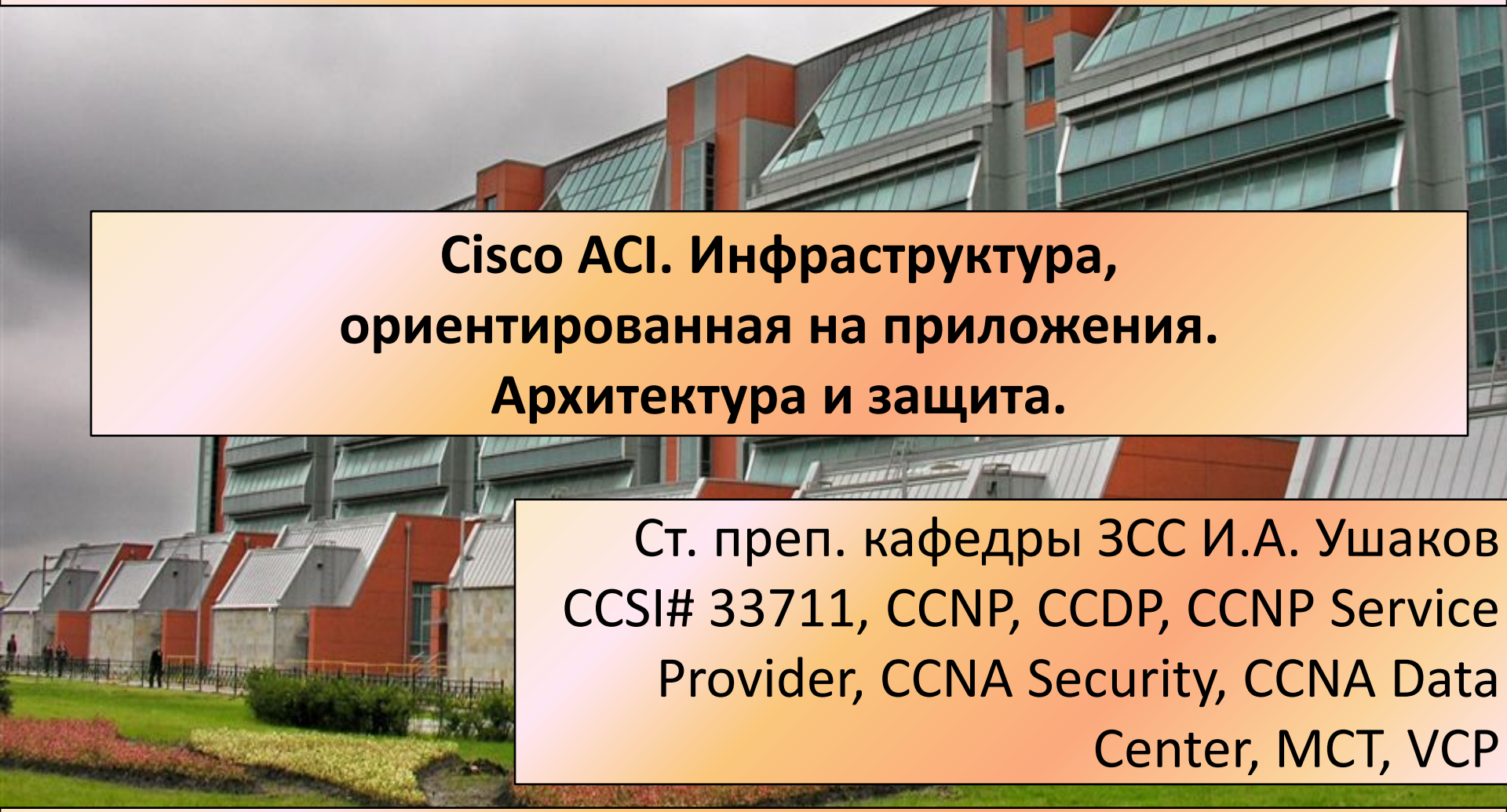
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
СПИИРАН



Cisco ACI. Инфраструктура, ориентированная на приложения. Архитектура и защита.

Ст. преп. кафедры ЗСС И.А. Ушаков
CCSI# 33711, CCNP, CCDP, CCNP Service Provider, CCNA Security, CCNA Data Center, MCT, VCP

IM&CTCPA 2018, СПб 23-25.10.2018

Cisco ACI Самое полное решение для сети ЦОД

Application Centric Infrastructure

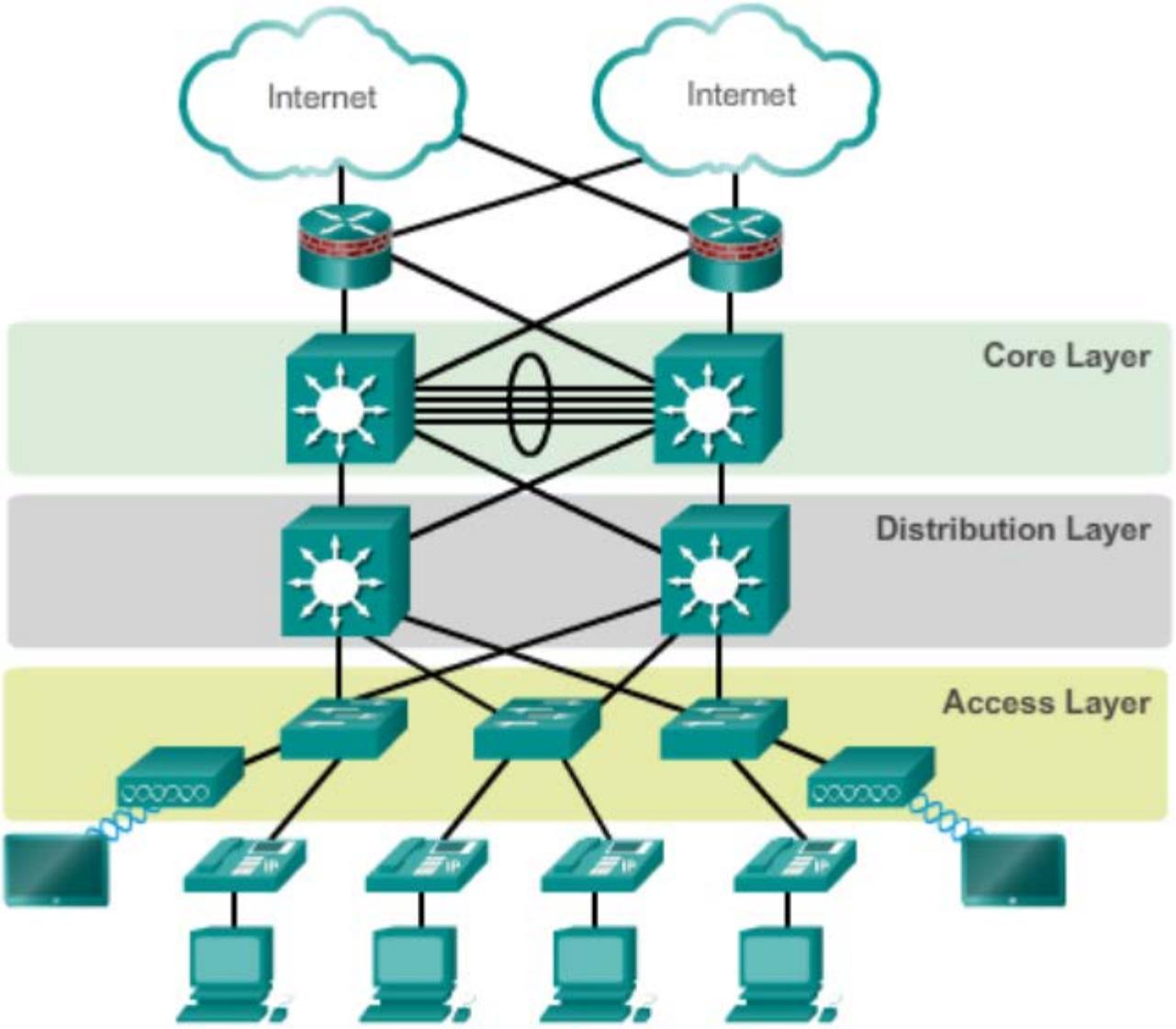
“SDN из коробки”

Открытость, опора на стандарты, встроенная безопасность

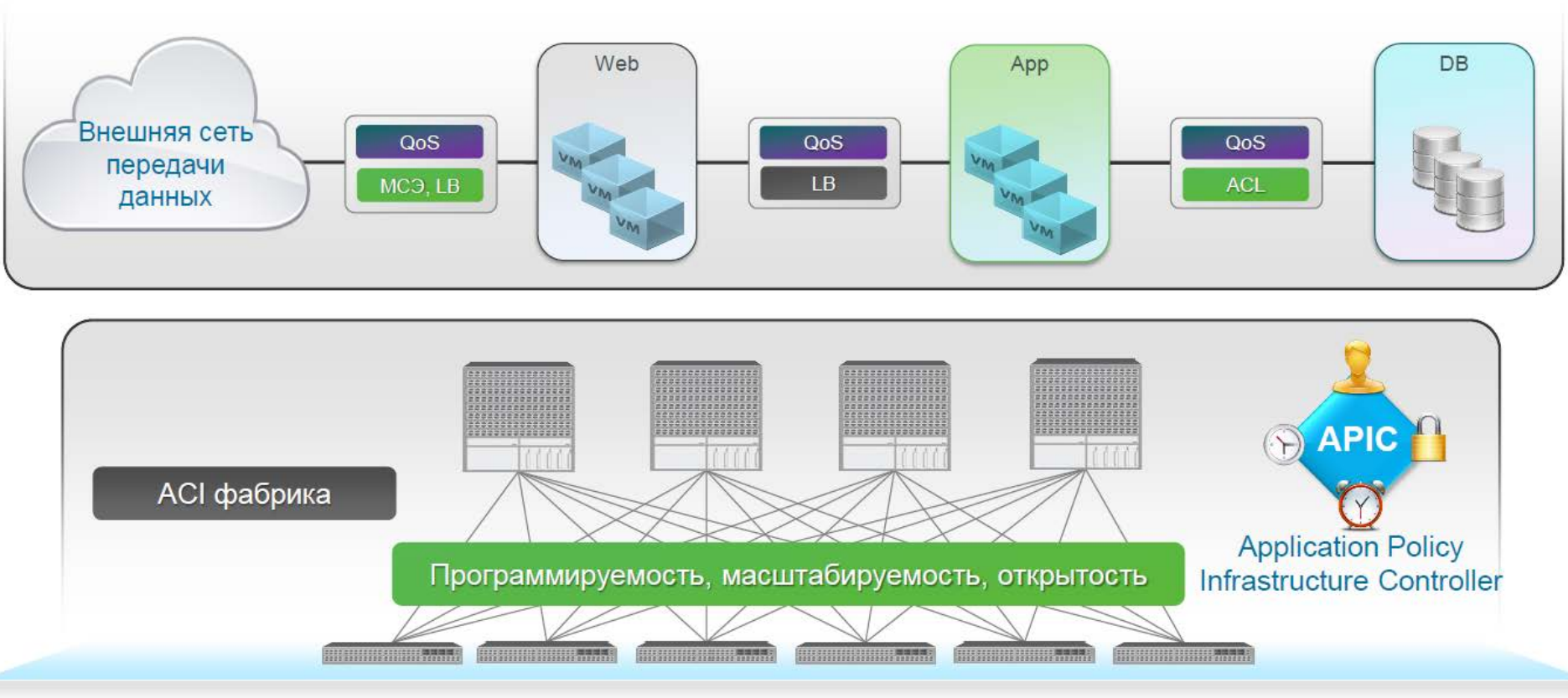
Физические серверы, виртуальные машины и контейнеры

