Обеспечение безопасности в виртуальной среде

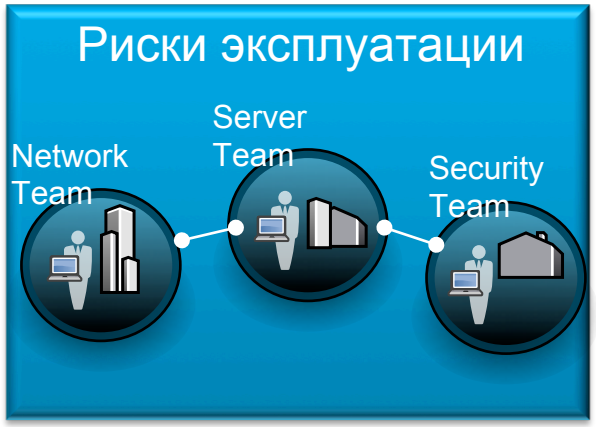
Владимир Илибман

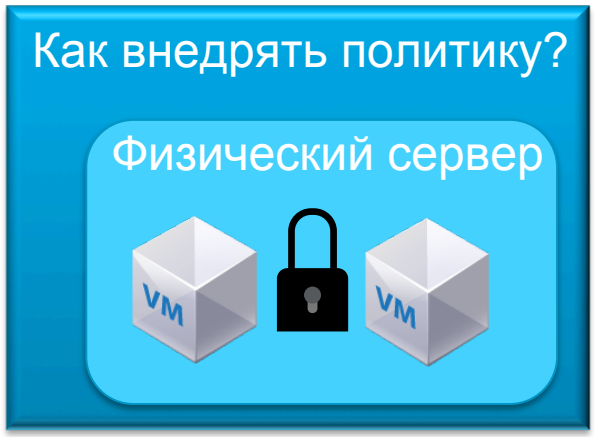
Инженер-консультант

Соблюдение баланса

Основные риски безопасности виртуализации связаны с небывалой консолидацией разнотипных данных, вычислительных и сетевых ресурсов в единой физической системе.

Основные вызовы безопасности в виртуальной среды



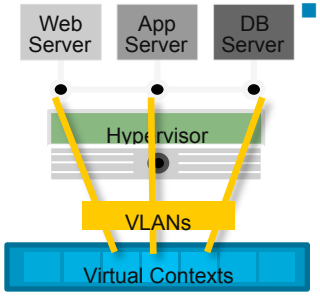


С чем сталкиваются заказчики ?

- **Внедрение политик информационной безопасности**
  - ✓ Перенос политики с физических устройств на виртуальные
  - ✓ vMotion и аналоги могут нарушать политику

- **Риски эксплуатации**
  - ✓ Разделение полномочий админов серверов, сети и безопасн.
  - ✓ Часто администраторы имеют завышенные полномочия
  - ✓ Несвоевременная установка обновления на VMs и гипервизор
  - ✓ “Забытые” виртуальные машины

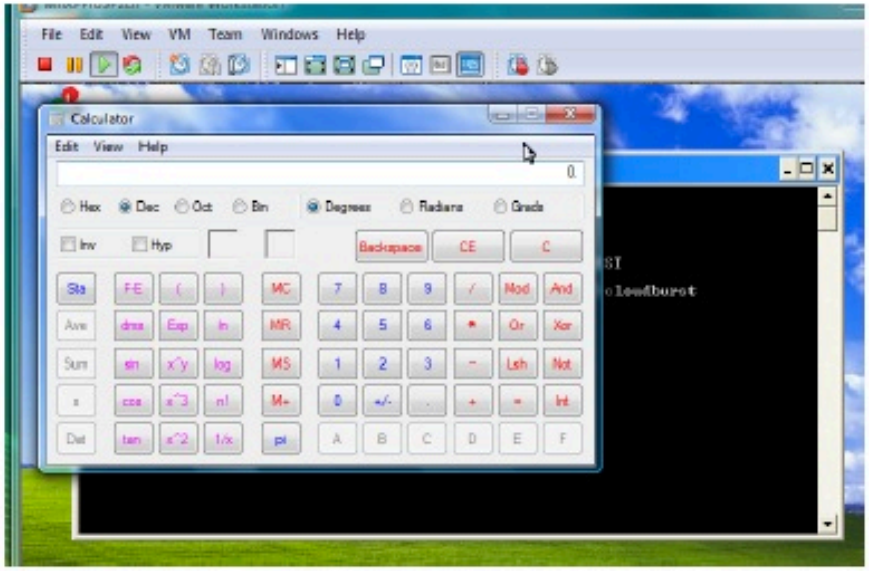
- **Отсутствие наблюдаемости**
  - ✓ Отсутствие контроля над трафиком между VMs



- **Сегментация и изоляция**
  - ✓ Потеря изоляции VM из-за ошибок конфигурации
  - ✓ Изоляция сетевых сегментов, сетевых контекстов
  - ✓ Уязвимости гипервизора*

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

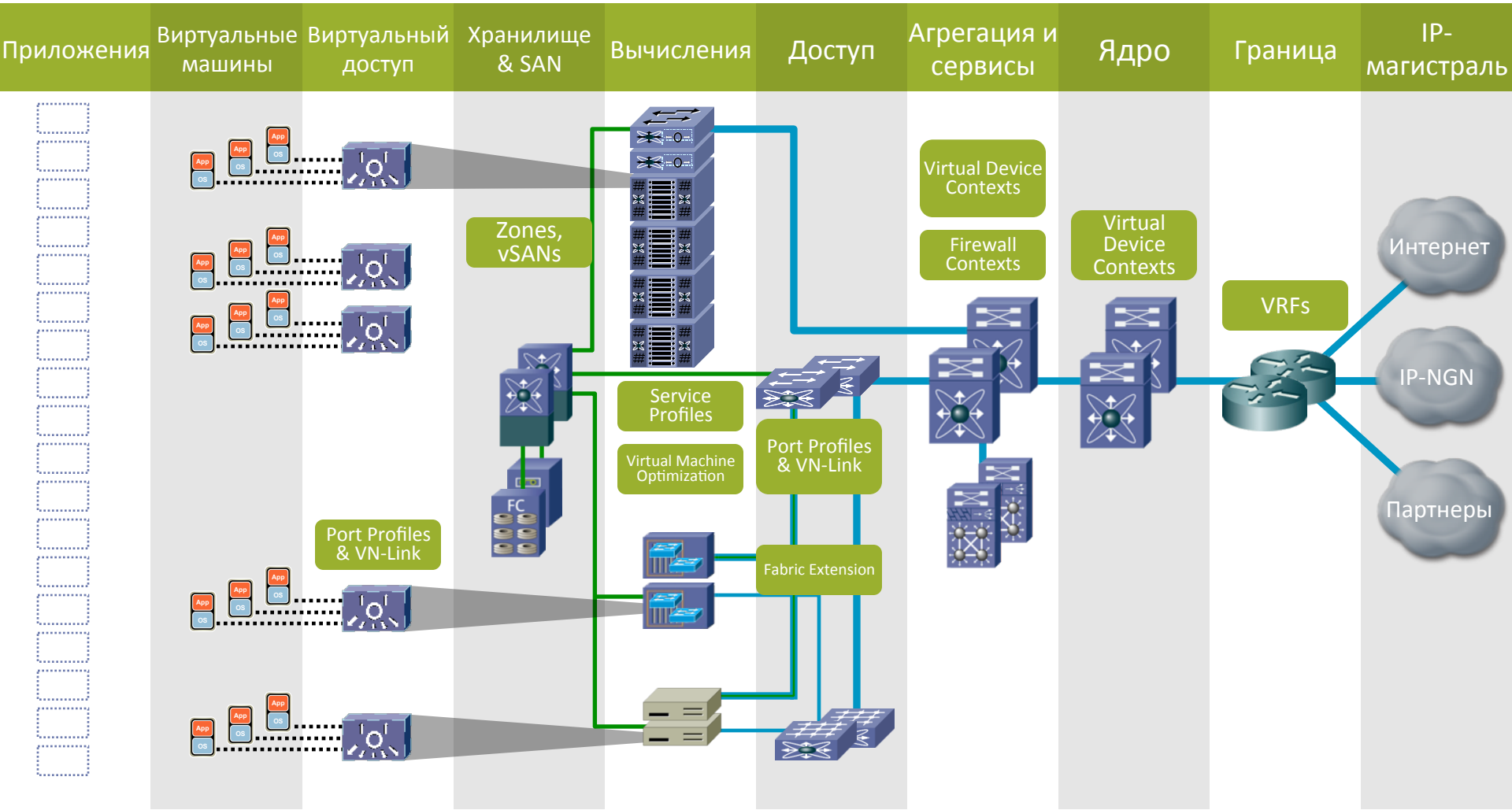


*Иксплойт Константина Корчинского

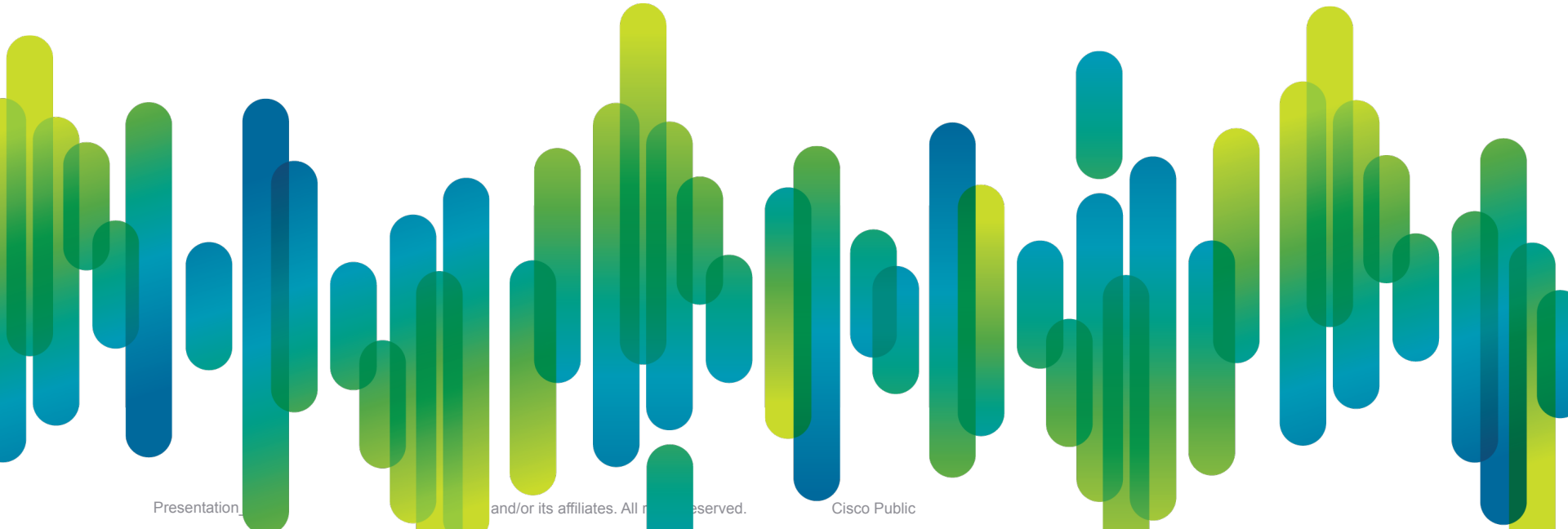
Експлойт Blue Pill разработанный Йоанной Рутковской для процессоров AMD переносил хостовую ОС в виртуальную среду (2006)

