

**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&СТСРА 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

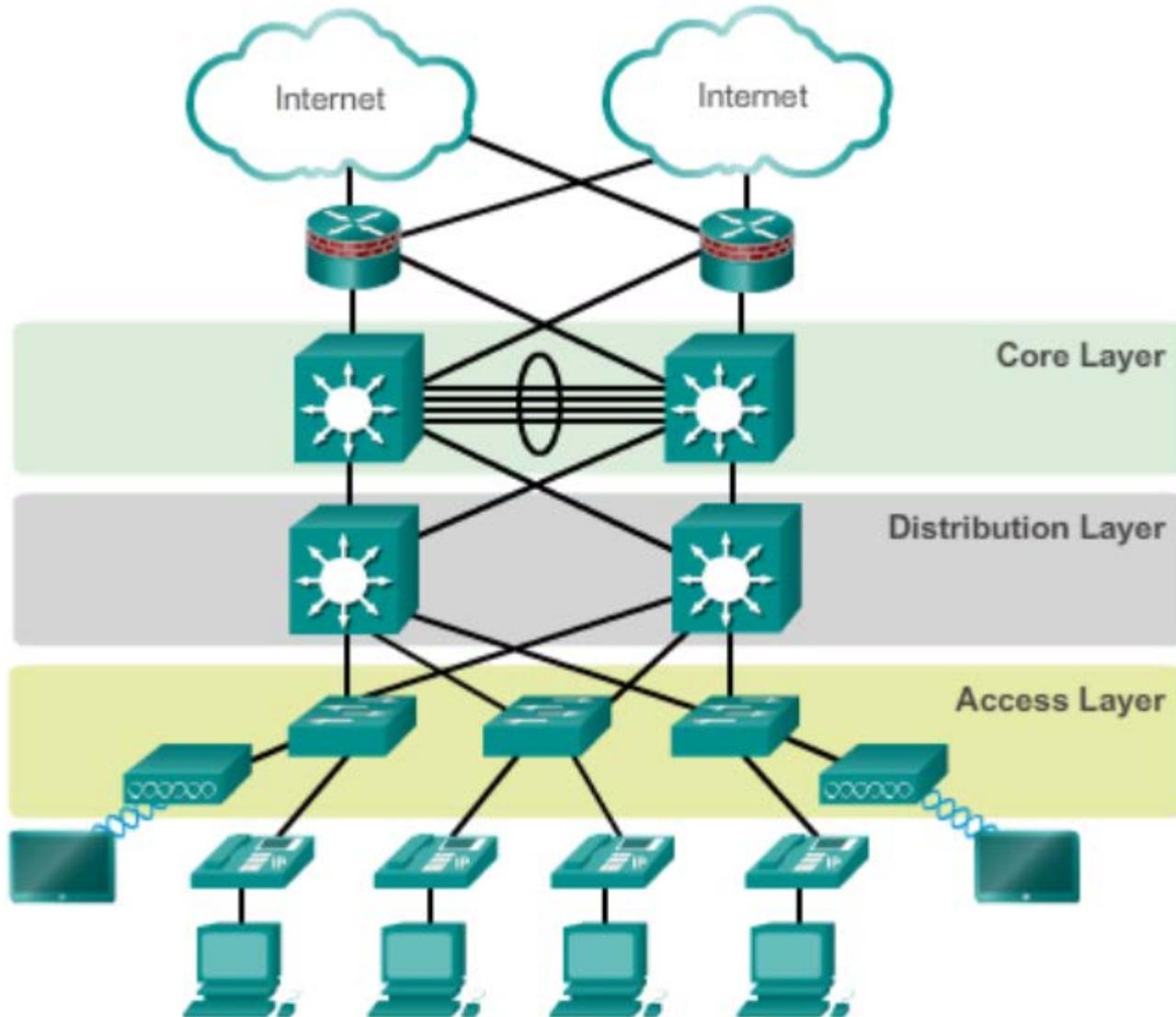