Автоматизация на основе политик

Hierarchical Design Model

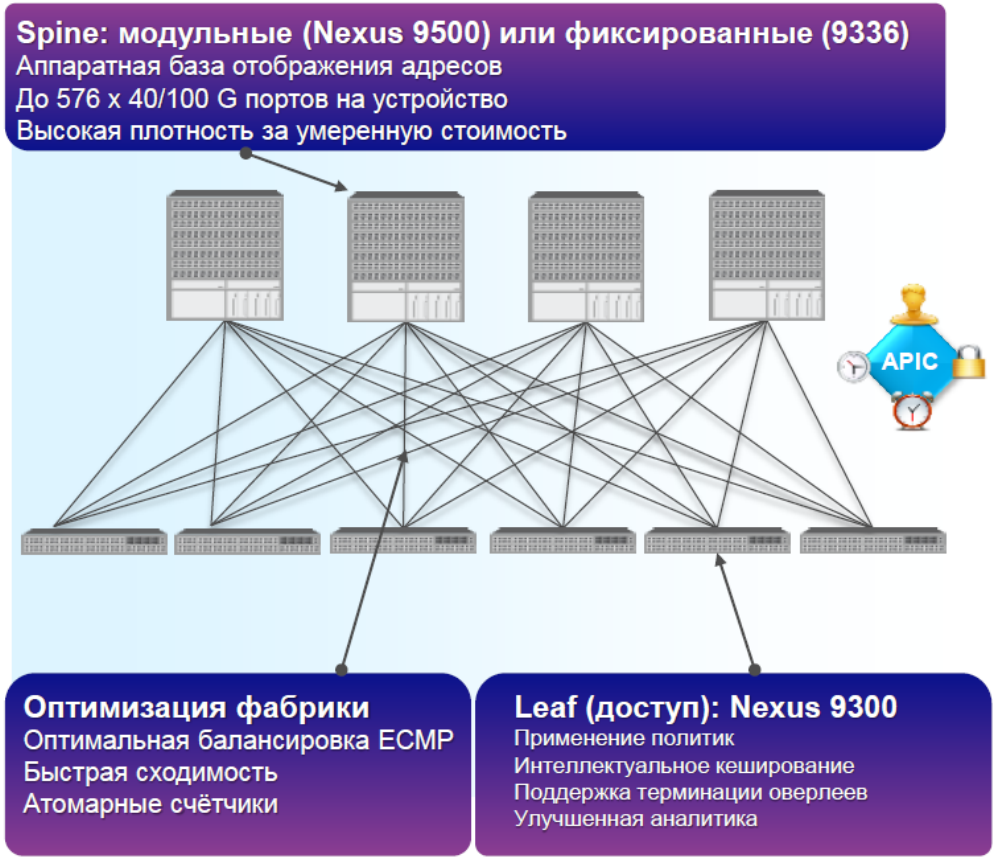


Cisco ACI новое поколение инфраструктуры ЦОД



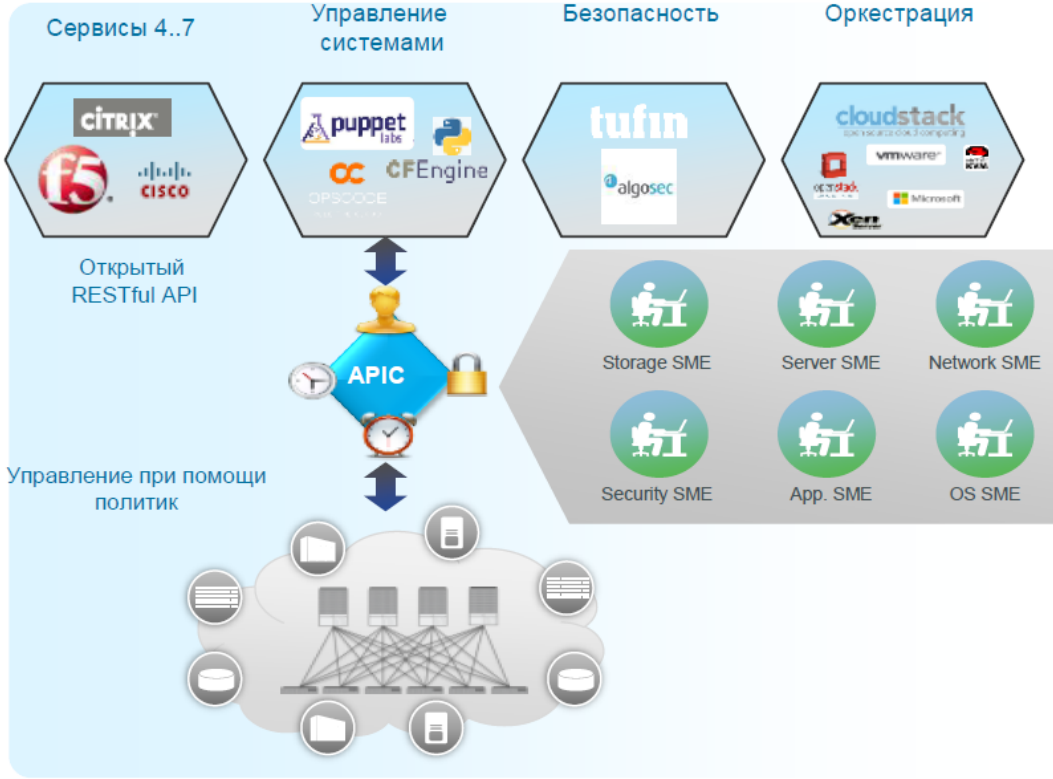
Сетевая фабрика ACI

- **Наиболее эффективная фабрика в индустрии:**
  - 1/10/25/40G на границе сети, высокая плотность 40/100GE на Spine
  - Низкая стоимость за порт / коммутатор
  - Интеграция с существующей инфраструктурой (Cisco или других производителей)
  - Высокая масштабируемость
- **Полная прозрачность – физические или виртуальные серверы, контейнеры**
- **Маршрутизируемая фабрика – оптимальная передача IP трафика**
  - Распределённая коммутация (L2) и маршрутизация (L3)
  - Не требуются программные шлюзы
  - Гибкость развертывания приложений и сервисов – нет ограничений в выборе точки их размещения
  - Улучшенная балансировка трафика (ECMP)
- **Передача метаданных вместе с трафиком**
  - Детальное управление по политикам без необходимости программировать потоки

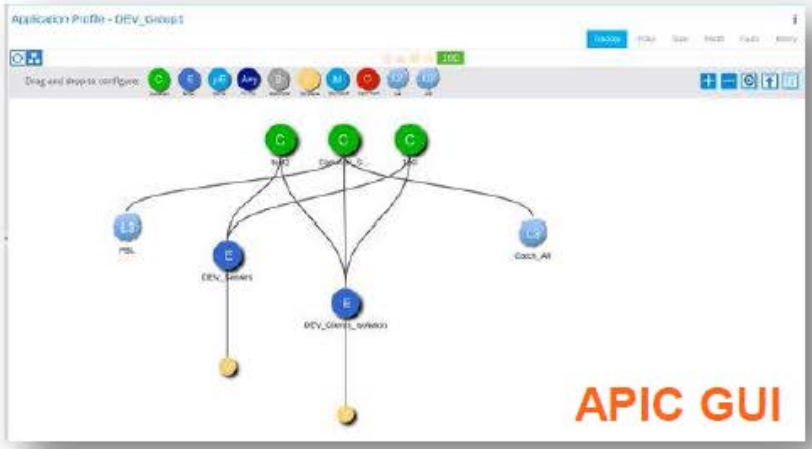


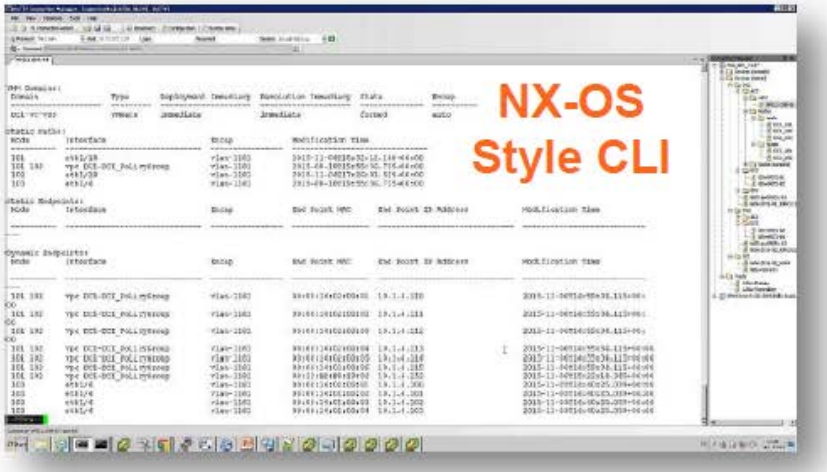
Application Policy Infrastructure Controller
Централизованная автоматизация и управление фабрикой