Архитектура Cisco Data Center

Зоны виртуализации

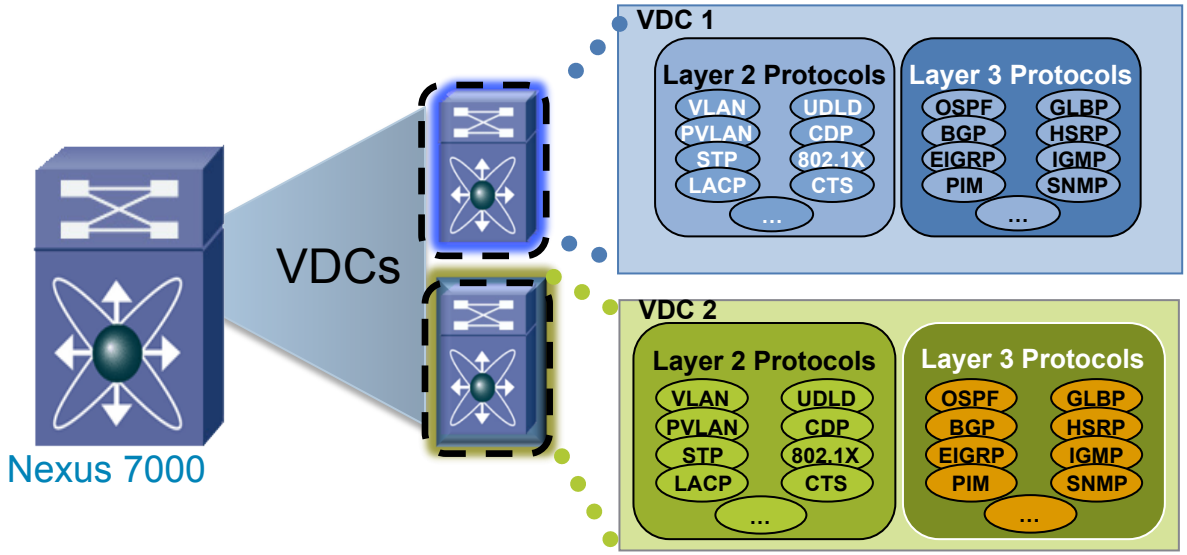


Безопасность сетевой виртуализации



Контексты коммутатора с помощью VDC

Ключевая функция

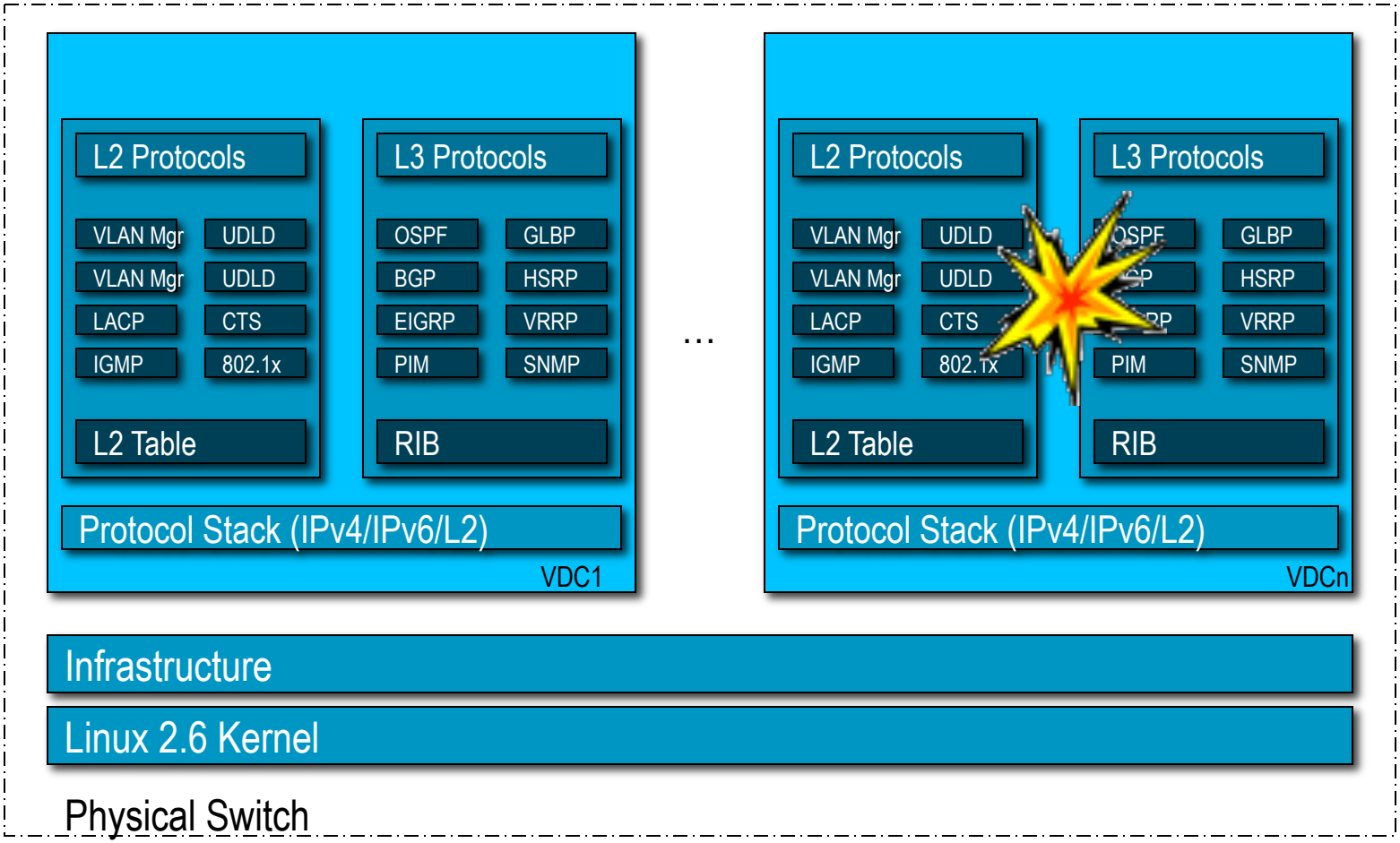


Nexus 7000 VDC – Virtual Device Context

- 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



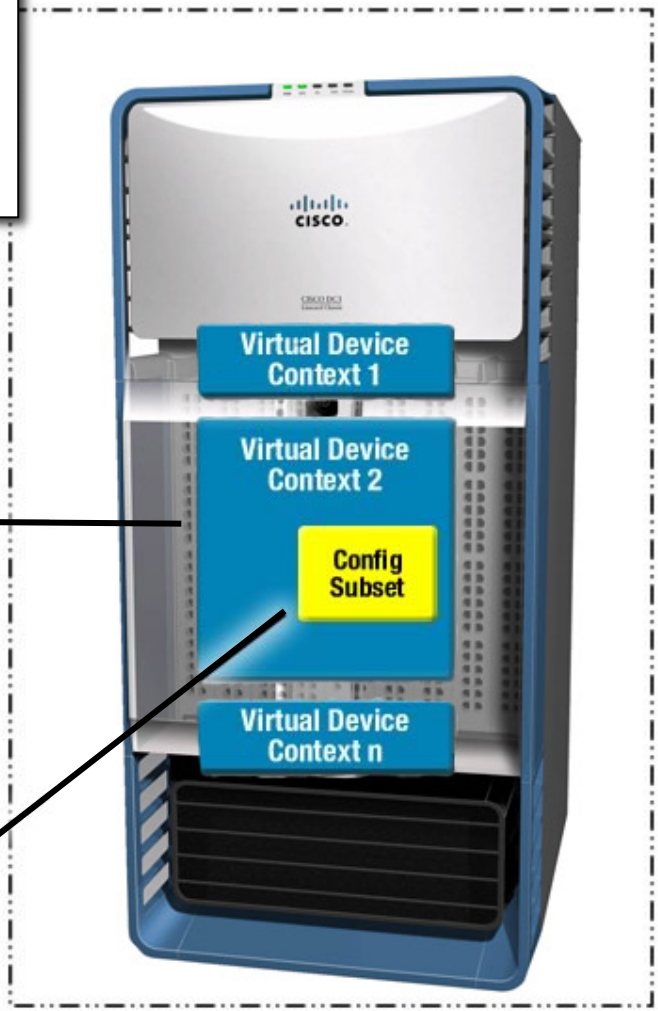
Virtual Device Contexts

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 Nexus7000 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

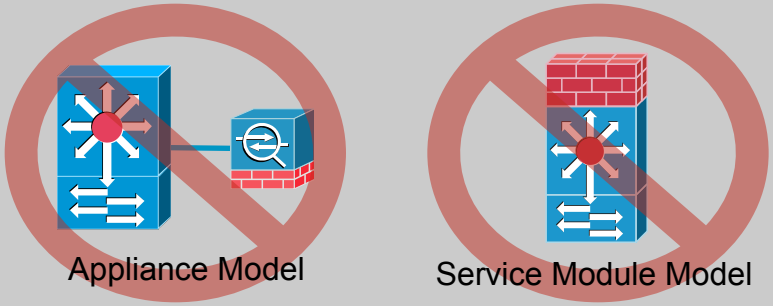
  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1533.pdf

- Cisco Nexus7000 получил сертификацию по требованиям Common Criteria с уровнем соотствествия EAL4 в 2011 году.

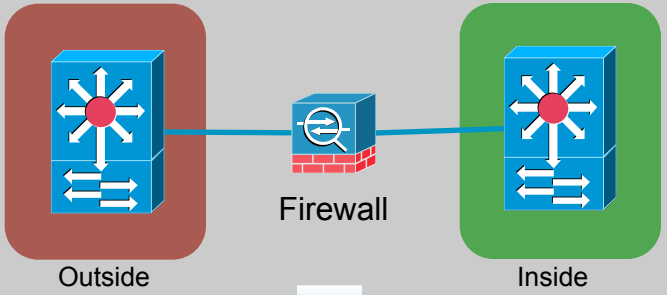
  http://www.niap-ccevs.org/cc-scheme/st/vid10349/

Примеры использования VDC
Безопасное разделение сетей

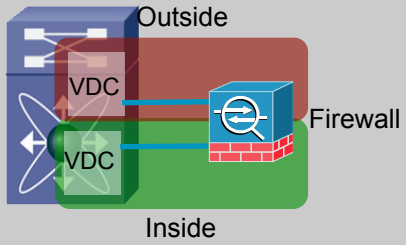
- Департаменты безопасности неохотно воспринимают **коллапсированную** инфраструктуру
- Обеспокоенность вызывает управление конфигурацией и потенциальные ошибки



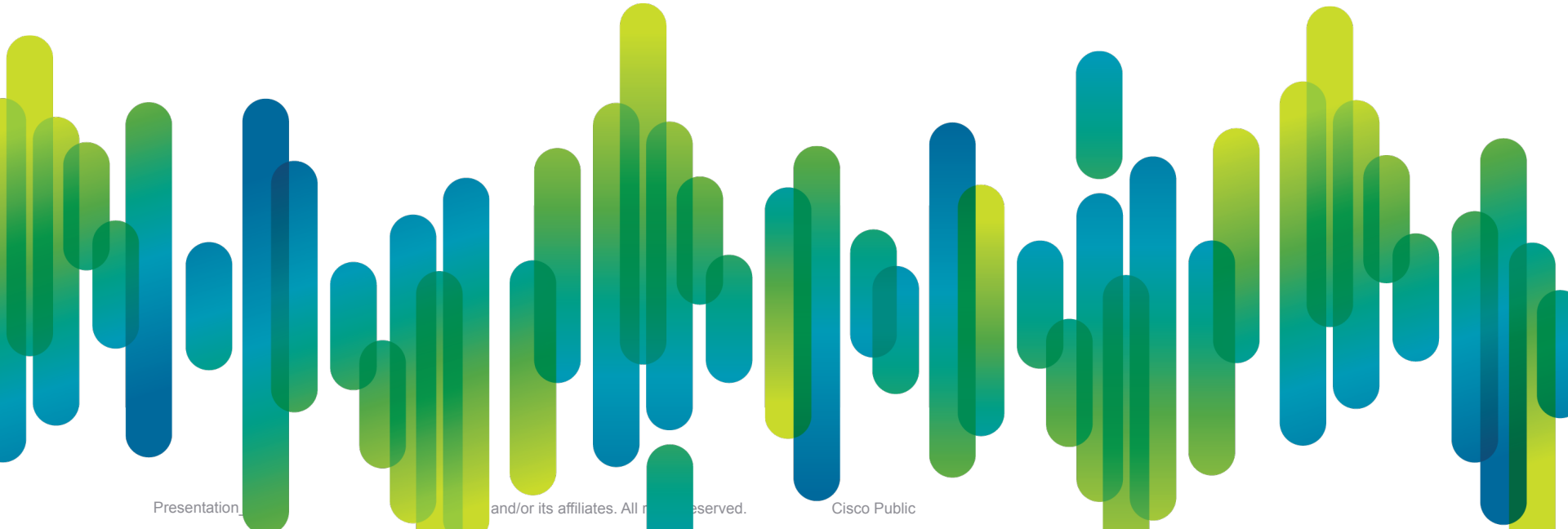
- **Идеальный** вариант – физически разделенная сетевая инфраструктура
- Достаточно накладно для больших сетей.



