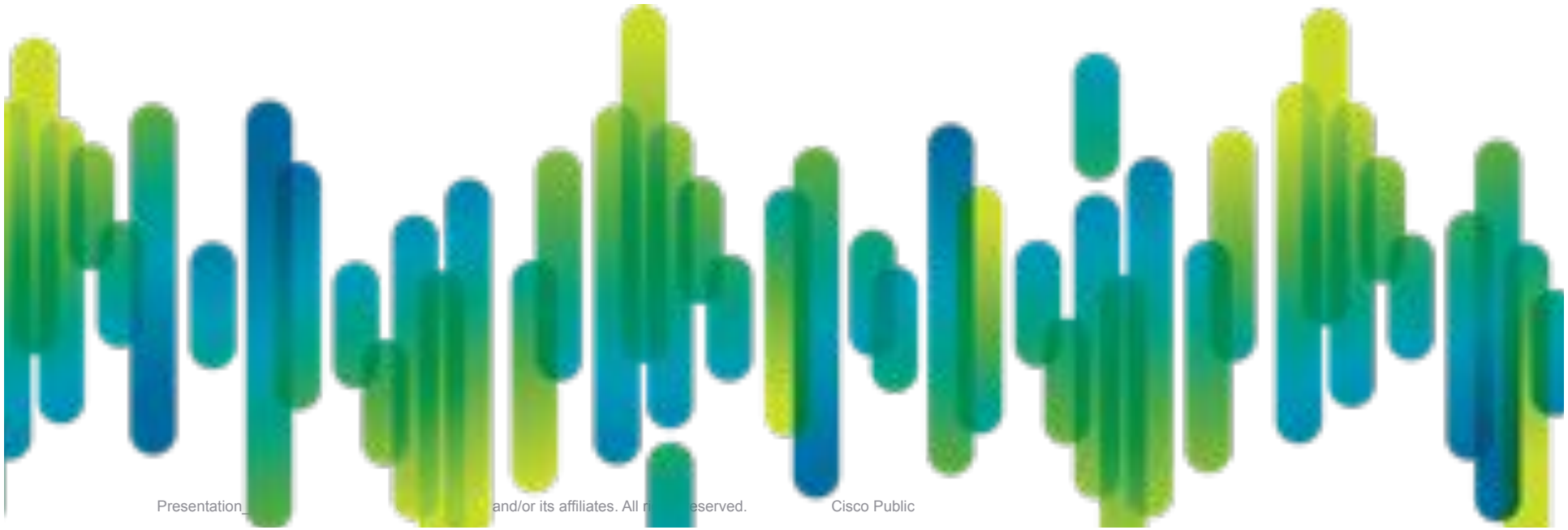
Позиционирование решения в современный ЦОД

Физическое устройство	Виртуальное
Устройства и модули защиты Cisco ASA для ЦОД	**Виртуальные и облачные МЭ** Увеличение виртуальной безопасности
	
Cisco ASA 5585-X	Cisco VSG
	
Cisco Catalyst® 6500 Series ASA Services Module	Cisco ASA 1000V Cloud Firewall
• Высочайшая производительность • Политики для защиты периметра ЦОД • Построение политик по атрибутам IP • Необходимость “отвода” трафика с помощью VLAN и VRF	• МСЭ для защиты виртуальных серверов, приложений и tenant • Автоматизация настройки политик • Построение политик на основе атрибутов VM и атрибутов сети • Фильтрация внутри серверной фермы

Сценарий 3. Модель безопасности ЦОД с комбинированными сервисами

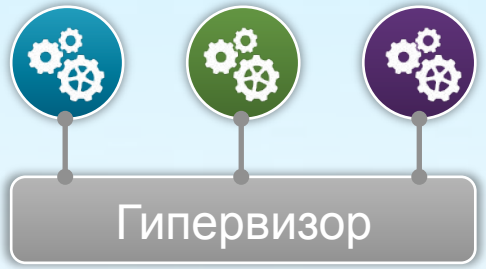
- Глубокая инспекция входящего/исходящего в виртуальный ЦОД трафика на ASA 1000V
- NAT и DHCP на ASA 1000V
- Шифрование трафика между облачным ЦОД и сетями клиентов на ASA 1000V
- Микросегментация на Cisco VSG