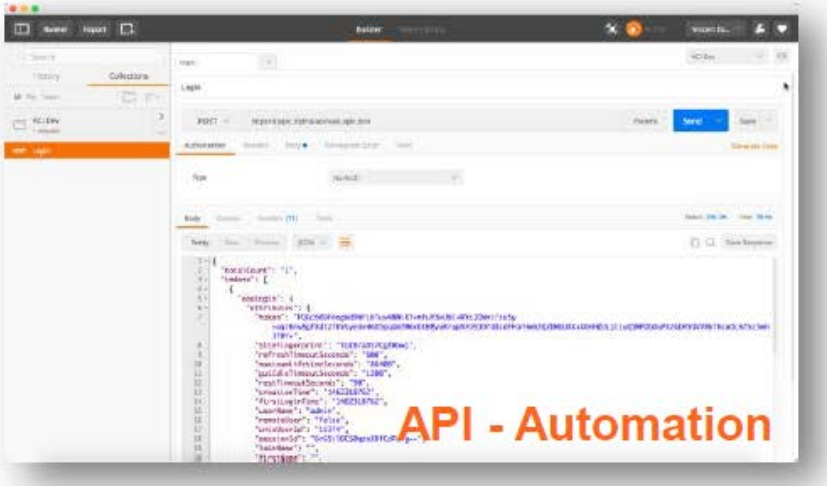
- **Единая точка управления сетью ЦОД на основе политик:**
  - Профили приложений
  - Политики безопасности
  - Инициализация фабрики
  - Управление конфигурациями
  - Управление ПО коммутаторов
  - Накопление и экспорт статистики/телеметрии
  - Мониторинг приложений
  - Поиск и устранение неисправностей
  - Открытая модель данных для управления при помощи внешних средств оркестрации
- **Не принимает непосредственное участие в передаче данных**
- **Единое управление наложенным транспортом и фабрикой**
- **Кластеризация для масштабирования и доступности (от 3 до 5 и более узлов)**



Разнообразие методов управления



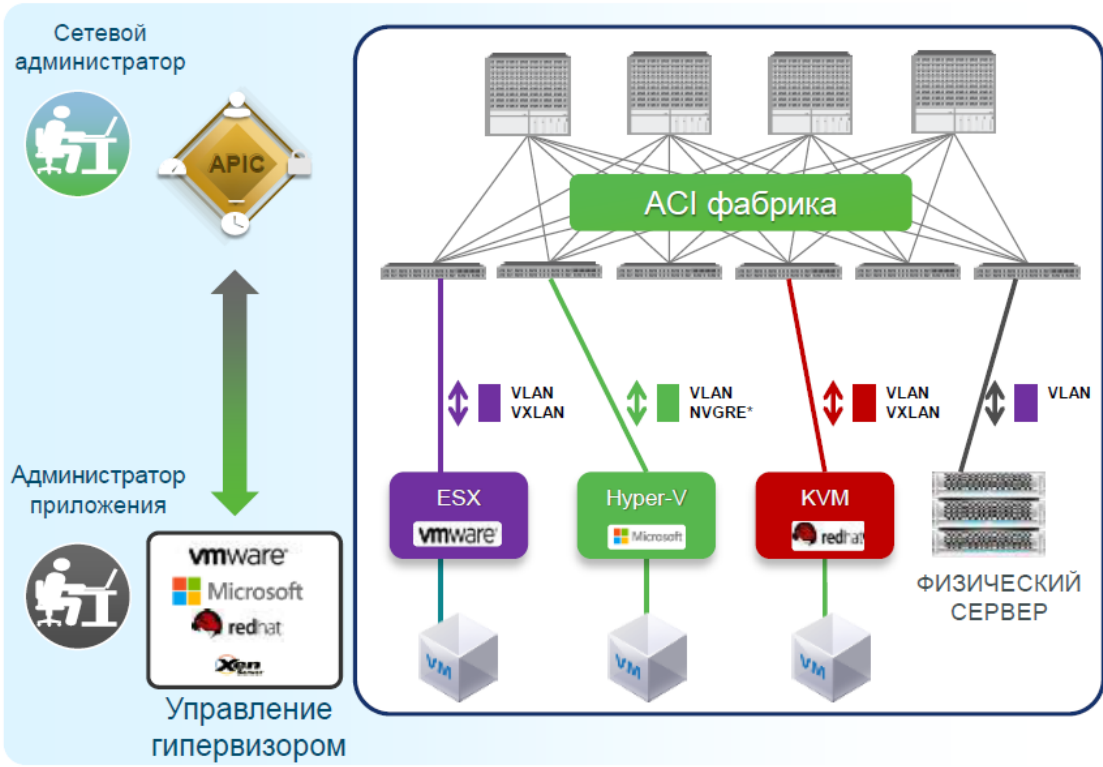




Фабрика с поддержкой нескольких гипервизоров

Интеграция с физическим и виртуальным миром

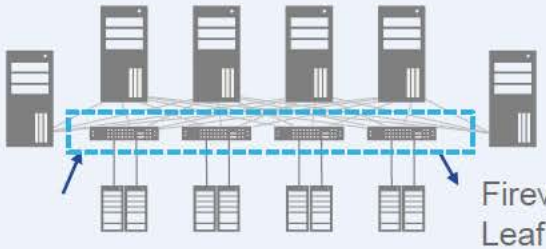
- Заказчик не ограничен в выборе платформы виртуализации: VMWare, Microsoft, KVM/OpenStack или невиртуализированных серверов
- Возможность использования нескольких VMM в одной группе EPG
- Интегрированный шлюз для VLAN и VxLAN сетей
- Не требуется дополнительное лицензирование
- Поддержка контейнеров – проект Contiv



Cisco ACI – разнообразие методов сегментации

Cisco ACI – варианты применения политик безопасности

L4 Stateless Security



Servers (Physical or Virtual)

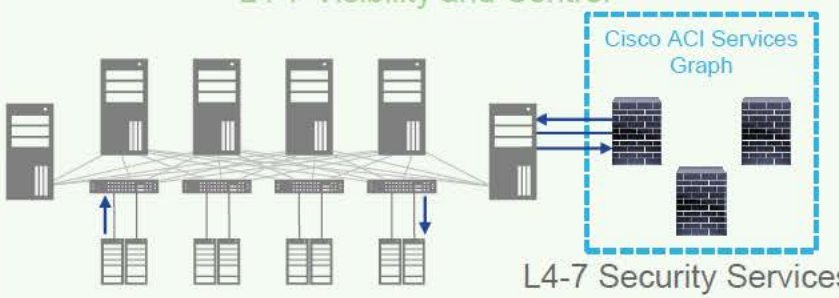
► L4 Distributed Stateless Firewall

L4 Stateless Firewall Attached to Every Server Port

Line Rate Policy Enforcement

Policy Follows Workloads

L4-7 Visibility and Control



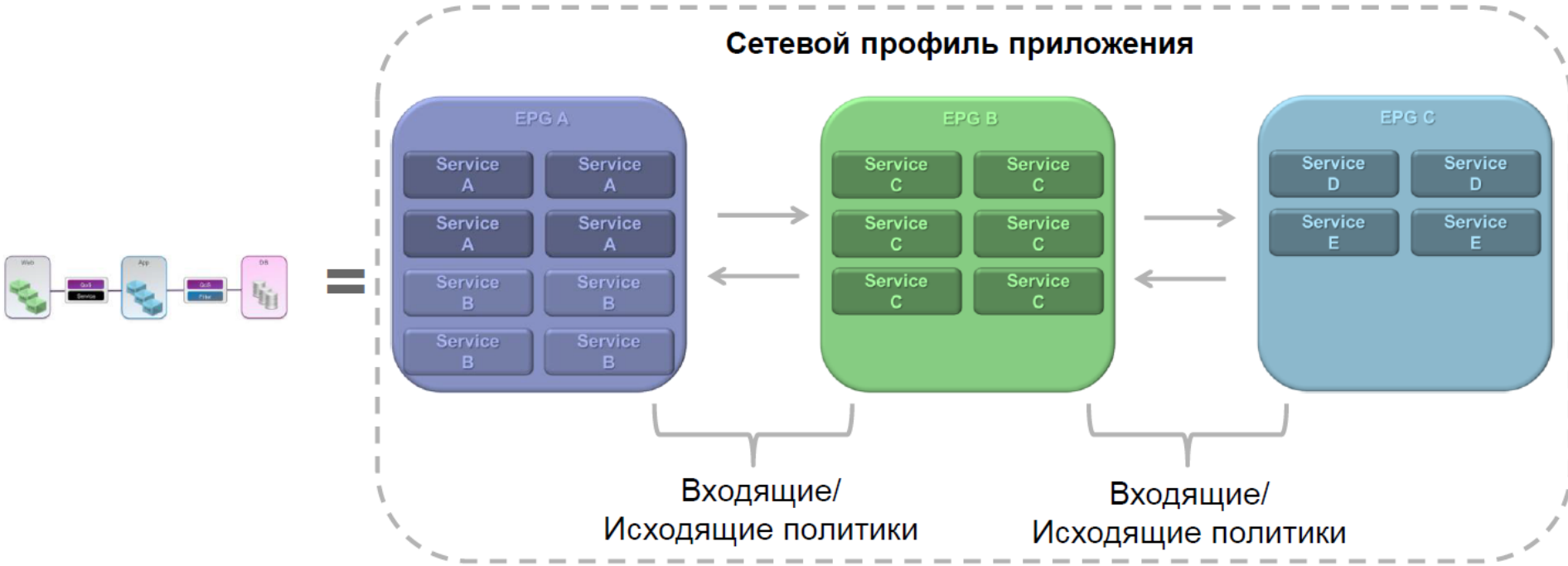
► L4–7 Security via Cisco ACI™ Service Graph

Advanced Protection with NGFW, IPS/IDS, DDoS Services Insertion

Sizing at Scale: Enabled via Pool and Cisco ACI Dynamic Redirection

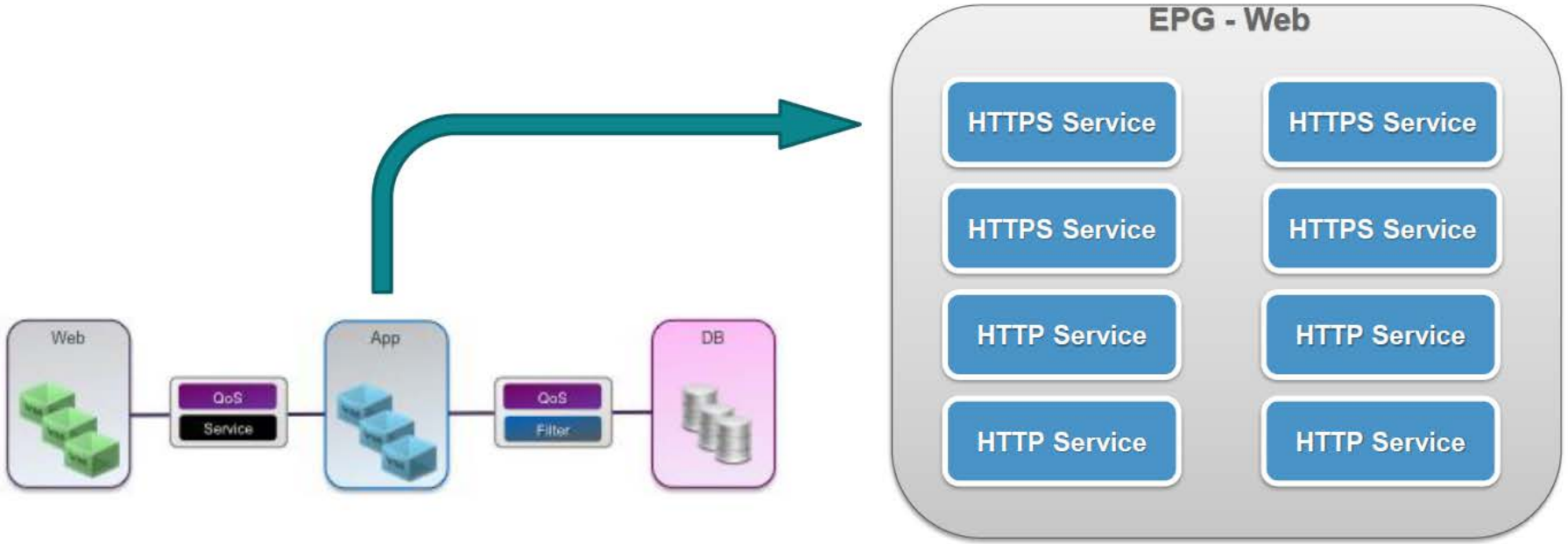
L4-7 Security Policy Applied Consistently for Any Workload