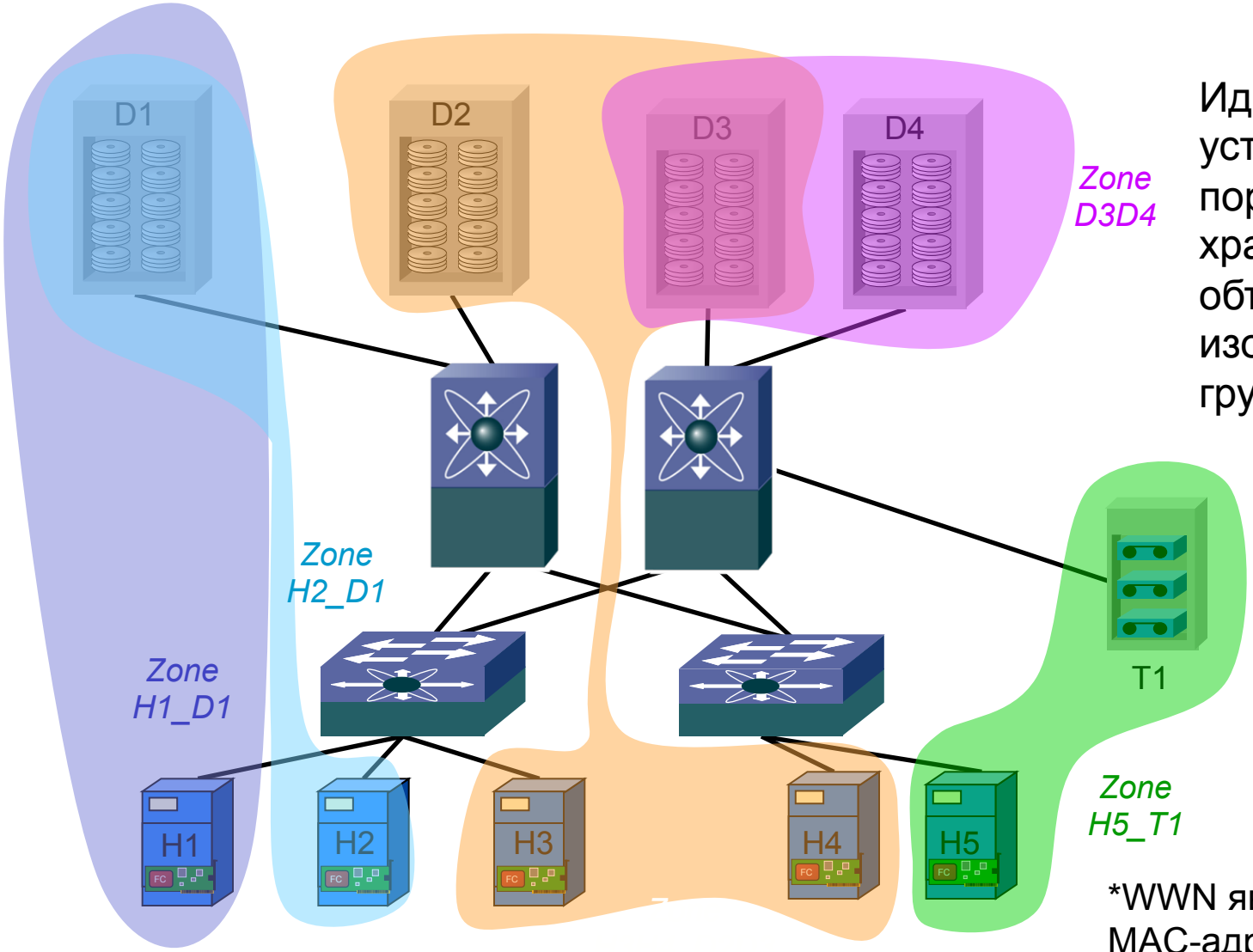
- **VDCs** предоставляет **логическое** разделение сетей, имитирующее физический разрыв
- Очень низкая вероятность обхода защиты
- Модель VDC может применять для выделения DC-сегментов с **тестовыми** или **чувствительными** данными



Виртуализация сетей хранения данных



Доступ к SAN: зонирование FC



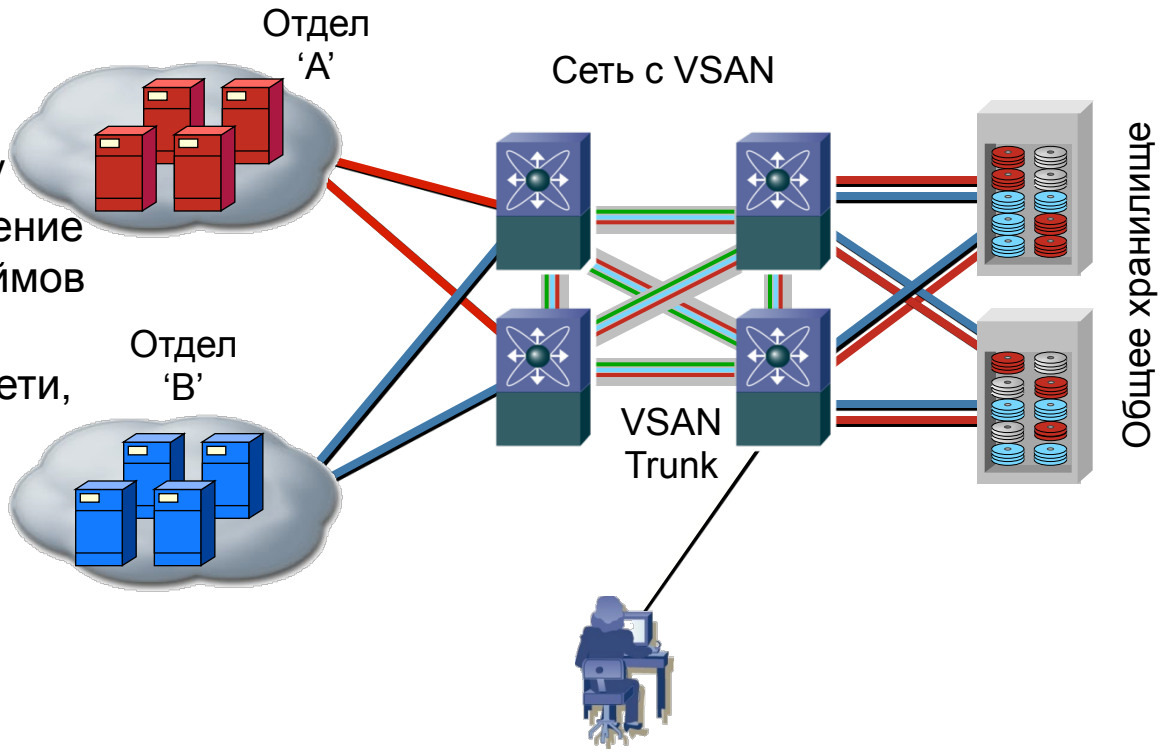
Идентификаторы устройств и портов сети хранения (WWN*) объединяются в изолированную группу.

*WWN является аналогом MAC-адресов в Ethernet

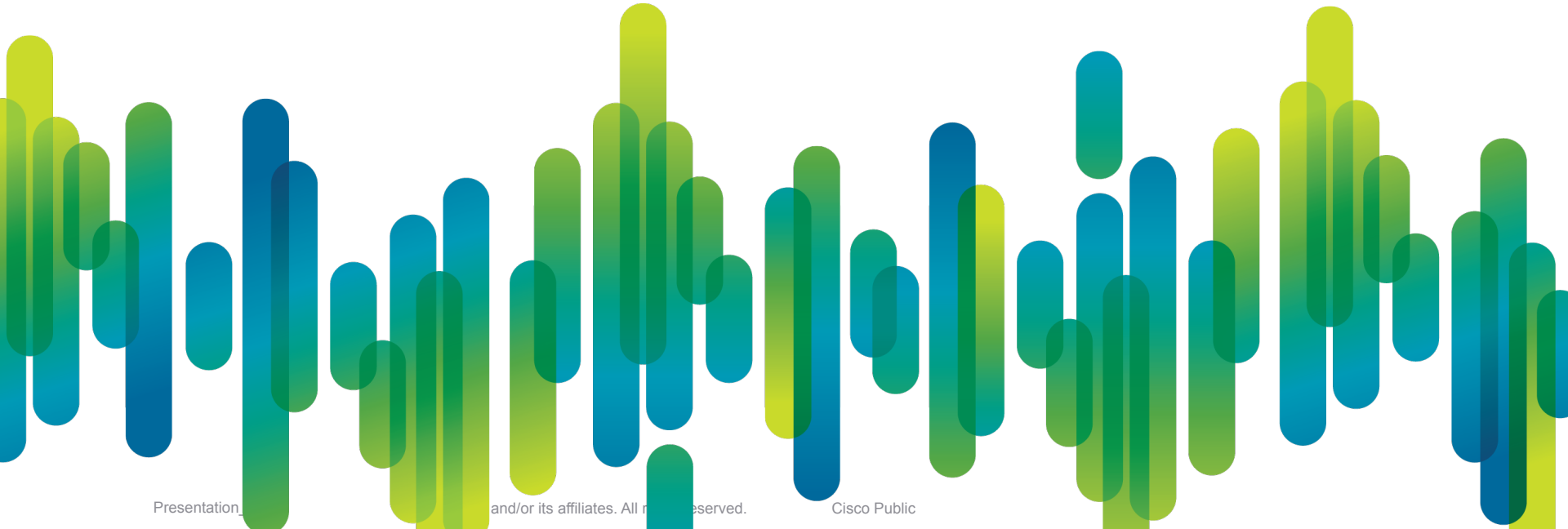
Безопасность уровня доступа: Виртуальные SAN (VSAN)

- 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

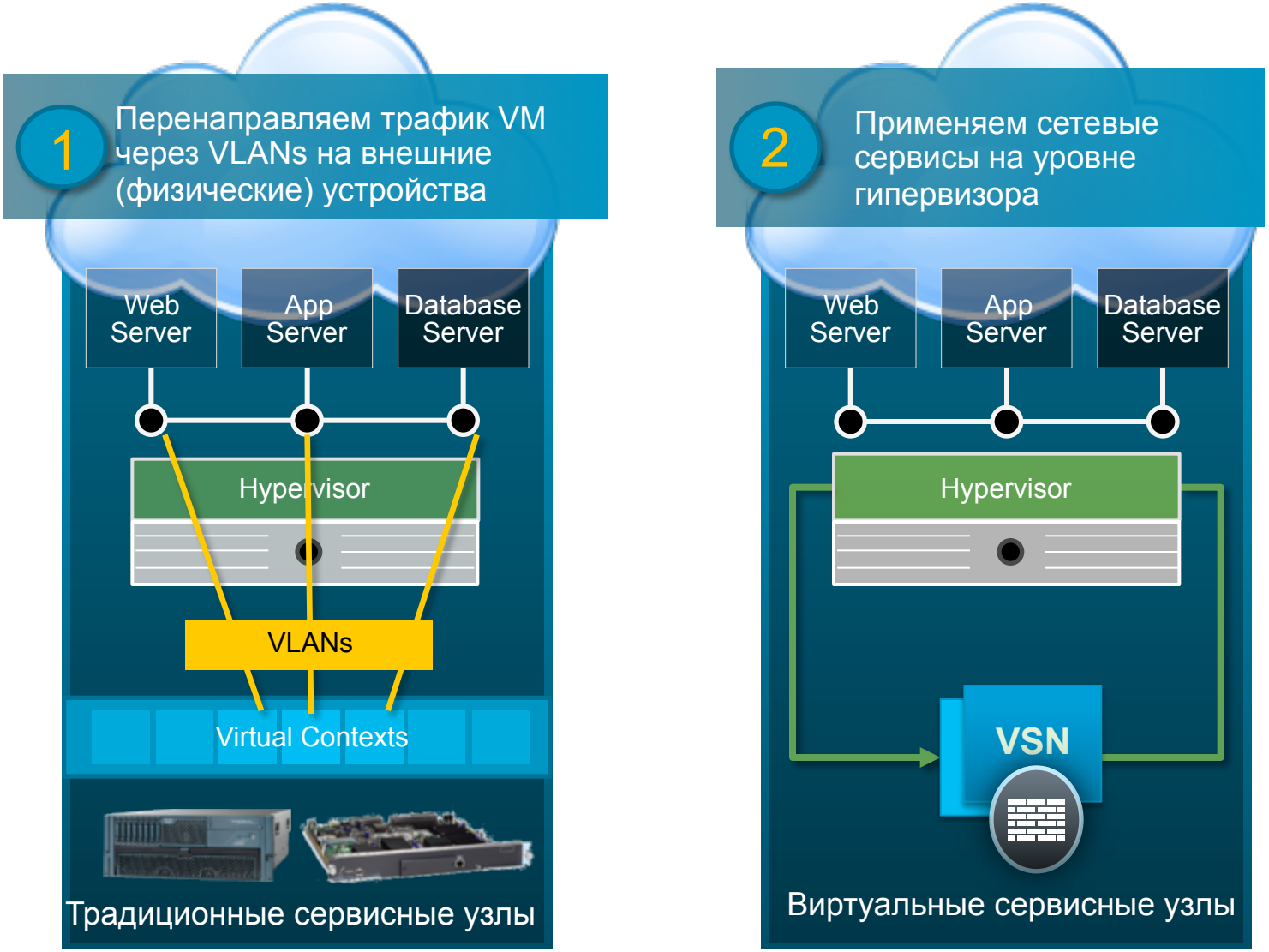
- VSAN обеспечивает:
  - Изоляцию трафика
    Строгая изоляция между VSAN используя разделение сети и тегирование фреймов
  - Сервисы сети в VSAN
    Независимые сервисы сети, включая сервер имен, зонирования, FSPF и менеджер домена в каждой VSAN.