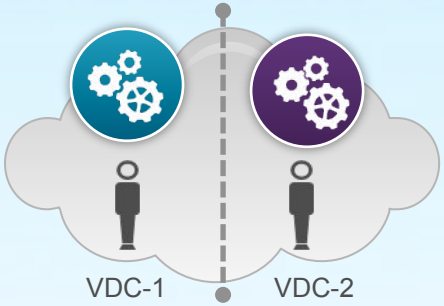
Безопасность облачных сервисов



Эволюция безопасности в IT

Физический ЦОД	Виртуальный ЦОД	Облачный ЦОД
• Одно приложение на сервере • Ручная конфигурация политик	• Множество приложений на сервере • Динамич. конфигурация	• Множество пользователей на сервере • “Чужая” инфраструктура





Согласованные : Политики, Функции безопасности, Управление

Коммутация	Nexus 7K/5K/3K/2K	Nexus 1000V, VM-FEX
Безопасность	ASA 5585, ASA SM	VSG*, ASA 1000V**
Вычисления	UCS for Bare Metal	UCS for Virtualized Workloads

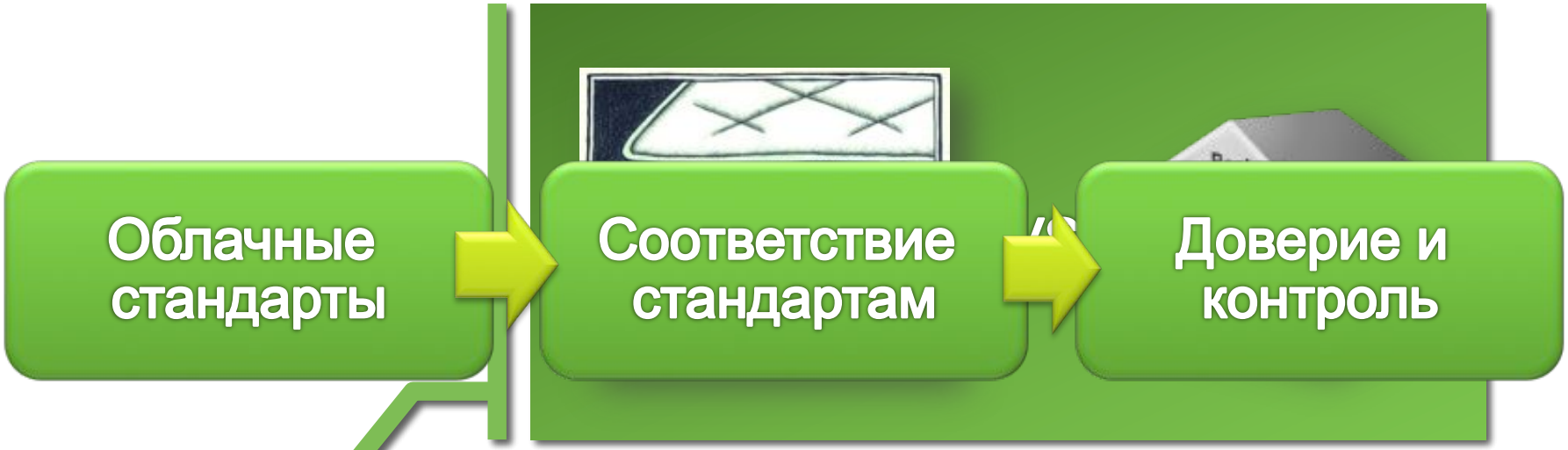
* Virtual only, ** Announced

Cloud Security Alliance (CSA)