Сетевой профиль приложения Application Network Profile (ANP)



Сетевой профиль - логическое объединение групп EPG и политик, определяющих правила взаимодействия между EPG

Модель политик ACI End-Point Group (EPG)



EPG – логическая **группа конечных хостов** представляющих приложение целиком или компоненты приложения, (в общем случае) **не зависящая** от сетевых атрибутов

Модель политик ACI различные методы определения элементов EPG

Сервер

Виртуальные машины или контейнеры

СХД

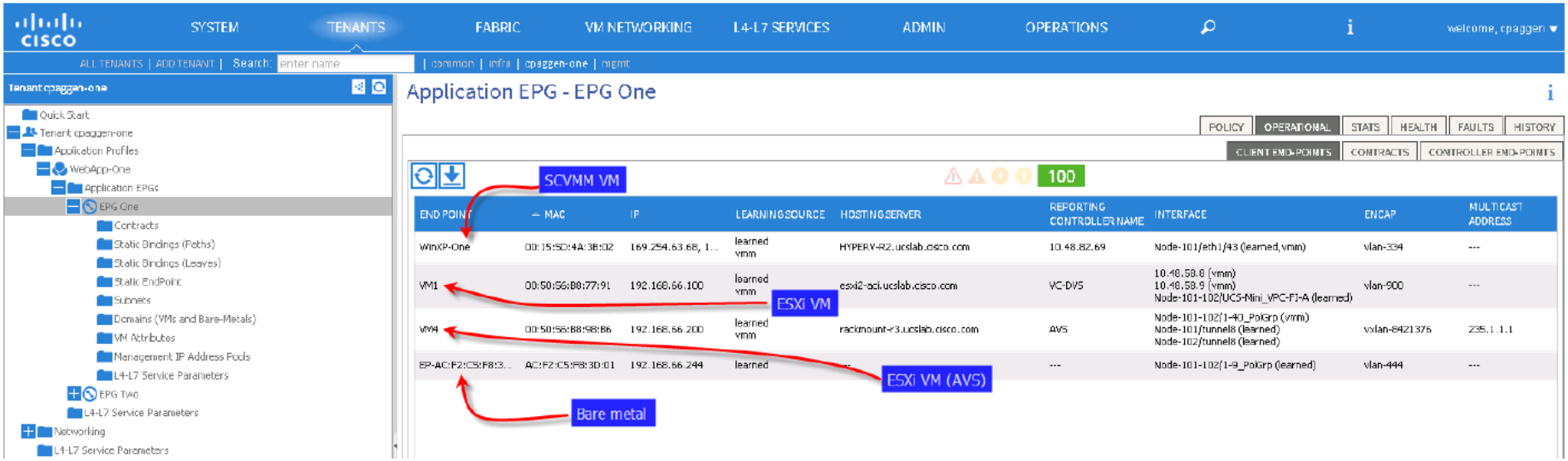
Клиенты

- Интерфейс, при помощи которого конечное устройство подключается к сети
- Имеет адрес (identity), местоположения, атрибуты (version, patch level)
- Может быть физическим или виртуальным

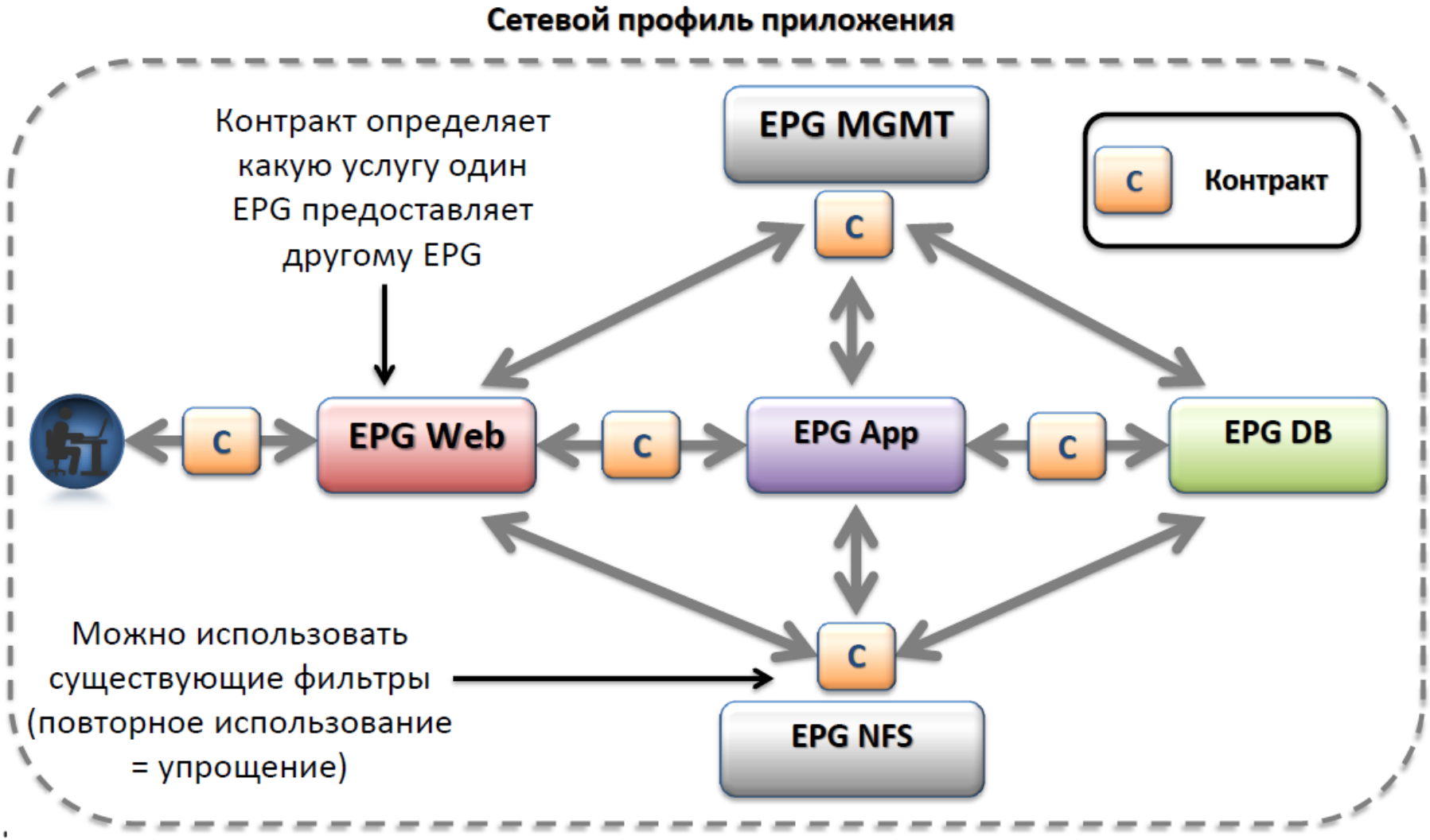
- Примеры критериев отнесения к EPG
  - Физический порт (на leaf или FEX)
  - Логический порт (VM port group)
  - VLAN ID
  - VXLAN (VNID)
  - Атрибуты виртуальных машин
  - IP адрес
  - IP подсеть (применительно ко внешним подключениям)

Нормализация инкапусуляции и универальные политики
Пример: 4 разных типа подключений в одной EPG

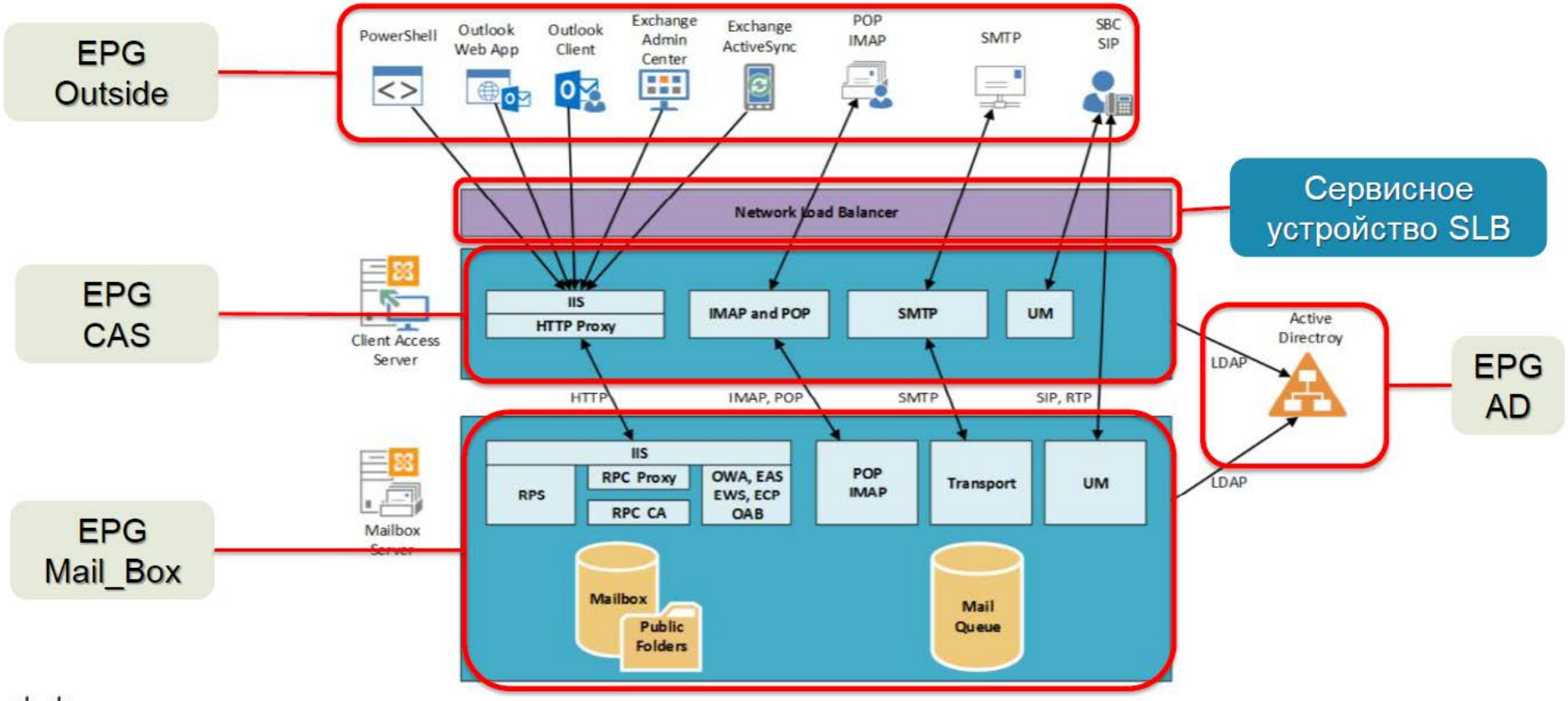
- ESX – распределенный коммутатор VMware (VLAN)
- ESX – коммутатор AVS от Cisco (VXLAN)
- Hyper-V – коммутатор от Microsoft (VLAN)
- Порт физического сервера (VLAN)