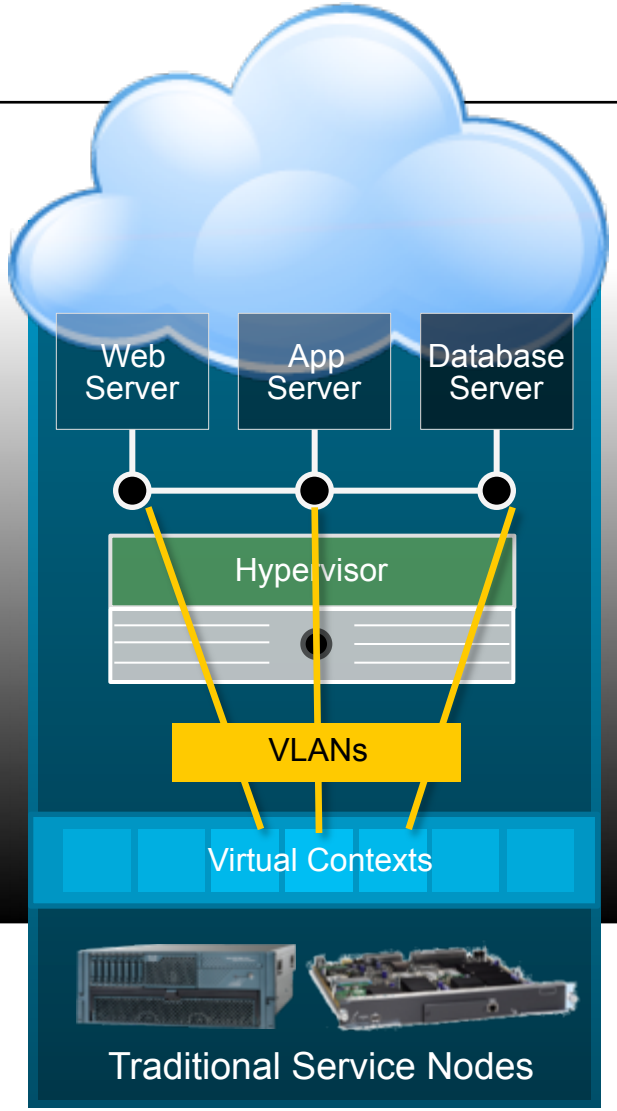
Виртуализация сервисов безопасности



Физические и Виртуальные сервисные сетевые узлы



Физические межсетевые экраны



Сервисный модуль ASA

Устройства ASA 5585

Поддержка виртуализации в ASA

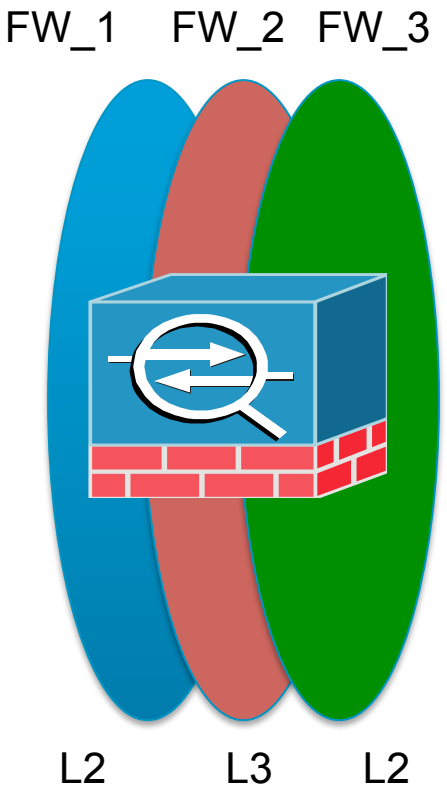
Виртуальные контексты на семействе ASA

- до 256 виртуальных контекстов на ASA 5585 SSP-20, 40, 60 и ASA SM
- до 1024 VLAN, которые могут разделяться между контекстами
- 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

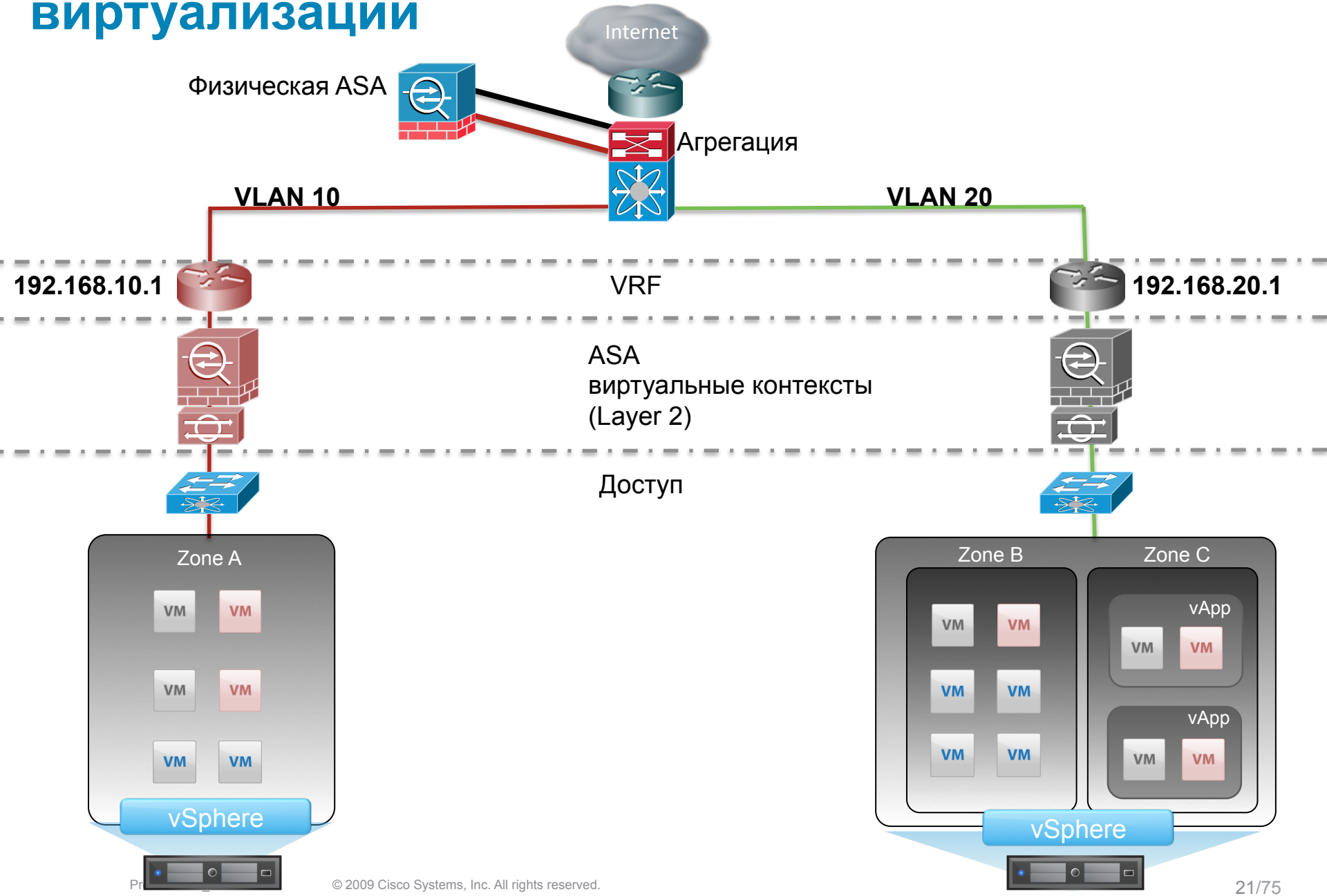
Поддержка полноценной маршрутизации и Site-to-Site IPSec в L3-контекстах летом 2012 года



Традиционная модель контроля трафика Север-Юг в ЦОД

- Входящий и исходящий трафик из каждой зоны маршрутизируется и фильтруется с помощью физического устройства
- Физические устройства защиты иногда нужны, но являются достаточно дорогим решением

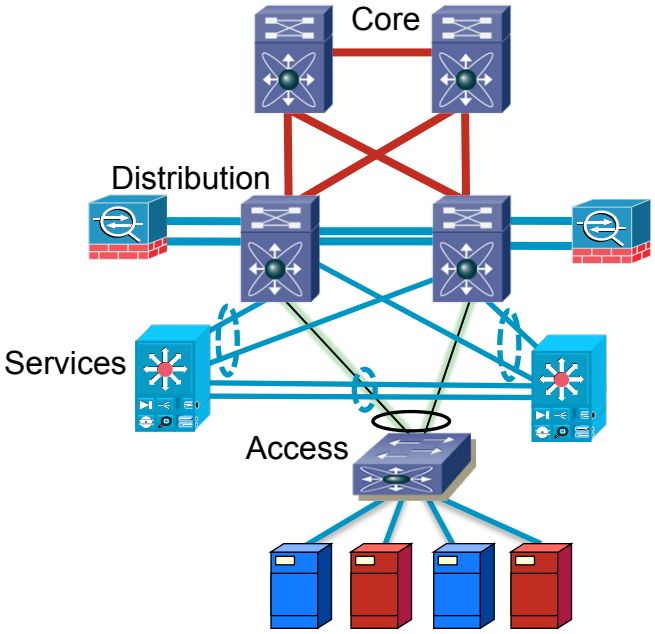
Контроль трафика Север-Юг с помощью сетевой виртуализации



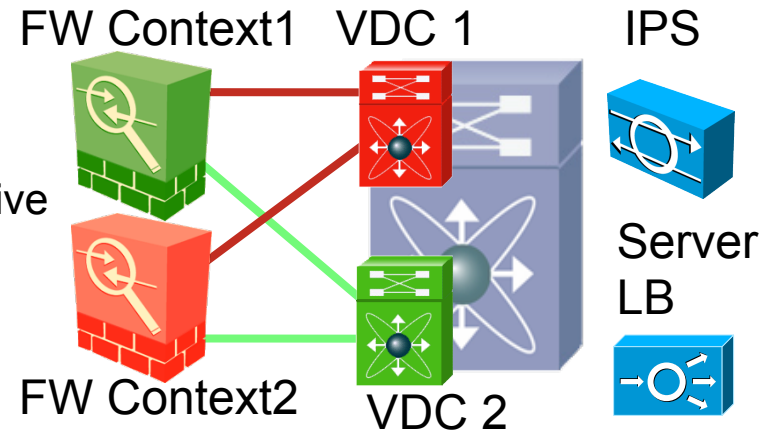
Опции внедрения функций ИБ

Уровень распределения

- Функции безопасности вынесены на уровень распределения
- Средства защиты могут фильтровать трафик между VDC и серверными VLAN