Физические серверы, виртуальные
машины и контейнеры

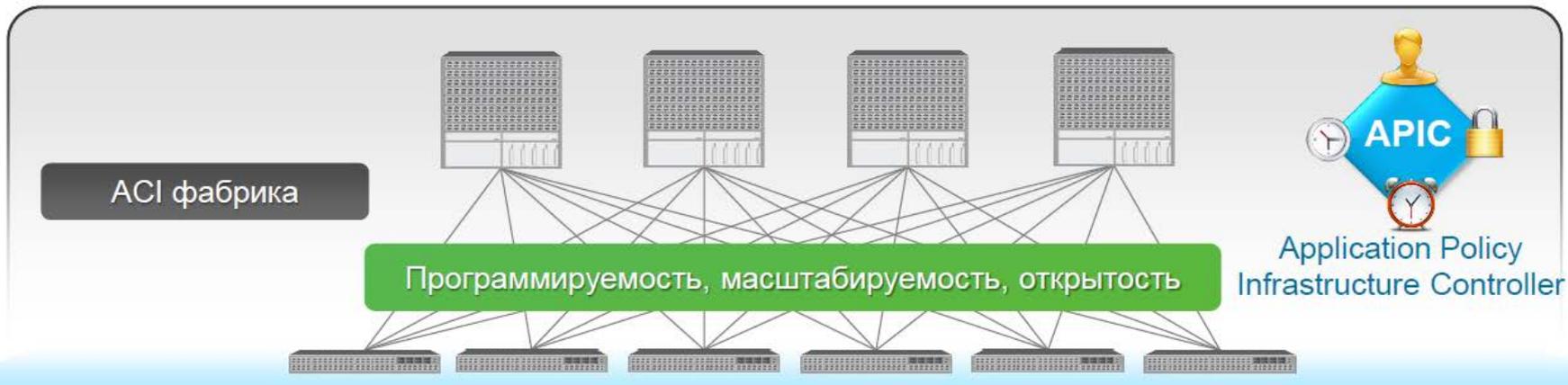
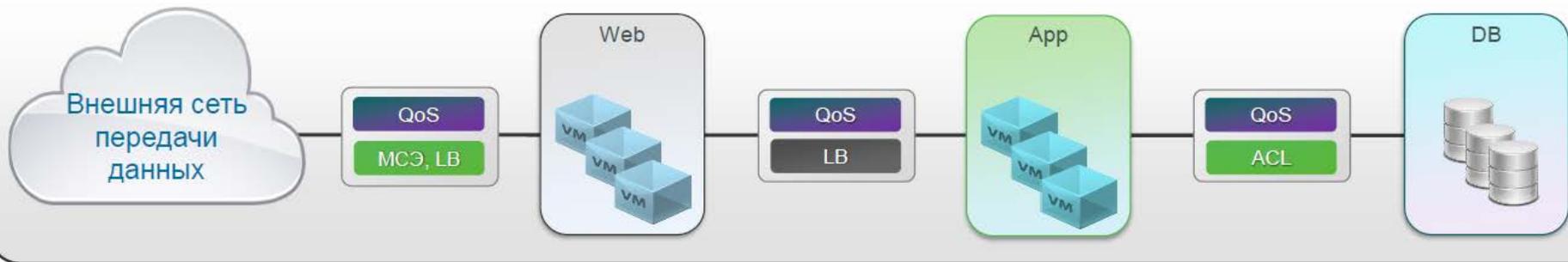