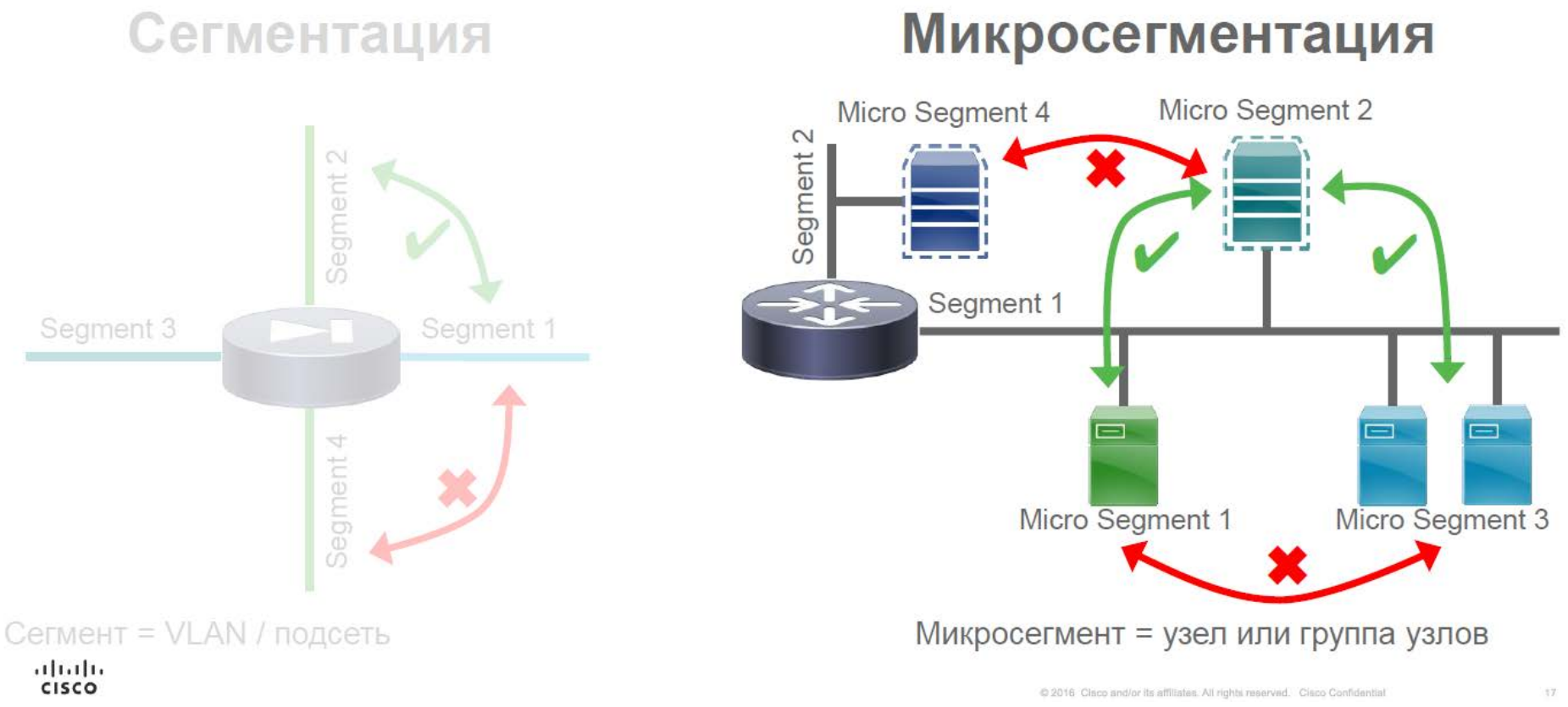
Контракты в сетевом профиле приложения Разрешённые виды взаимодействия



Внедрение традиционных приложений с Cisco ACI На примере Microsoft Exchange



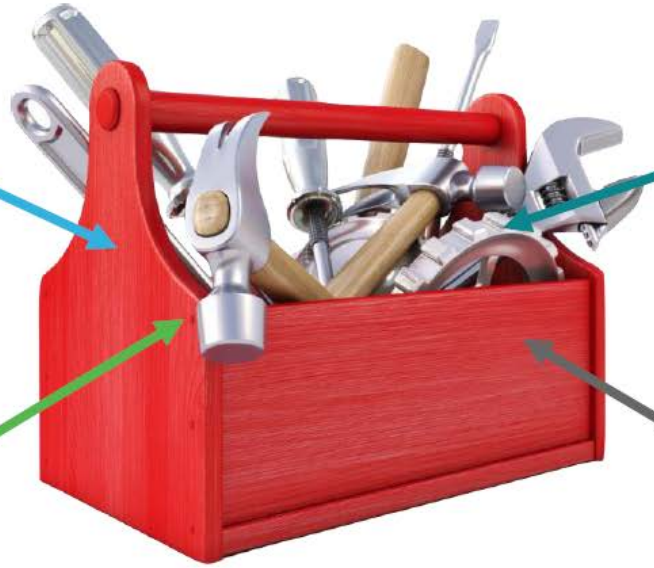
Микросегментация?