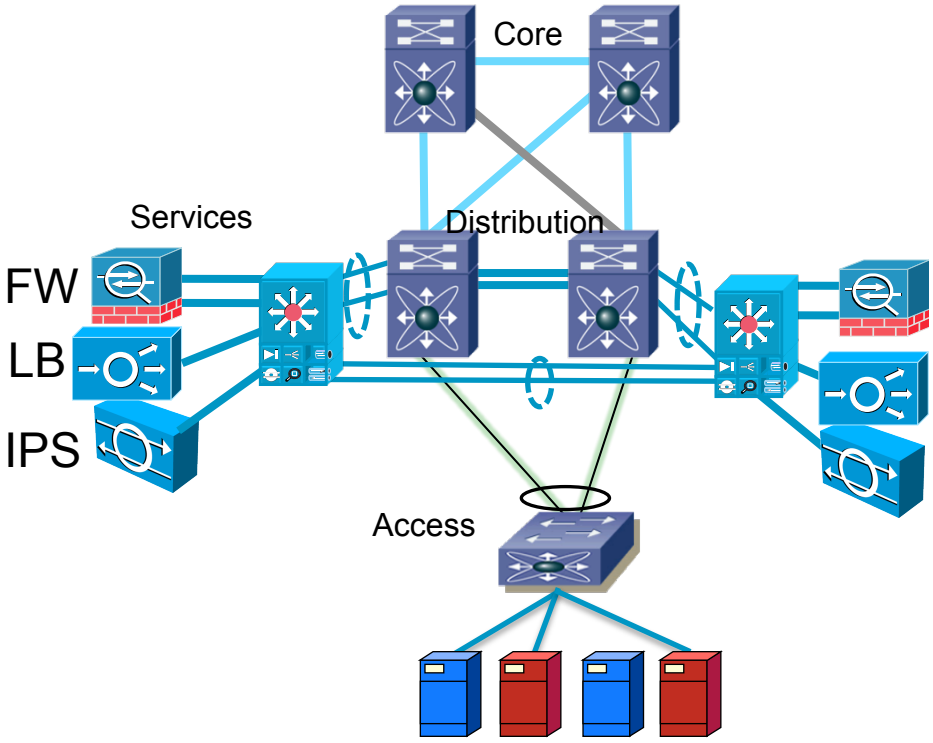


- Routed или Bridge
- IPS inline или passive
- Single или Multiple Contexts



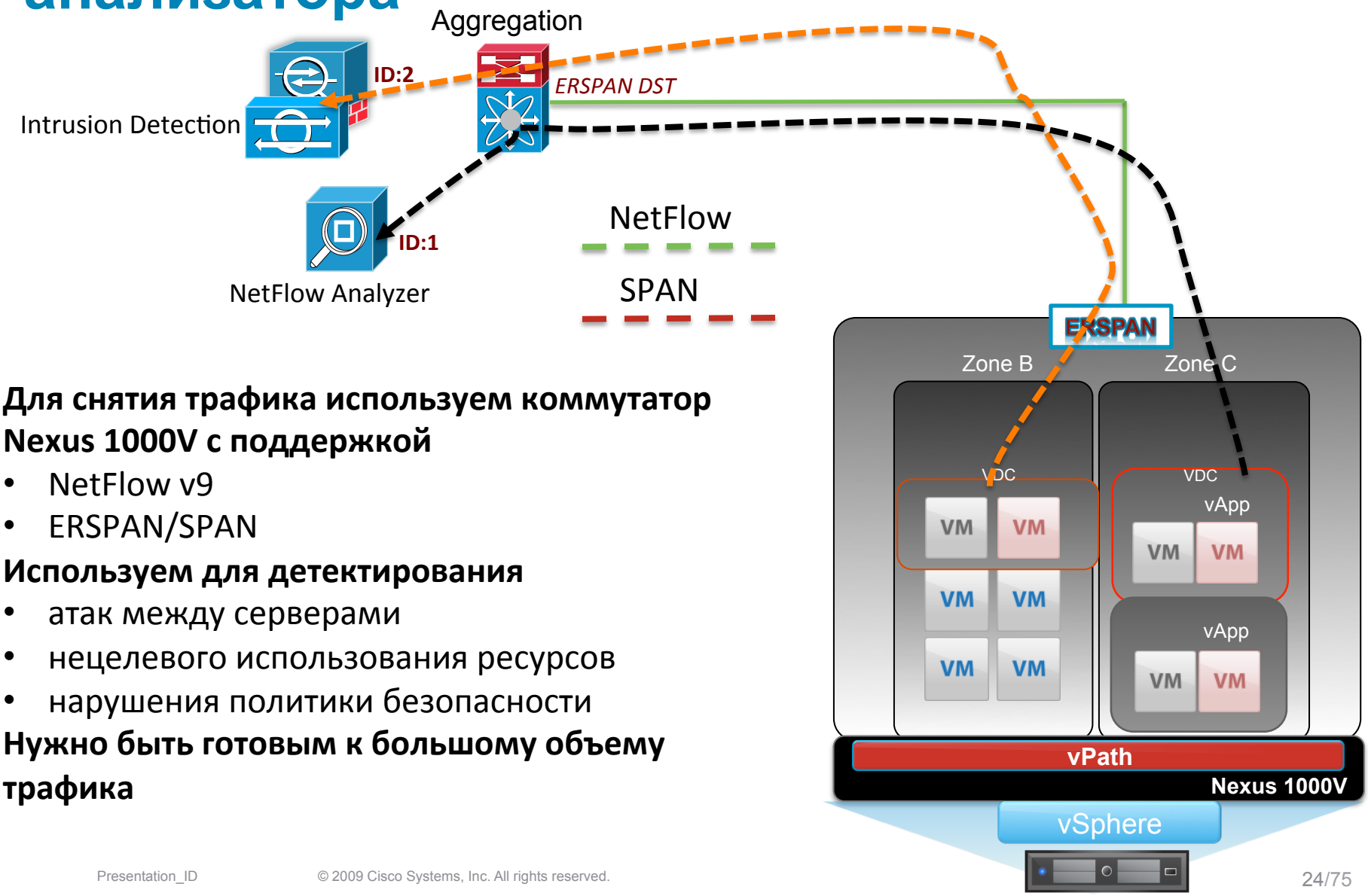
Опции внедрения функций ИБ

Блок сервисов



- Централизованное внедрение и управление средствами защиты, балансировки, оптимизации приложений
- Решение масштабируется и расширяется без изменения дизайна
- Гибкие варианты внедрения (модули или устройства)