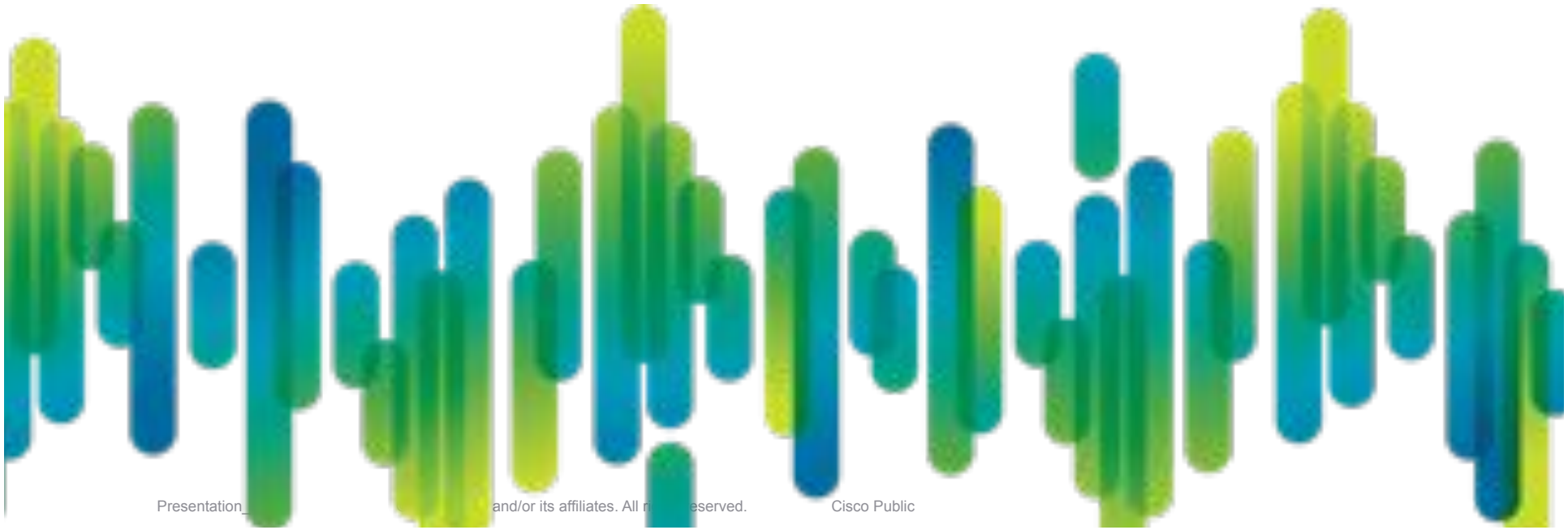
- **“Security Guidance for Critical Areas of Focus in Cloud Computing” Whitepaper:** комплексное руководство, которое говорит как защищать облачные архитектуры, как управлять Облаками и как безопасно использовать облачные среды: http://www.cloudsecurityalliance.org/csaguide.pdf
- Также разработан модель угроз для облачных сред “Top threats to Cloud Computing” : http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
- В состав корпоративных членов CSA входят:

Cloud Security Alliance: Руководство по безопасности облачных вычислений

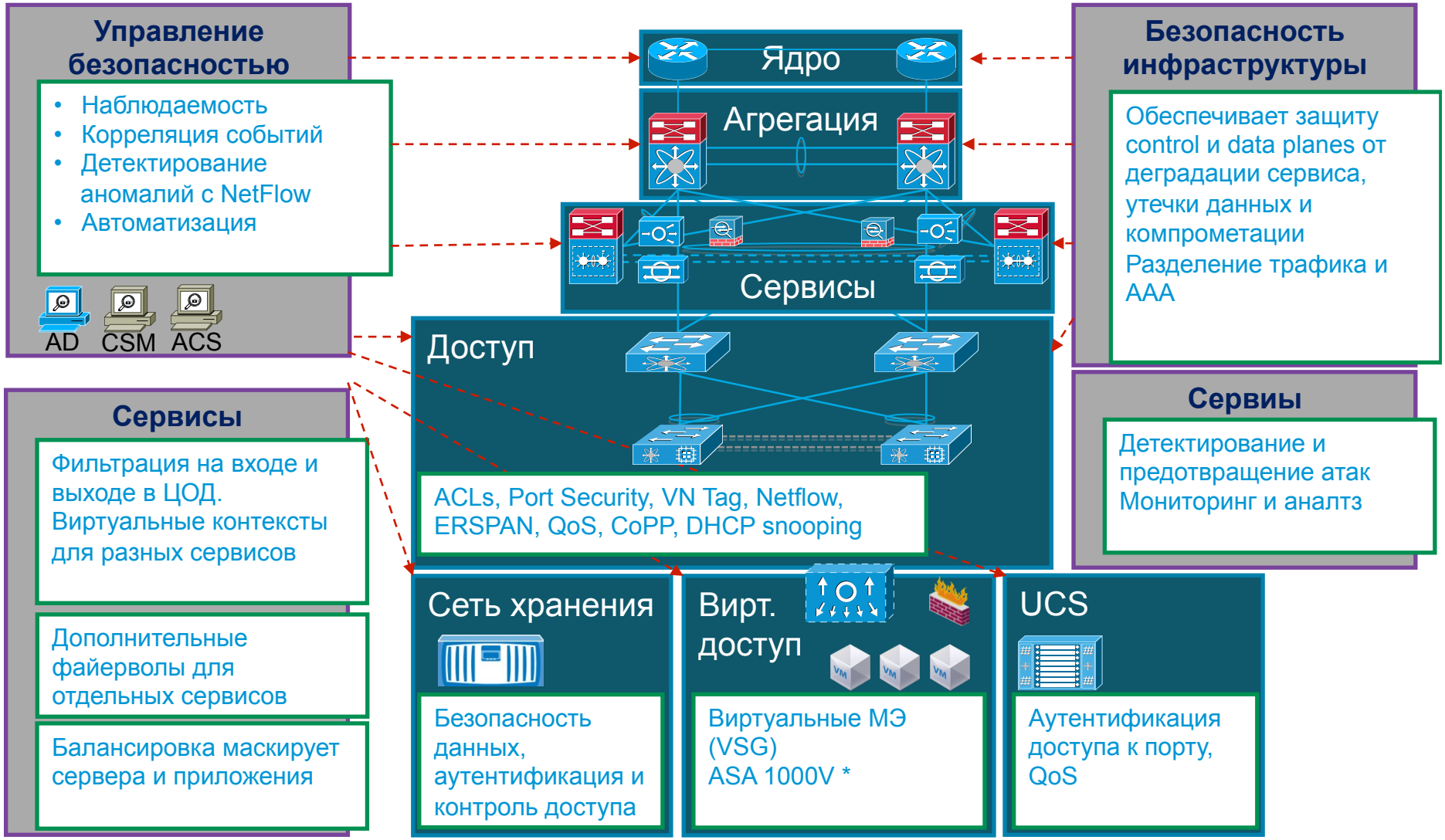
Использование облаков требуют доверия!



Архитектура Cisco для виртуализированных и облачных ЦОДов



Архитектура Cisco Virtualized Multi-Tenant Data Center (VMDC)



Выводы

- Внедрение виртуализации и облачных сервисов требует пересмотра оценки рисков в организации
- Для эффективного обеспечения безопасности виртуальной среды требуется объединение традиционных физических устройств и виртуальных средств!!
- Безопасно построенная виртуализированная и облачная среда не уступает по уровню надежности и защищенности традиционной системе

ВИРТУАЛИЗАЦИЯ

Полезные ресурсы по теме

- **Cisco**
  - Virtualization Security
  - http://www.cisco.com/en/US/netsol/ns1095/index.html
  - Design Guide: Security and Virtualization in the Data Center
  - http://www.cisco.com/en/US/partner/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_sec_design.html
  - Cisco VMDC Unified Data Center for cloud or traditional environments.
  - http://www.cisco.com/go/vmdc
- **Vmware**
  - Vmware Security Hardening Guide
  - http://www.vmware.com/resources/techresources/10198
- **Microsoft**
  - Hyper-V Security Guide
  - technet.microsoft.com/en-us/library/dd569113.aspx
- **PCI DSS**
  - https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf
- **NIST - Guide to Security for Full Virtualization Technologies**
  - http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf
- **Cloud Security Alliance**
  - https://cloudsecurityalliance.org/


CISCO


CHIMPANZEES