Инструментарий микросегментации Cisco ACI

EPG и контракты
Модель политик ACI

Изоляция внутри EPG

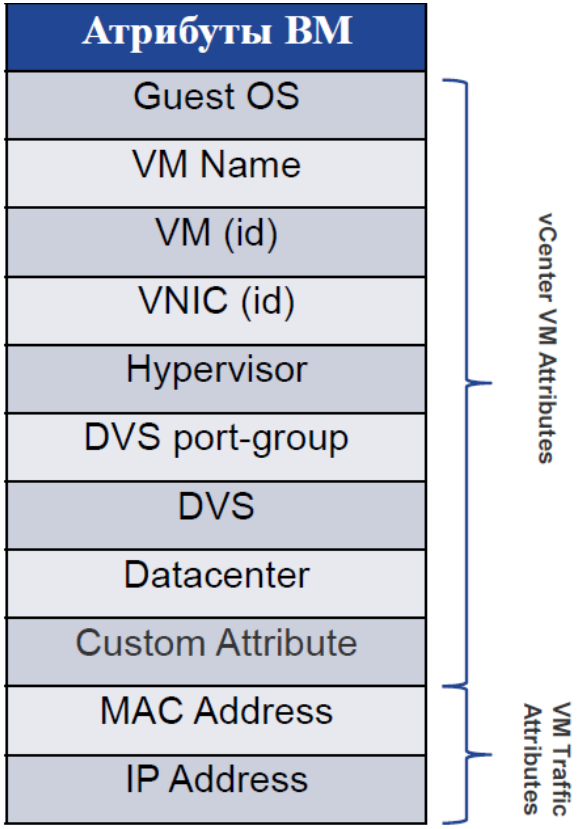


Микросегментация с использованием атрибутов

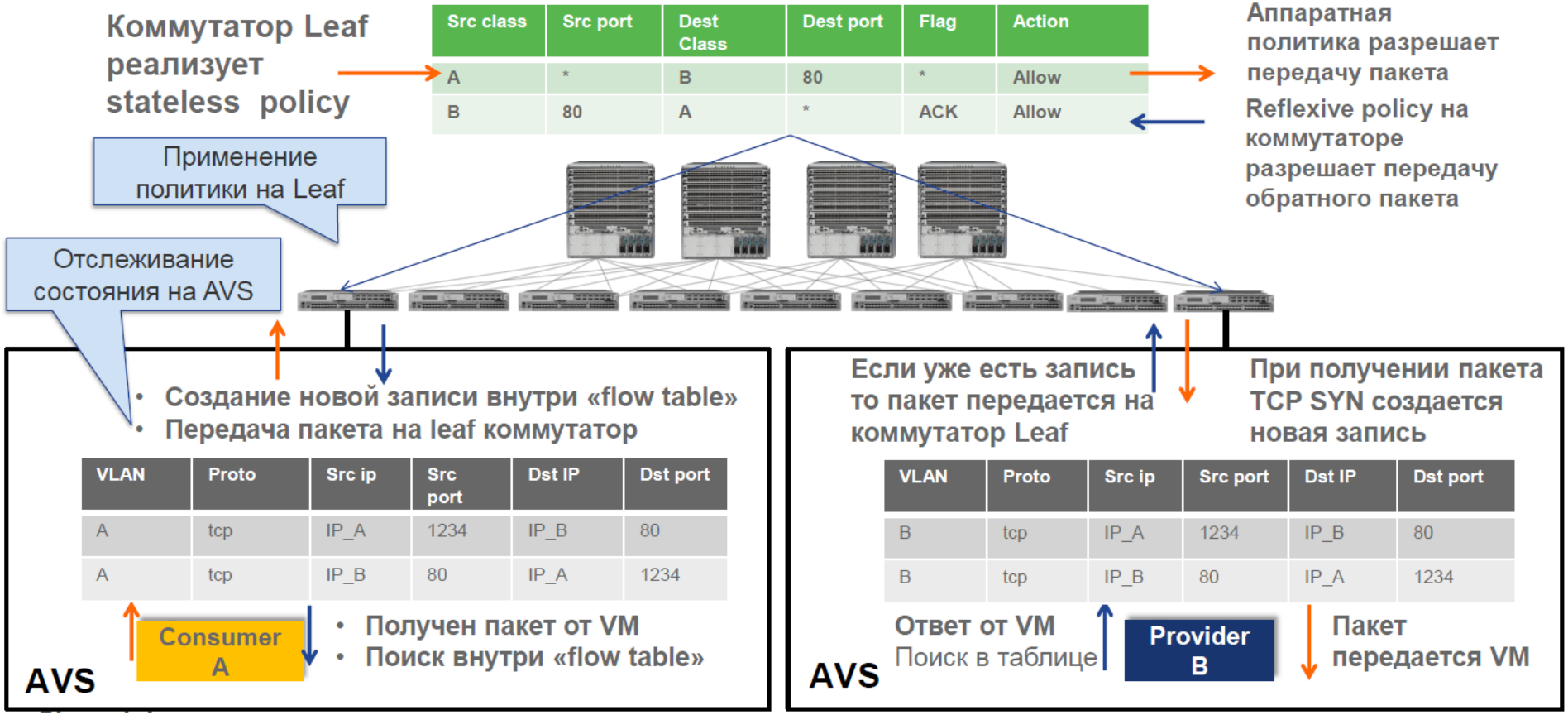
Интеграция с сервисами L4/L7

Микросегментация на базе ACI EPG классификация при помощи атрибутов VM

- End Point Group (EPG) могут использовать несколько методов для классификации
- VM Port Group – это самый простой механизм классификации ВМ
- Атрибуты сервера/VM также могут использоваться для классификации EPG
- Могут дополняться изоляцией трафика внутри EPG
- Поддержка микросегментации:
  - VMWare vSphere с виртуальными коммутаторами Cisco AVS или VMware vDS (с коммутаторами 9300-EX)
  - Microsoft Hyper-V
  - Невиртуализированные хосты (для сетевых атрибутов)
  - Openstack (планируется)

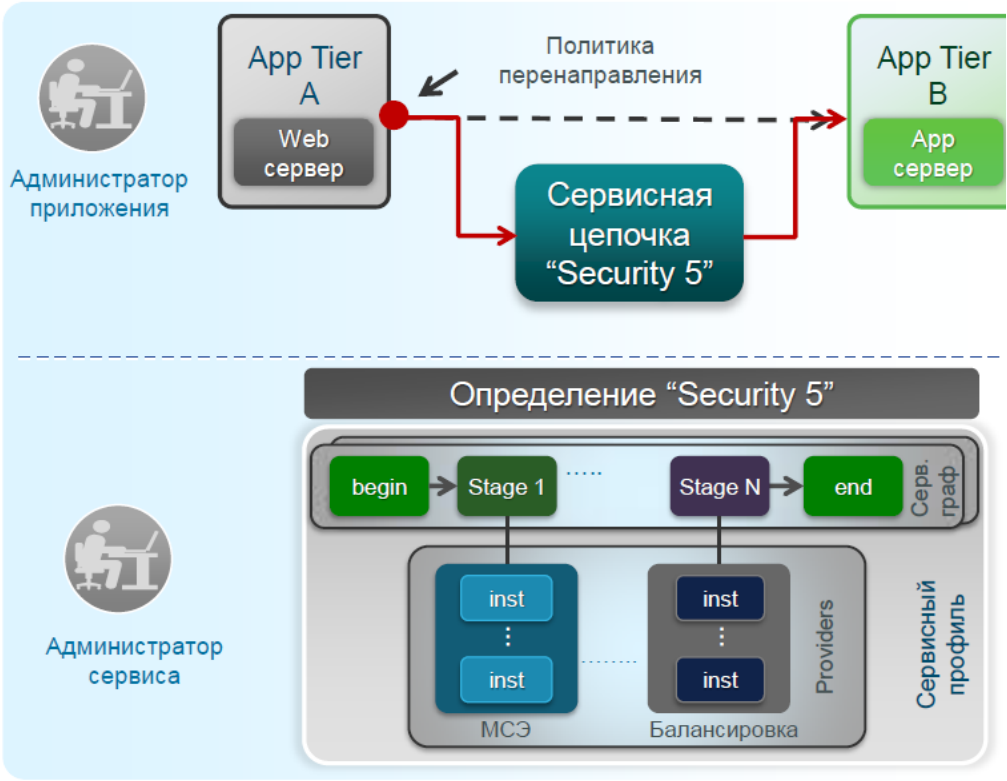


«Распределенный межсетевой экран» на базе ACI

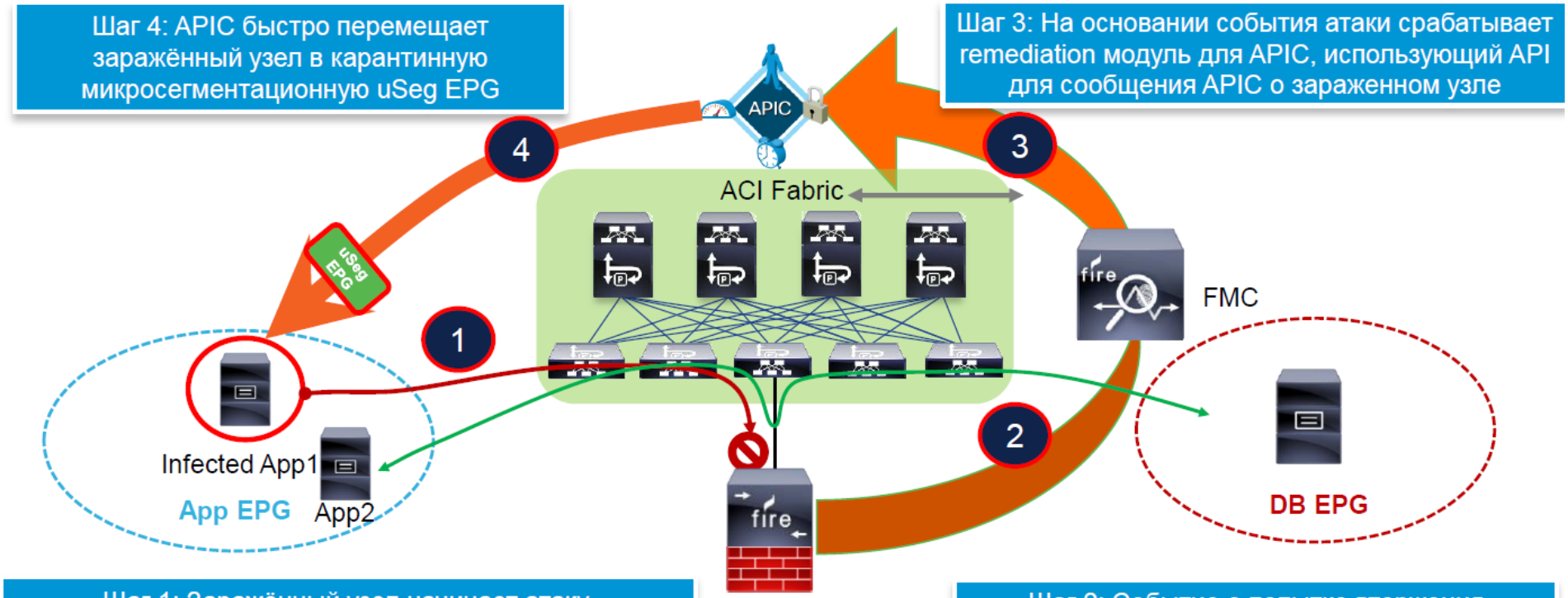


ACI: интеграция с сервисами 4 - 7 уровня

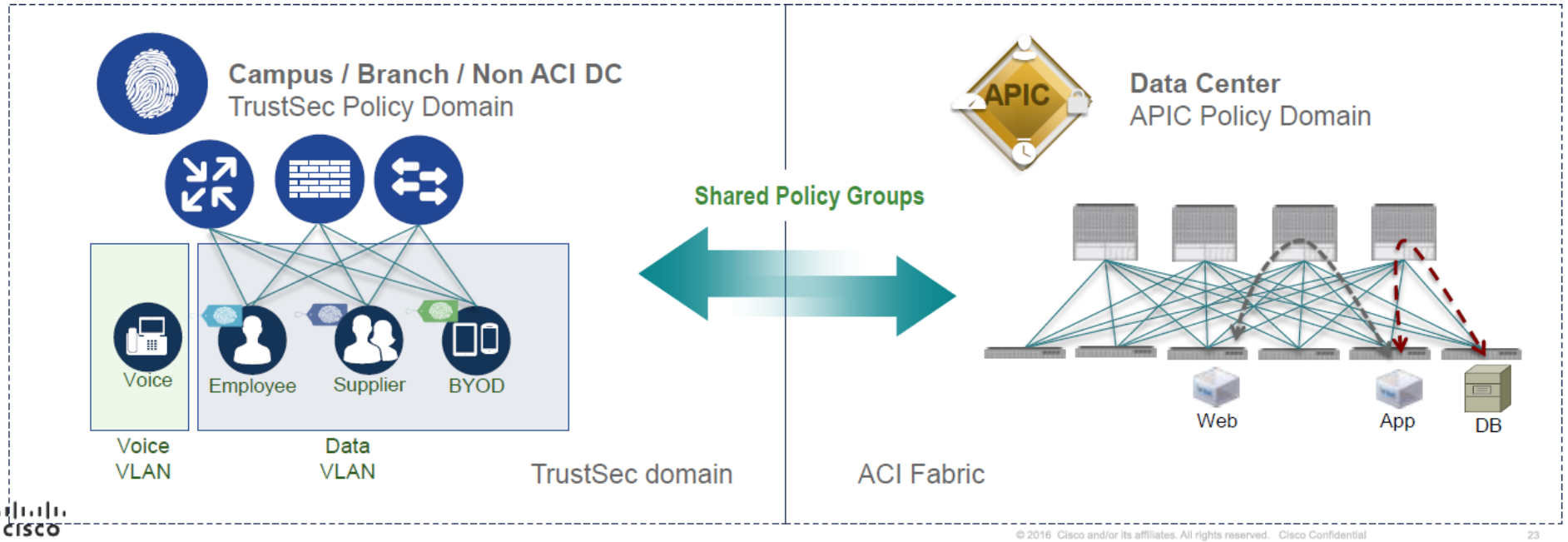
- Автоматизация вставки и настройки сервисов
- APIC – центральная точка контроля сети и согласования политик
- Безопасность (FW/IPS/…) и балансировка нагрузки
- От Cisco или от других компаний (включая российские)
- Физические или виртуальные сервисы
- Одиночные сервисы или цепочки
- Применение сервиса вне зависимости от места нахождения приложения
- Уведомление сервисов о подключенных узлах в EPG
- Помощь в административном разделении между уровнями приложения и сервиса