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



Для снятия трафика используем коммутатор Nexus 1000V с поддержкой

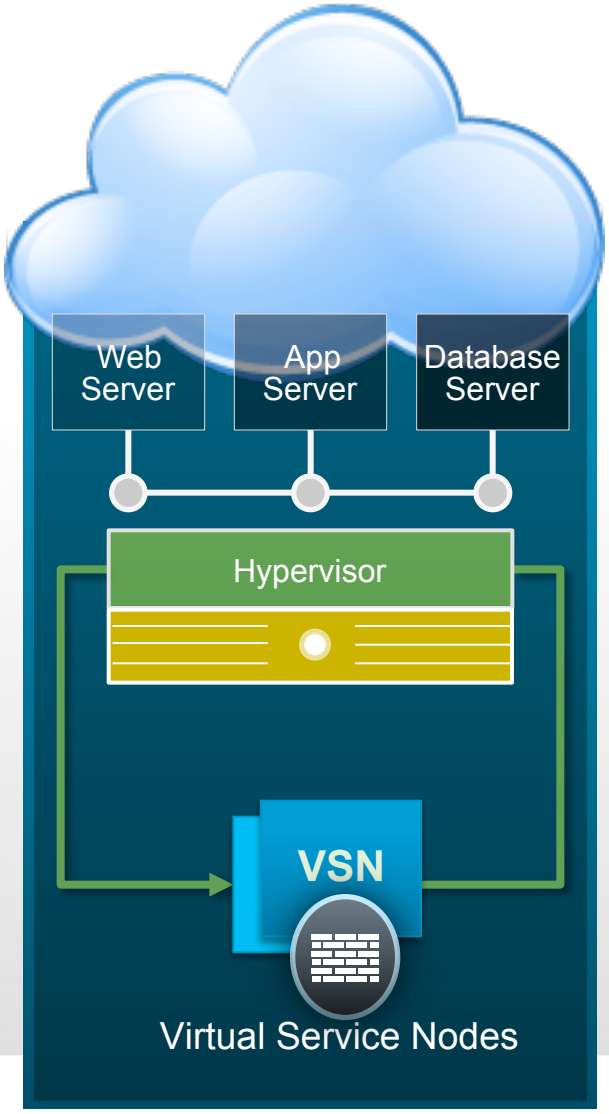
- NetFlow v9
- ERSPAN/SPAN

Используем для детектирования

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

Нужно быть готовым к большому объему трафика

Виртуализация & Виртуальные сервисные узлы



Virtual Security Gateway

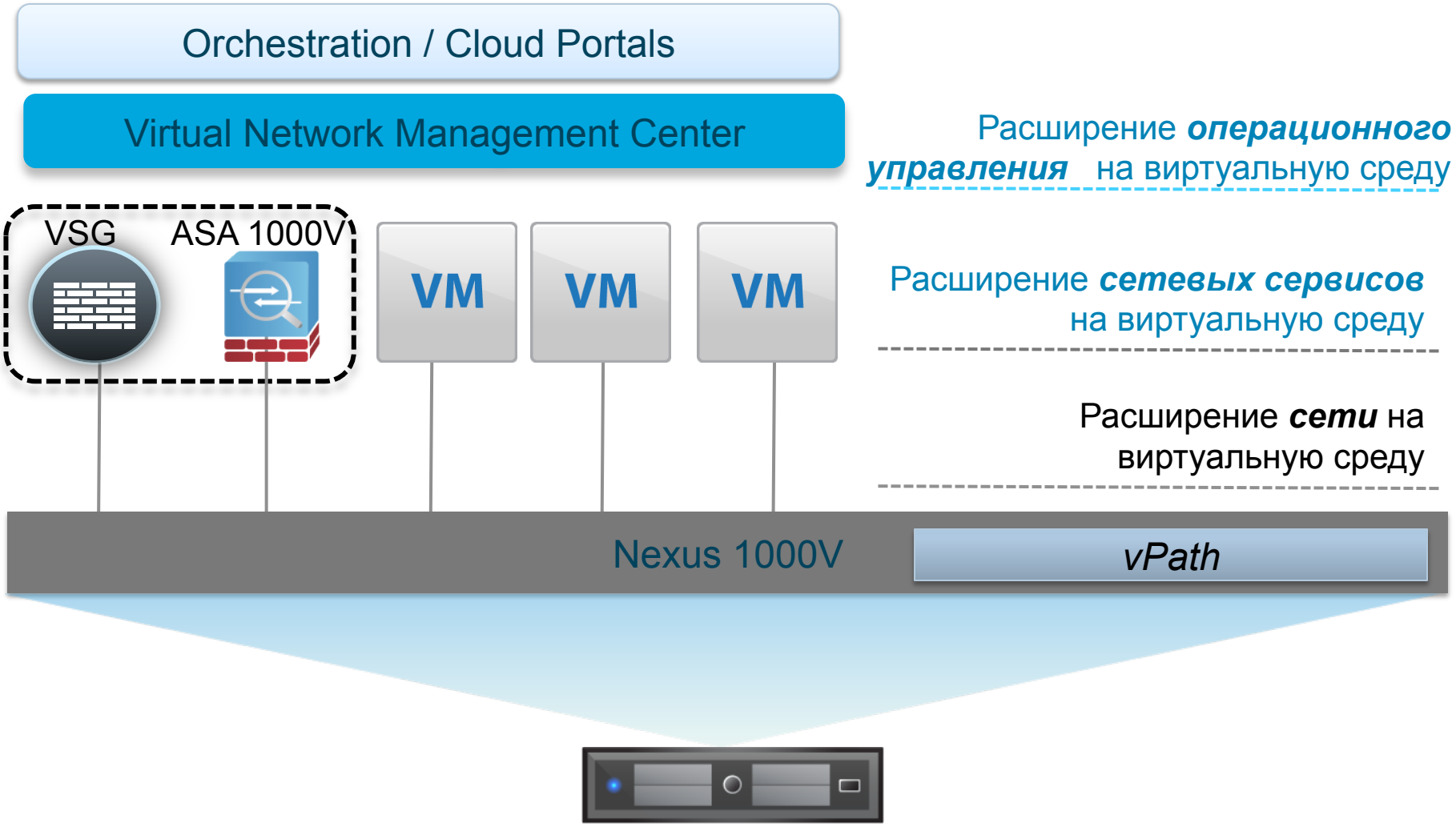
Nexus 1000V

Сегментация VMs на основе зон внутри виртуального ЦОД

ASA 1000V

Внедрение на границе виртуального ЦОД

Архитектура виртуальных сервисов безопасности

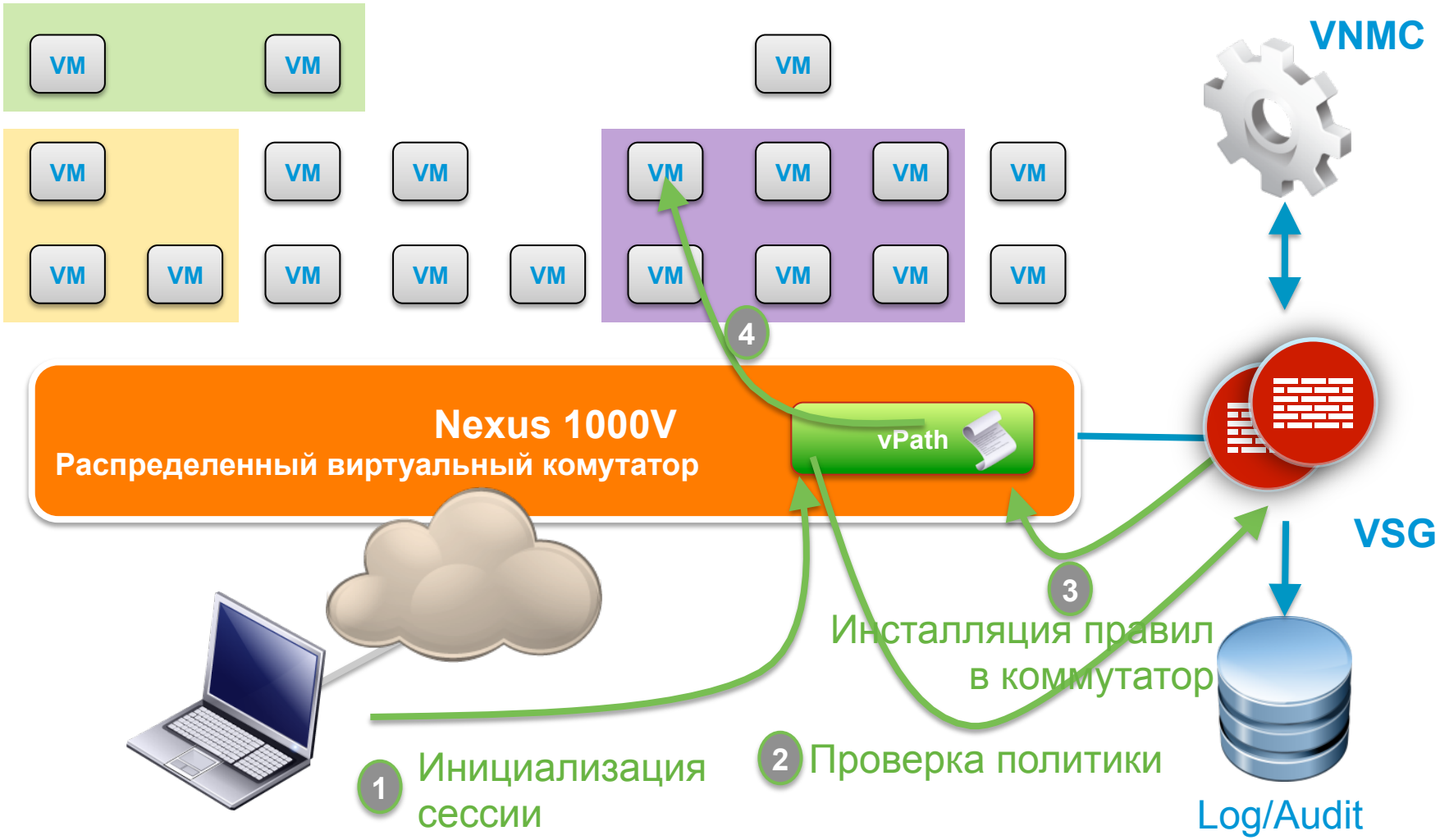


Расширение ***операционного управления*** на виртуальную среду

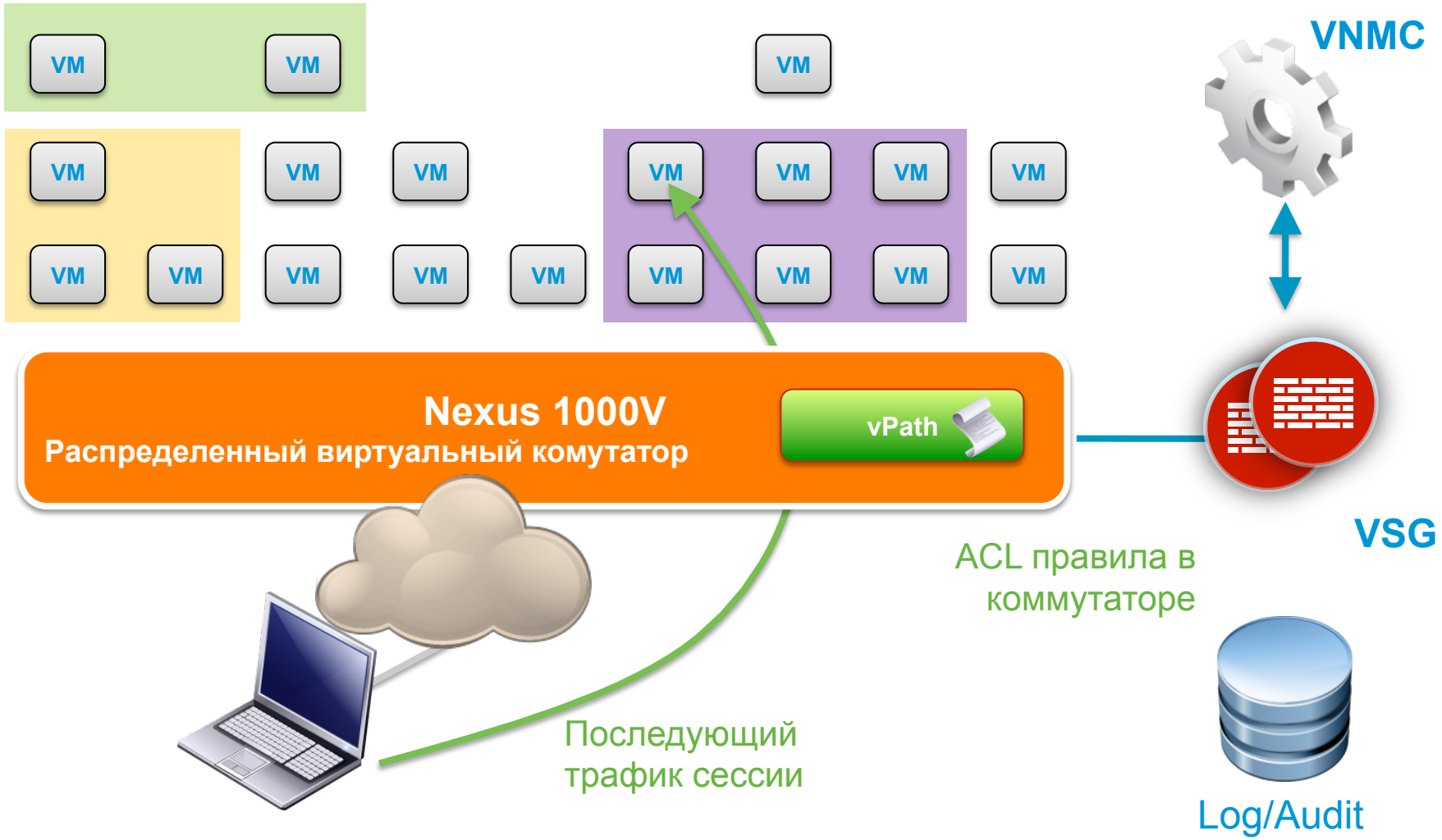
Расширение ***сетевых сервисов*** на виртуальную среду

Расширение ***сети*** на виртуальную среду

vPath: Высокая Производительность



VSG: Высокая Производительность



Cisco Virtual Security Gateway

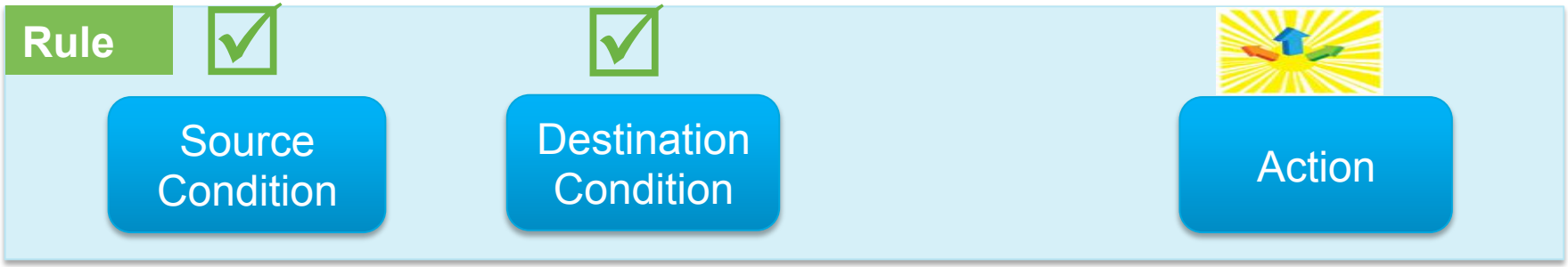
Virtual Security Gateway (VSG)

Контекстная безопасность	Правила с атрибутами VM
Контроль на основе зон	Создание зон безопасности
Динамическая политика	Политика следует за vMotion
Масштабируемая архитектура	Отказоустойчивость, VSG обслуживает несколько VMs

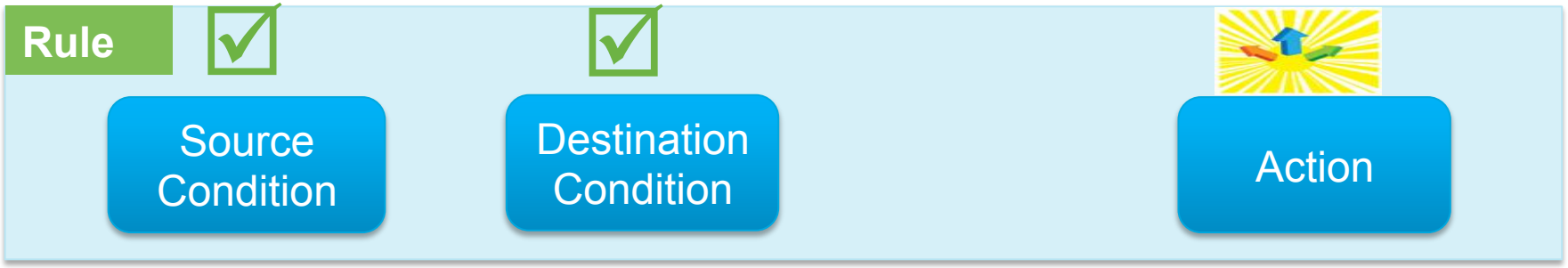
Virtual Network Management Center (VNMC)

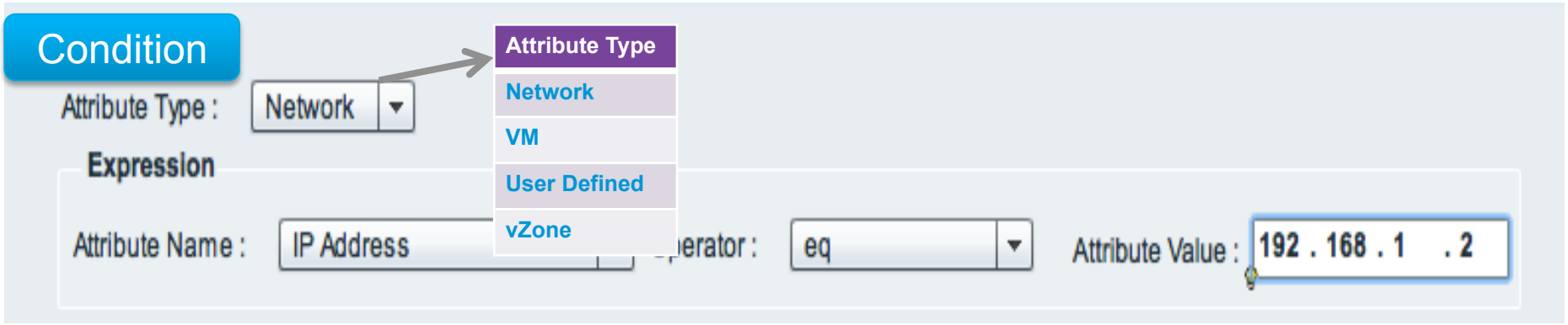
Непрерывные операции	Команда безопасности управляет политиками
Управление на основе политик	Централизованное управление, multi-tenancy
Автоматизаци	XML API, профили безопасности

Профиль безопасности: правила

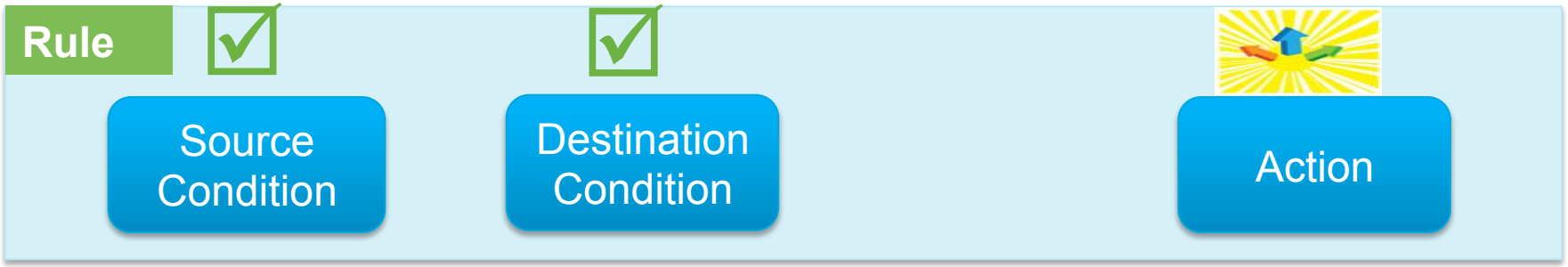


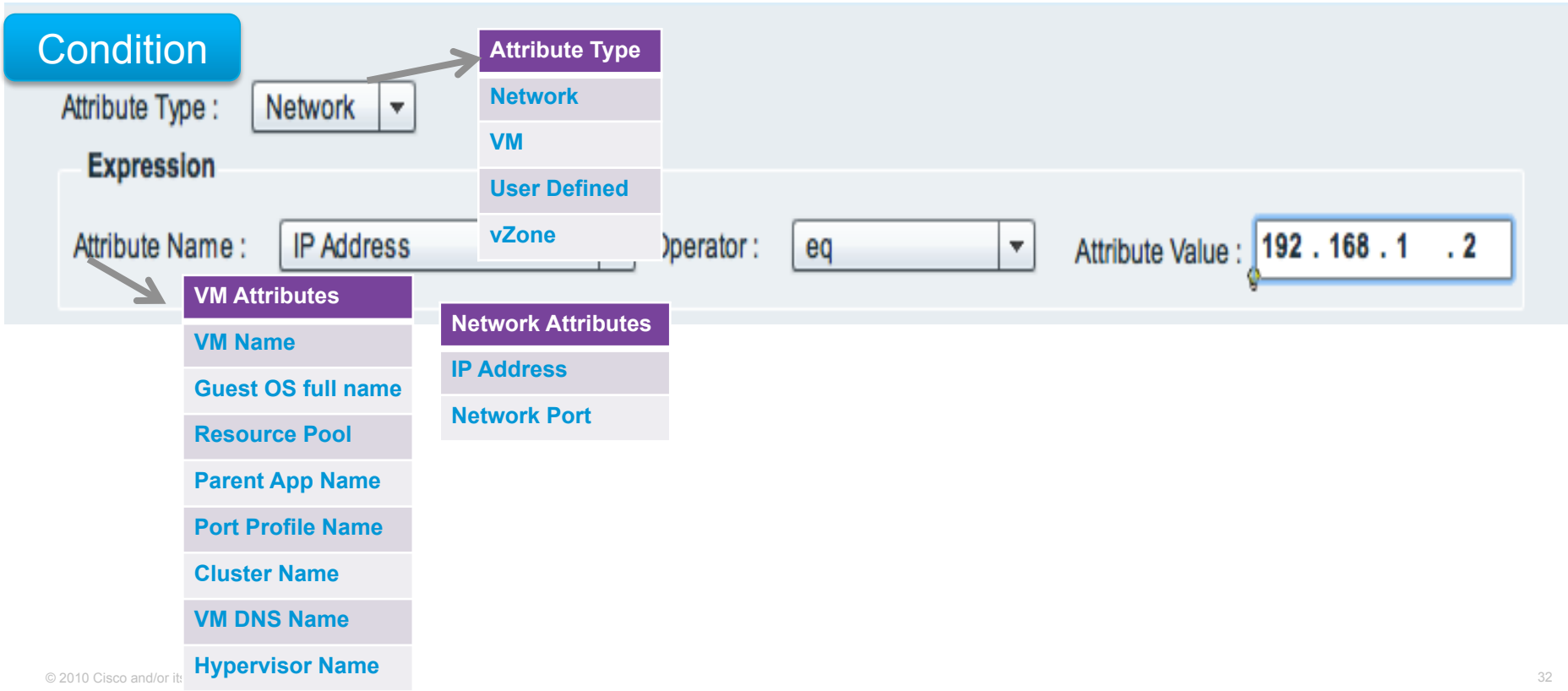
Профиль безопасности: правила



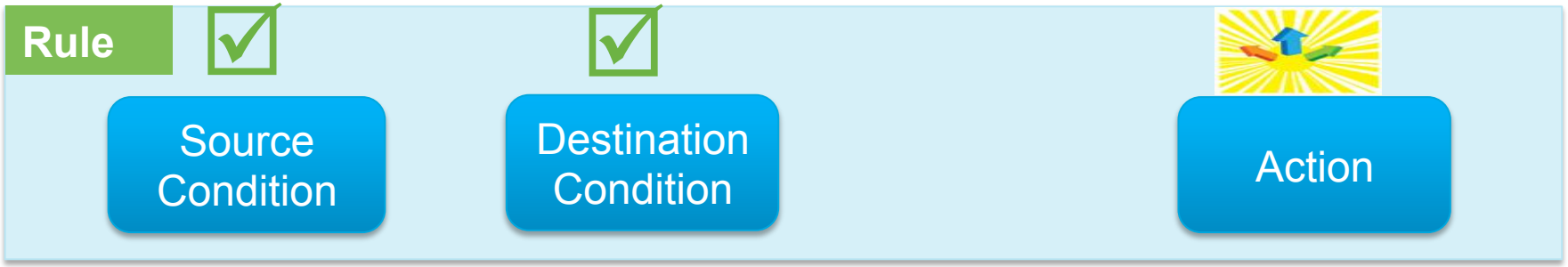


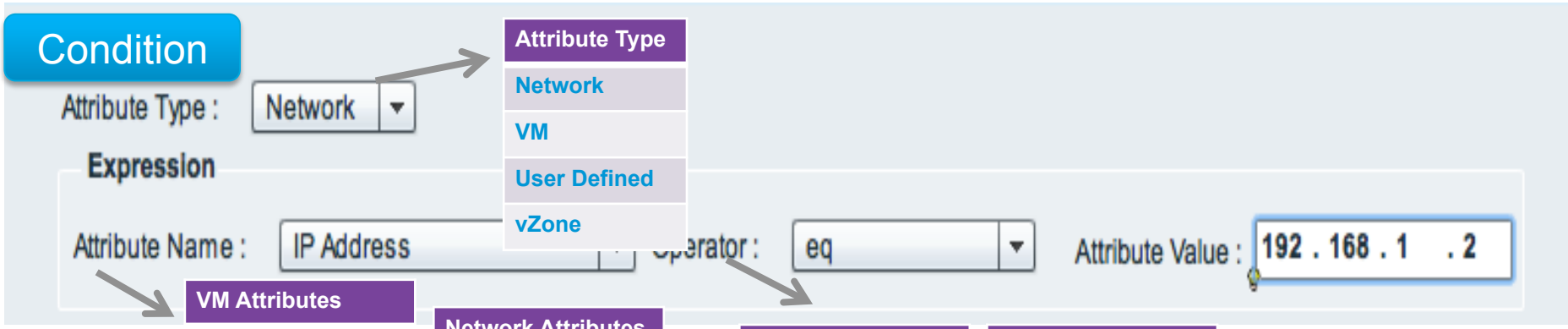
Профиль безопасности: правила





Профиль безопасности: правила





Attribute Type
Network
VM
User Defined
vZone

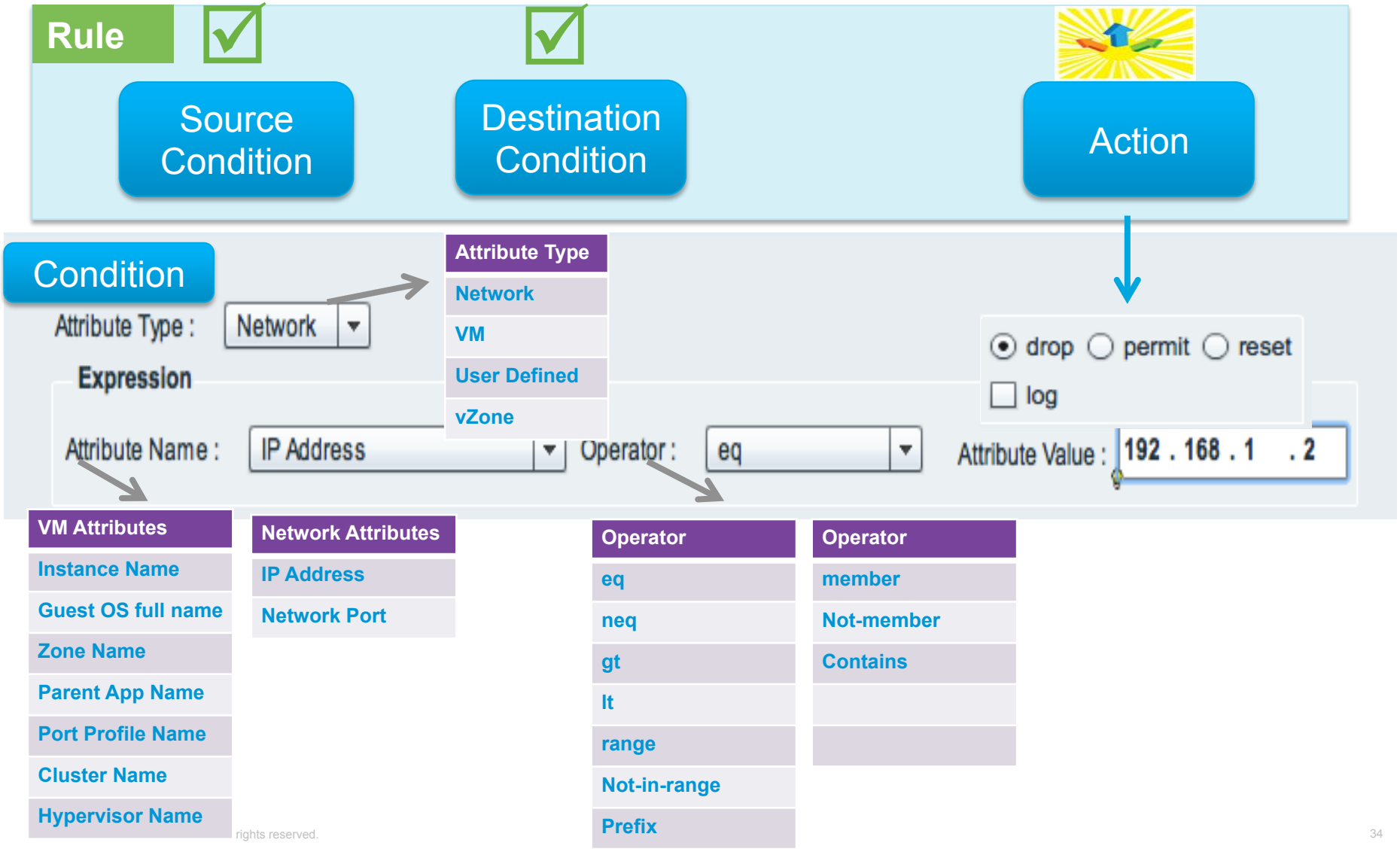
VM Attributes
VM Name
Guest OS full name
Resource Pool
Parent App Name
Port Profile Name
Cluster Name
VM DNS Name
Hypervisor Name

Network Attributes
IP Address
Network Port

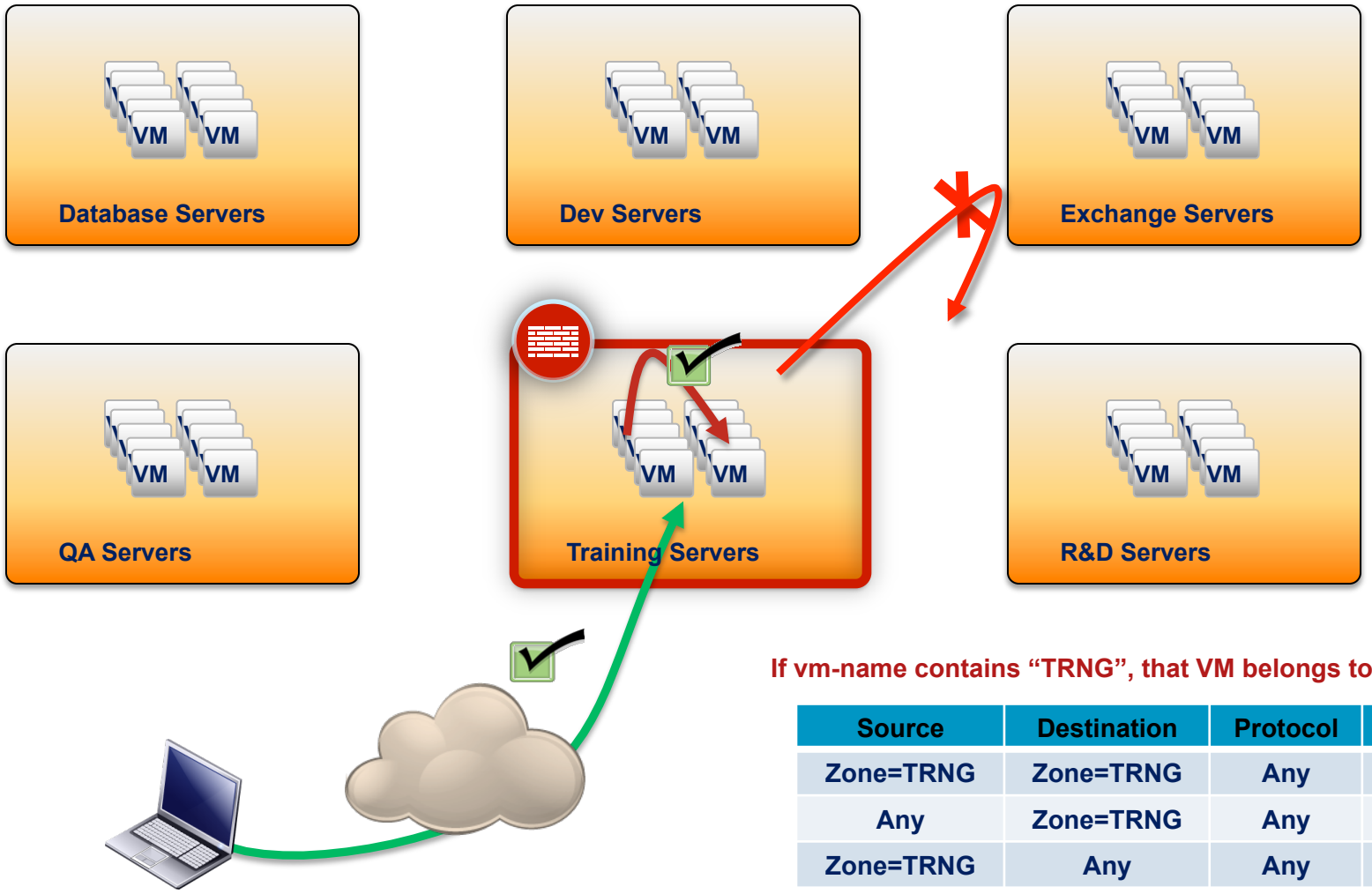
Operator
eq
neq
gt
lt
range
Not-in-range
Prefix