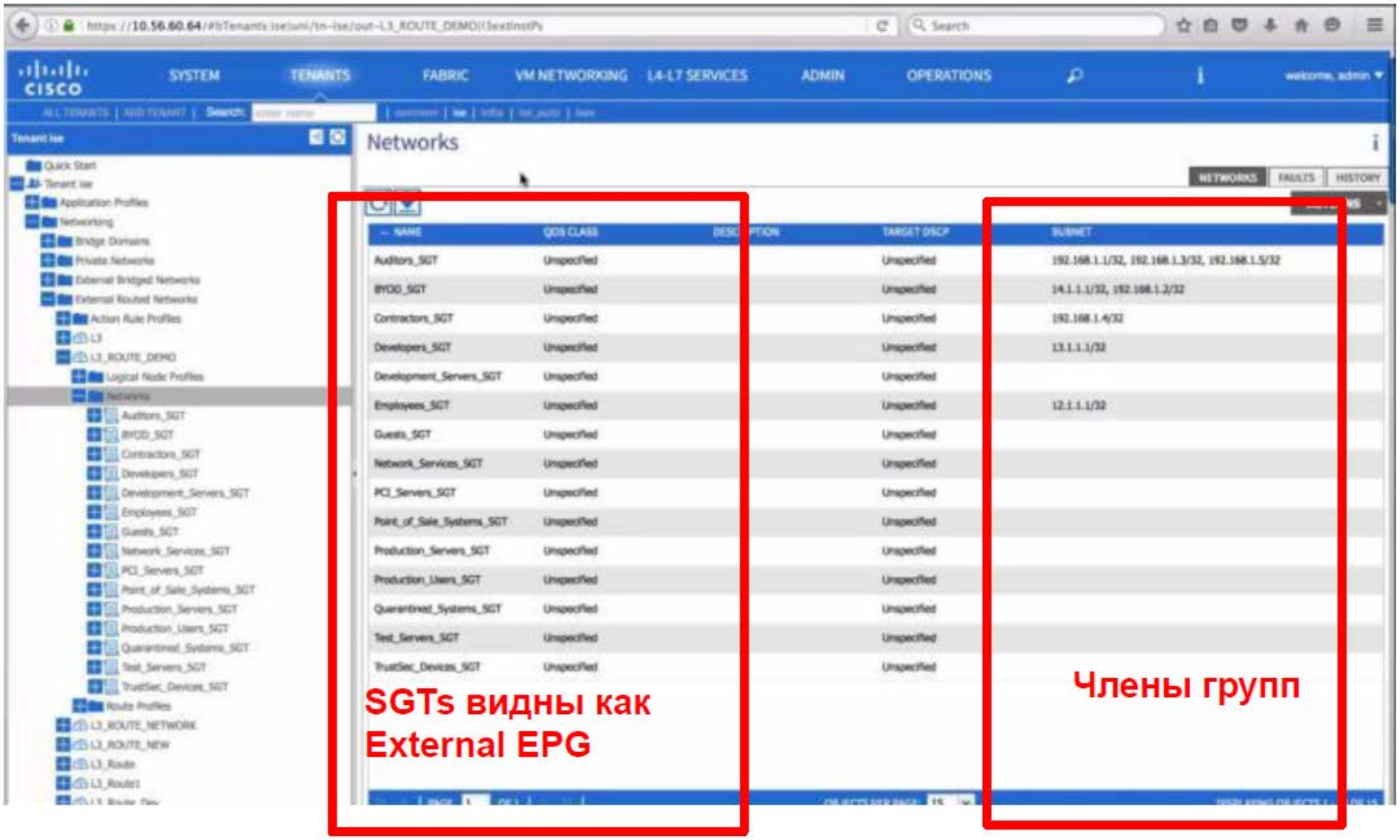
FMC to APIC Rapid Threat Containment FMC Remediation Module для APIC DB



Внедрение сквозных групповых политик в масштабах организации

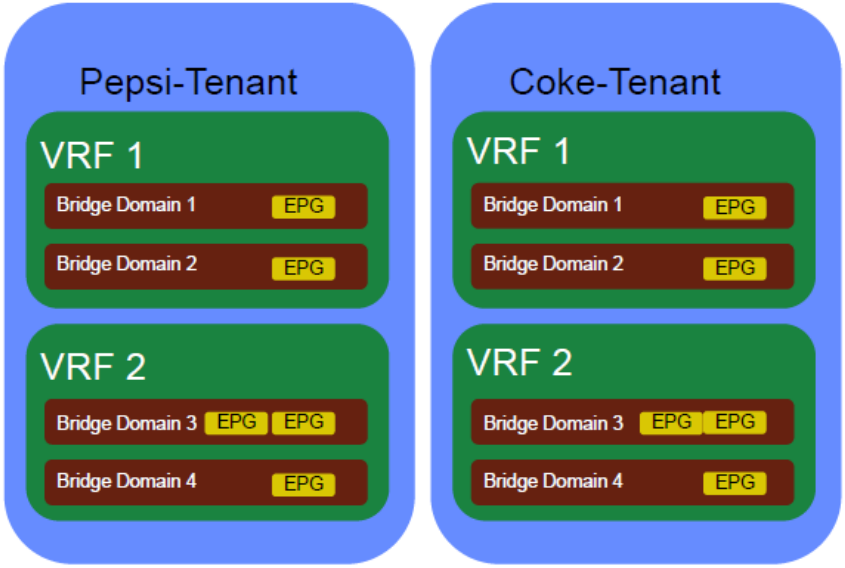


Группы TrustSec и членство в них - представление в ACI



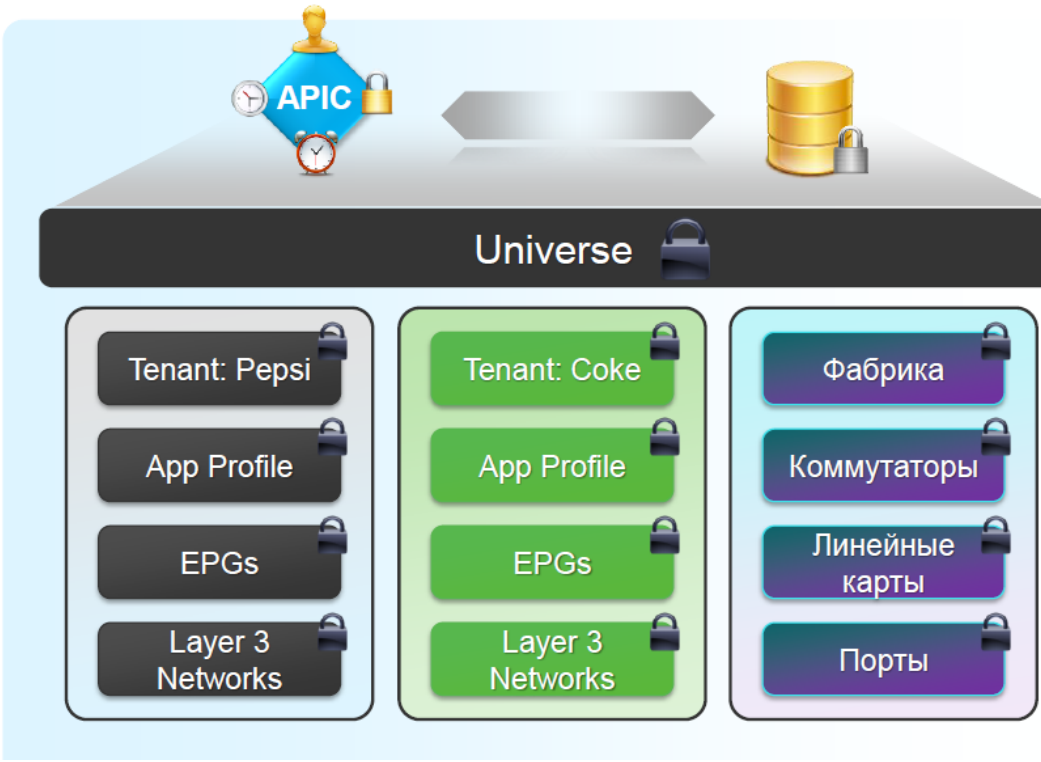
Изоляция контекстов/организаций «Тенанты»

- **Логические контейнеры с наборов изолированных ресурсов – приложений, сетевых элементов, политик, сбора и экспорта статистики и т.д.**
- **Управление доступом администраторов**
- **Возможность контролируемого взаимодействия между тенантами и совместного доступа к разделяемым ресурсам**
- **Сценарии использования**
  - Разные заказчики оператора
  - Среды разработки/тестирования/продуктива
  - Слияние/разделение организаций
  - Резервирование многих ЦОД



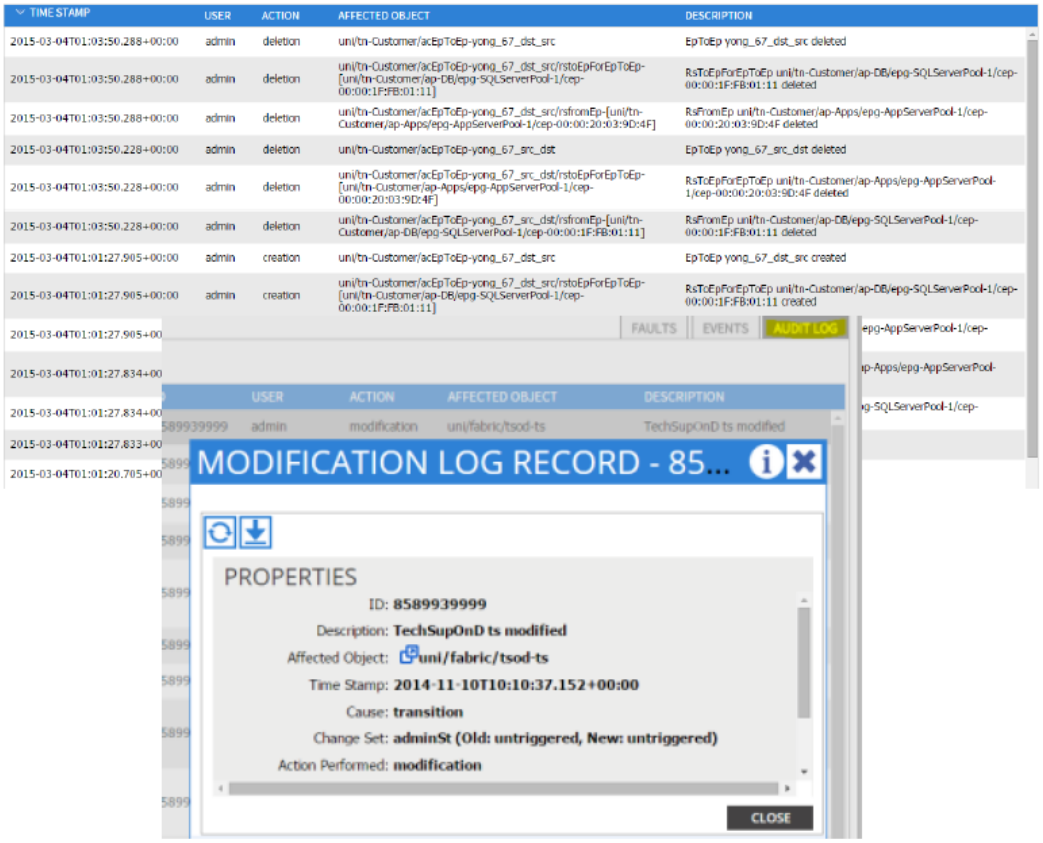
ACI фабрика – безопасность управления Аутентификация, Авторизация, RBAC

- Доступ ко всем объектам управления после аутентификации и по защищенному каналу
- Каждый объект имеет уникальный набор RBAC атрибутов на ЧТЕНИЕ и ЗАПИСЬ
- APIC и фабрика спроектированы изначально с поддержкой multi-tenancy
- Локальный и внешний сервис AAA (TACACS+, RADIUS, LDAP) для авторизации и аутентификации
- Аудит всех действий администраторов - на уровне любого объекта или фабрики в целом



Аудит действий администраторов

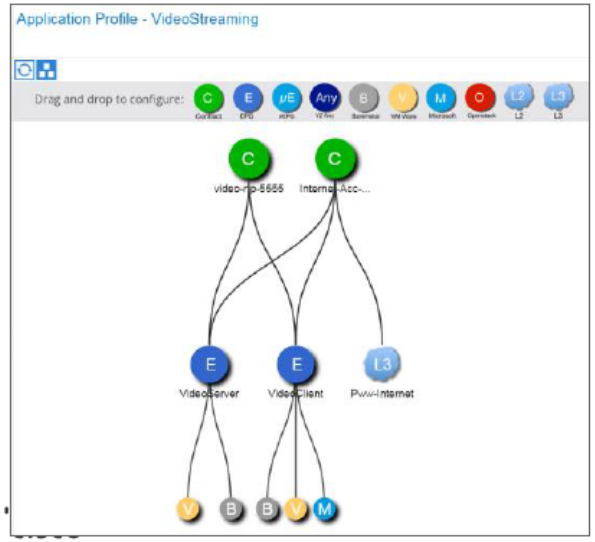
- **Все действия администратора фиксируются**
  - На уровне системы в целом
  - На любом уровне иерархии (логическом/физическом)
  - Независимо от пути выполения (GUI/CLI/API)
- **Разные виды доступа к журналу действий**
  - Через GUI – для задач устранения проблем
  - Через API – для аналитики и контроля соответствия требованиям
  - Экспорт событий на внешние серверы

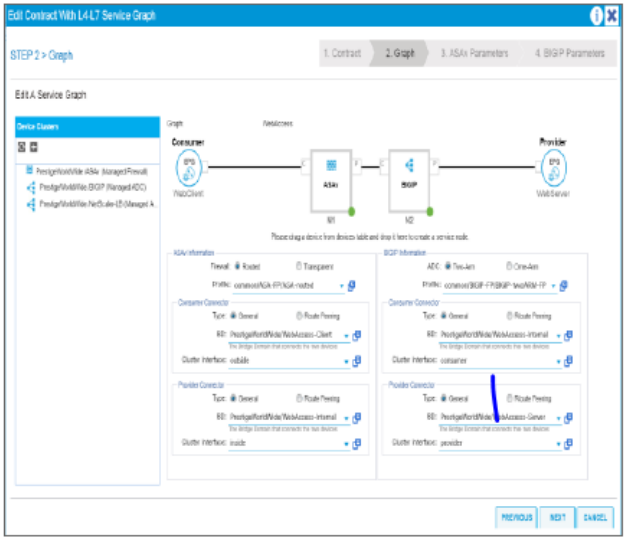


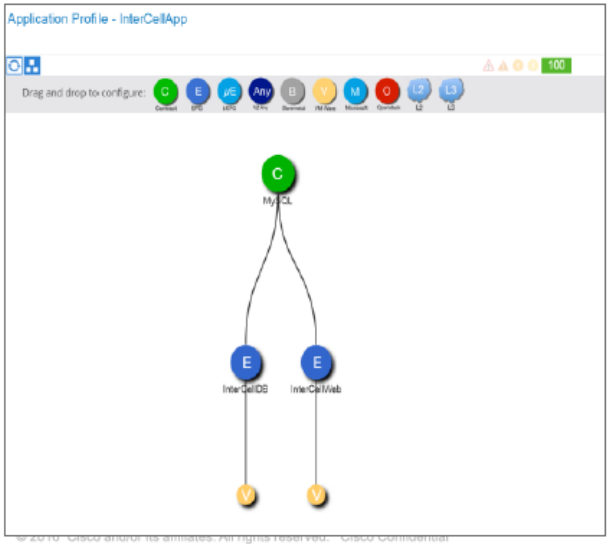
Автоматический отчёт о политиках безопасности

No	Tenant	VRF	BD	Application	Consumer EPG/Endpoints	Provider EPG/Endpoints	Contract	Filter Protocol	Filter Source Ports	Filter Destination Ports	Service Graph ID	Service Node	Service Node	Permit Hits	Deny Hits
1	Cisco	IT	IT	VideoStreaming	VideoClient/90	VideoServer/5	Video	UDP	*	5555	1 (managed)	ASAv	IPS	234,934	122,344
2	WorldCom	Test	Test	WebAccess	WebClient/50	WebServer/4	WebAccess	TCP	*	https http	1 (managed)	ASAv	F5-BigIQ	554,934	326,093
3	InterCom	Sim	Sim	InterCellApp	Web/1,000	DB/200	App	TCP	*	300-10,000	1 (managed)	ASAv	F5-BigIQ	320,192	290,392
								TCP	*	ICMP	1 (managed)	ASAv	F5-BigIQ	123,456	12,456

ACI Security Policy Translated to a Security Compliance Report

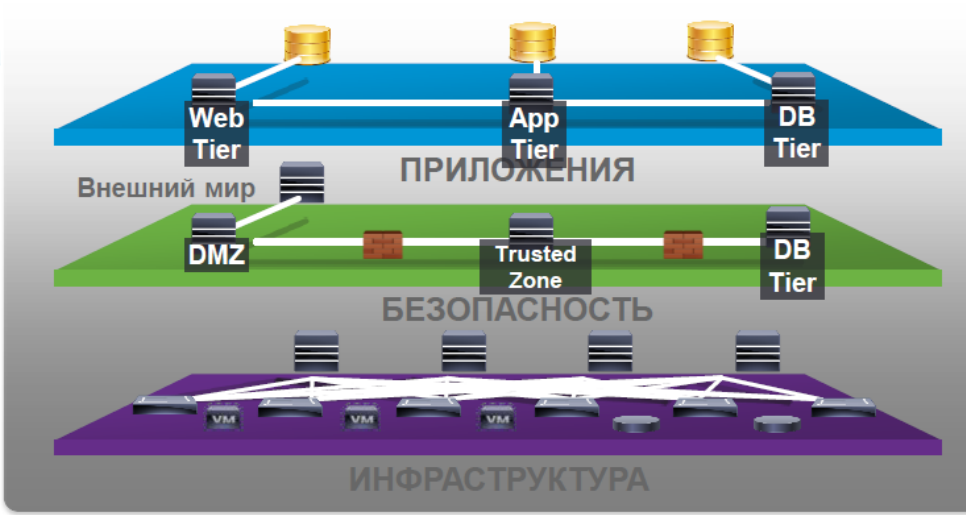






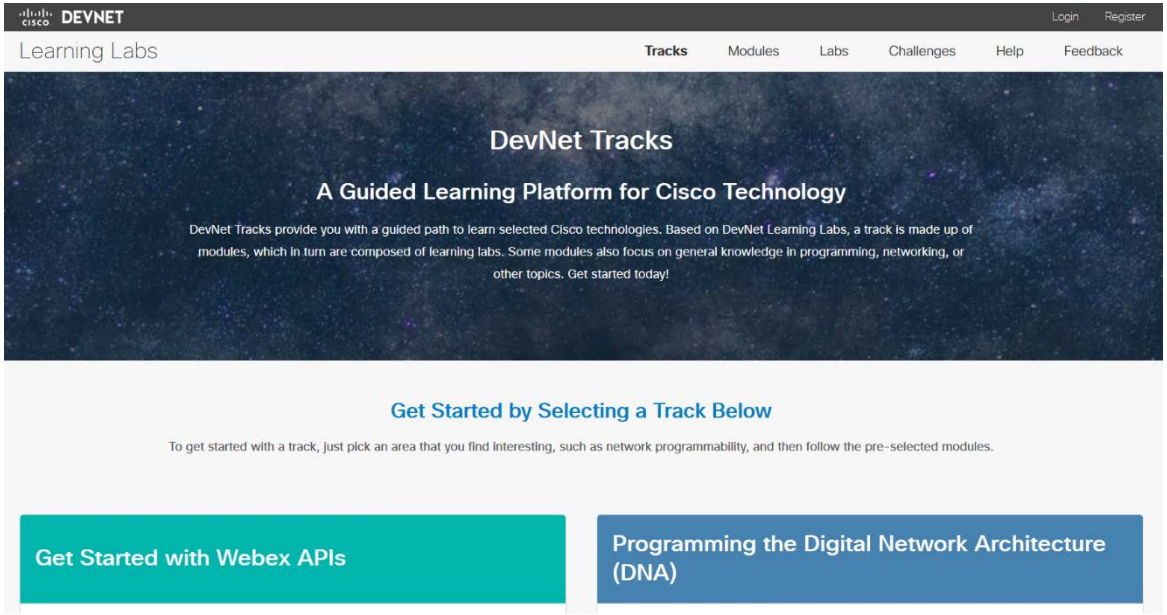
Application Centric Infrastructure … для администраторов безопасности

- **Управление правилами доступа**
  - Единая точка контроля политик взаимодействия
  - Структура правил/контрактов увязана с сервисами, а не с адресами
  - Нет «накопления» неиспользуемых правил МСЭ
- **Модель «белого списка»**
  - Всё, что не разрешено, по умолчанию запрещено
- **«Распределённый МСЭ»**
  - Микросегментация и контроль сессий
- **Встраивание средств безопасности**
  - Физические или виртуальные
  - Cisco или другие разработчики
- **Полная изоляция организаций (tenants)**
- **Интегрированные возможности аудита**
  - Протоколирований действий администраторов
  - API для внешнего анализа соответствия политикам
- **Безопасность управления ACI**
  - Контроль доступа и ролевое управление



Спасибо за внимание!

https://cisco.com
https://ciscoclub.ru
https://ciscolive.cisco.com/
https://vk.com/cisco
http://blogs.cisco.com/
https://learninglabs.cisco.com/
https://dcloud.cisco.com/



dCloud