Operator
member
Not-member
Contains

Профиль безопасности: правила



Пример VSG
Логические Зоны, vMotion & масштабирование

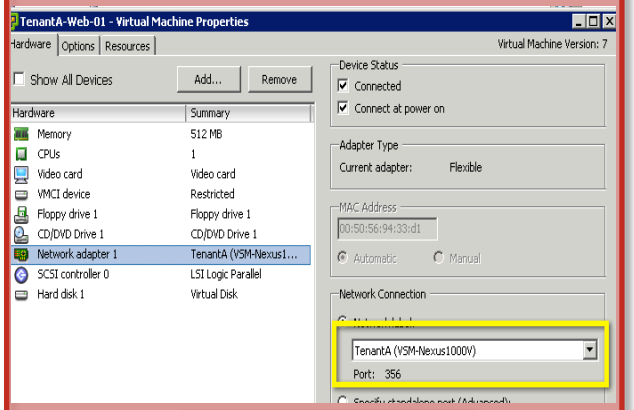


If vm-name contains “TRNG”, that VM belongs to TRNG zone

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

Модель управления безопасностью в виртуальной среде

vCenter



Port Group

Администраторы серверов

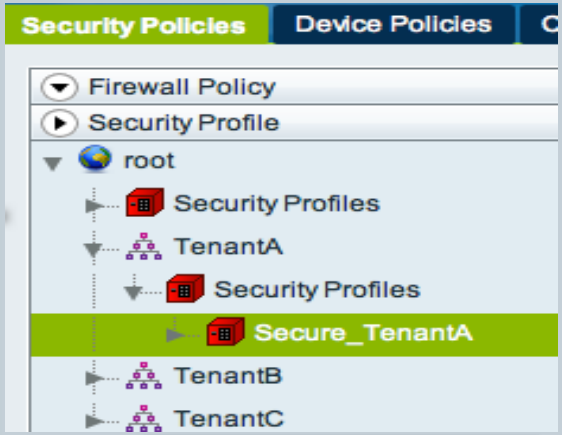
Nexus 1KV

```
port-profile type vethernet TenantA
  vmware port-group
  switchport access vlan 10
  switchport mode access
  org root/TenantA
  vn-service ip-address 192.168.173.42 vlan 20 security-profile Secure_TenantA
  state enabled
```

Port Profile

Сетевые администраторы

VSG +VNMC

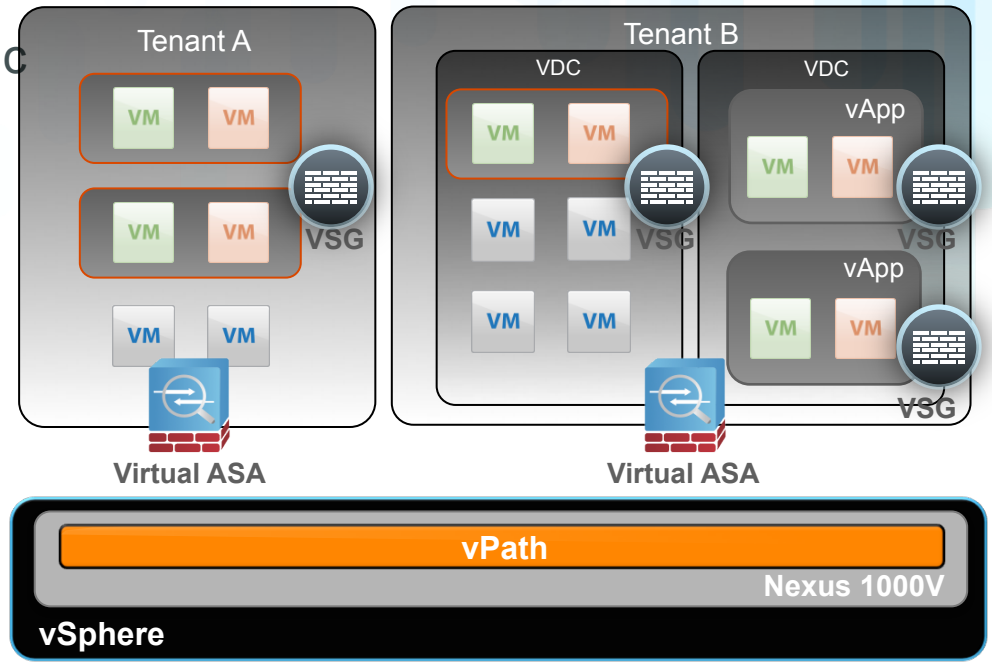


Security Profile

Администраторы безопасности

ASA 1000v – облачный межсетевой экран

- Использует такой же код как и устройства и модули Cisco ASA
- Поддержка глубоких инспекций ASA с учетом состояния.
- IPSEC site-to-site VPN
- Совместная модель безопасности
  - VSG для зон безопасности в пределах одного клиента
  - Virtual ASA для контроля безопасности на границе ЦОД клиент
- Интеграция с Nexus 1000V & vPath

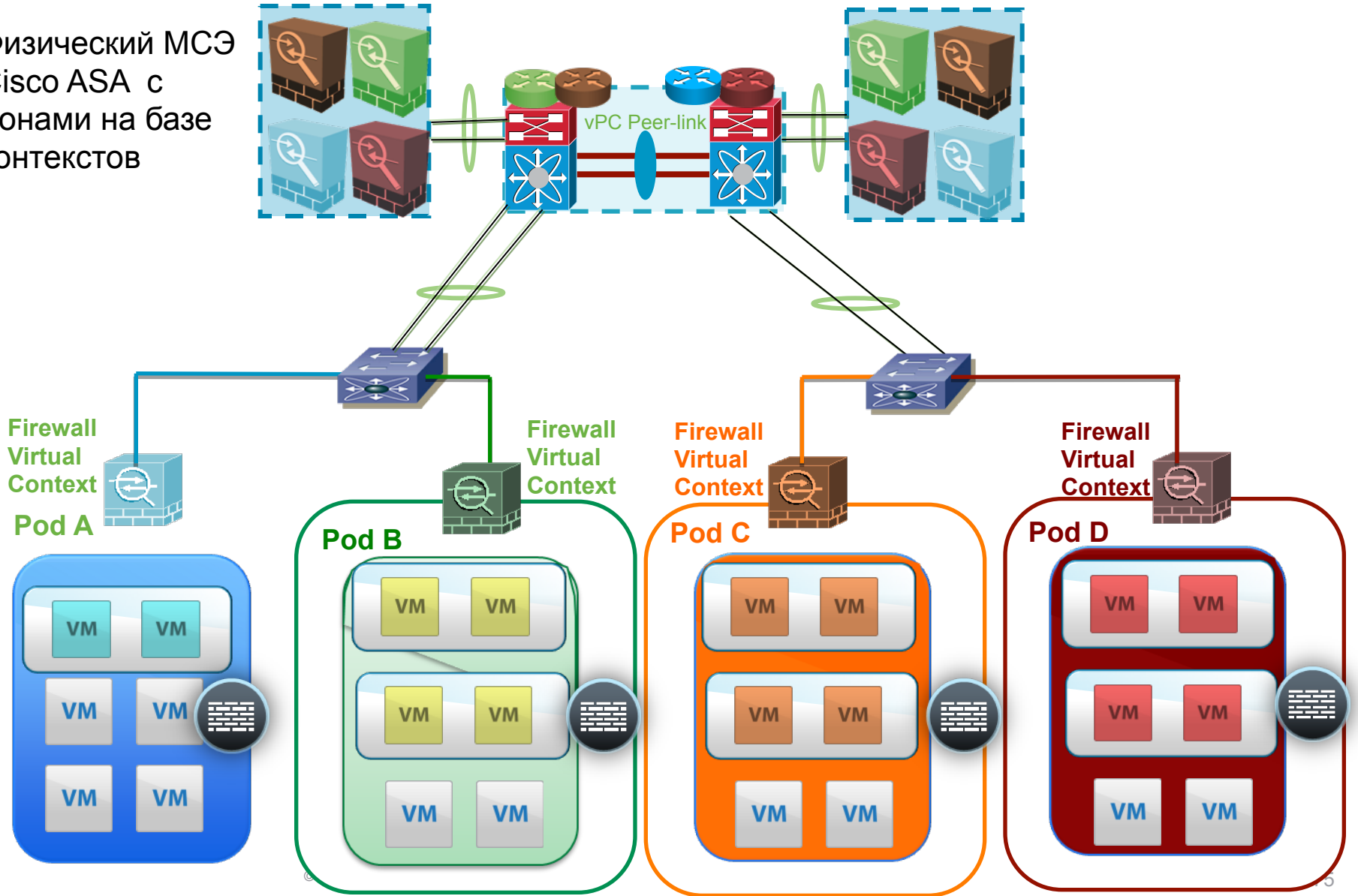


Модель безопасности облачного ЦОД с микросегментацией

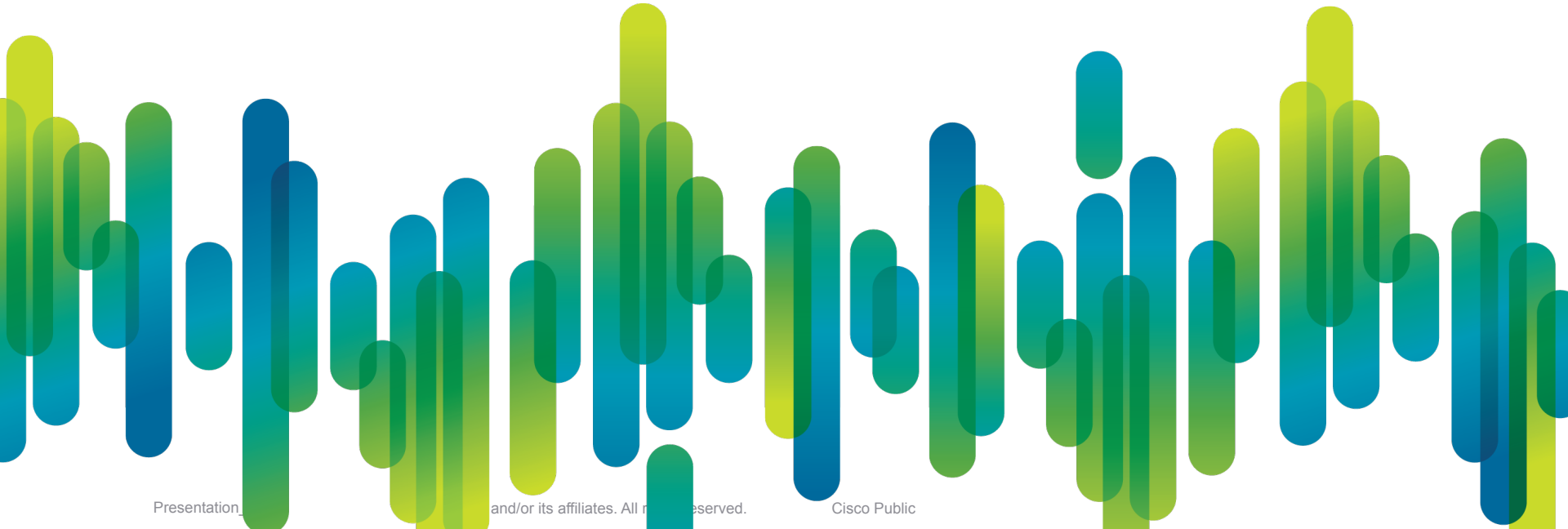
- Глубокая инспекция входящего/исходящего в виртуальный ЦОД трафика на ASA 1000V
- NAT и DHCP на ASA 1000V
- Шифрование трафика между облачным ЦОД и сетями клиентов на ASA 1000V
- Микросегментация на Cisco VSG

Модель безопасности корпоративного ЦОД с микросегментацией

Физический МСЭ Cisco ASA с Зонами на базе контекстов



Безопасность виртуальных десктопом VDI/VXI



Безопасность VDI/VXI инфраструктуры

В целом VDI/VXI инфраструктура более безопасна чем традиционная сеть из PC

- пользовательская среда жестко контролируется администраторами
- управление конфигурацией/патчами централизовано
- пользовательские данные централизованы
- вся конфиденциальная информация централизована

НО возникает ряд дополнительных задач безопасности !!

- Возникает новый уровень доступа в ЦОД
- Необходимо контролировать доступ в сеть тонких клиентов
- Удаленные подключения к VDI через Интернет
- Использование персональных устройств для VDI

Безопасность инфраструктуры VDI/VXI

1. Разделяем сервера и HVD с помощью файервола Cisco ASA и VSG.
2. Контролируем доступ виртуальных десктопов к виртуальным портам – vNIC на UCS, VM-FEX, Nexus 1000V
3. Контролируем доступ тонких клиентов в физическую сеть – Cisco TrustSec/ ISE
4. Подключаем удаленных клиентов через Интернет с Cisco ASA и Cisco AnyConnect

Выводы

- Внедрение виртуализации требует пересмотра оценки рисков в организации
- Для защиты виртуализированных сред требуются новые типы средств защиты либо адаптация традиционных средств с учетом особенностей гипервизора
- Правильно построенная система безопасности виртуализированной среды не уступает по уровню надежности и защищенности традиционной системе

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

- **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


CISCO