Автоматизация на основе политик

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

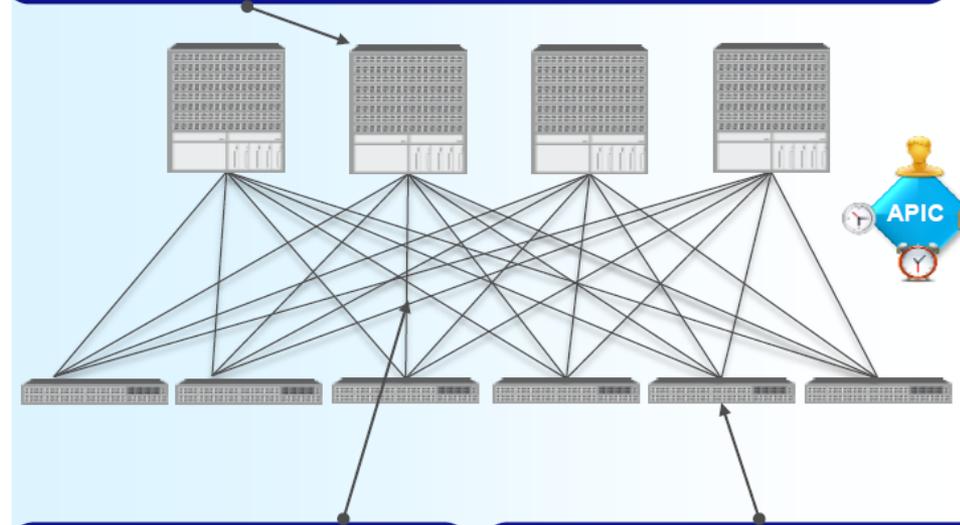


Spine: модульные (Nexus 9500) или фиксированные (9336)

Аппаратная база отображения адресов

До 576 x 40/100 G портов на устройство

Высокая плотность за умеренную стоимость



Оптимизация фабрики

Оптимальная балансировка ECMP

Быстрая сходимость

Атомарные счётчики

Leaf (доступ): Nexus 9300

Применение политик

Интеллектуальное кеширование

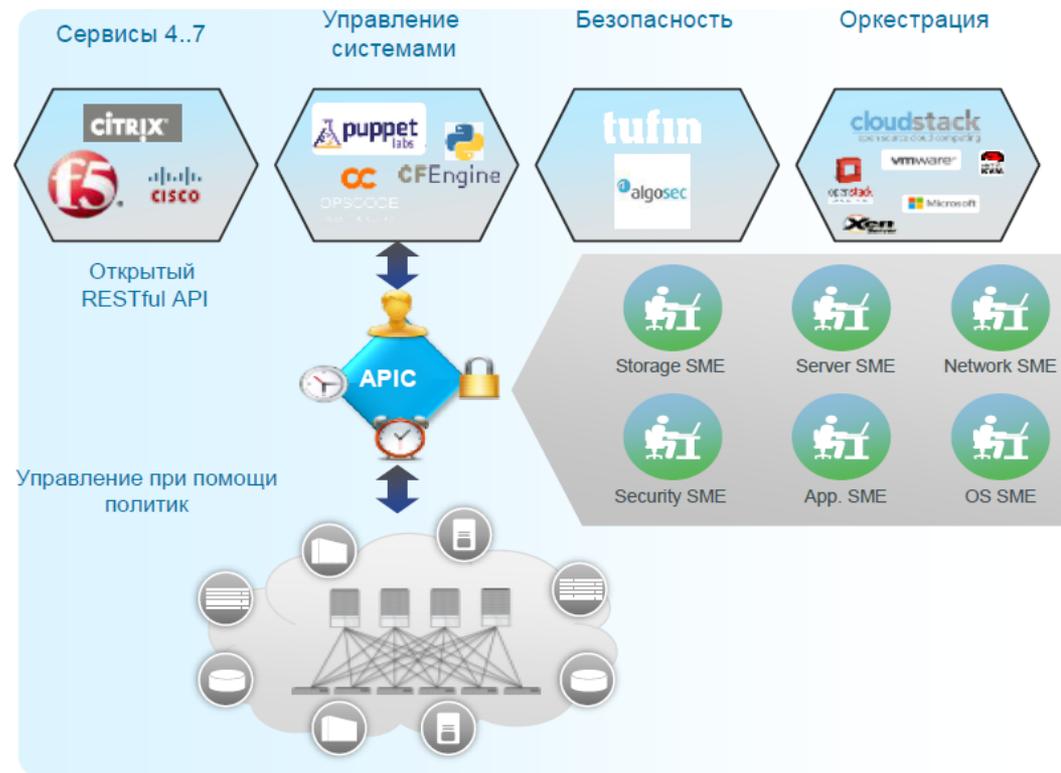
Поддержка терминции оверлеев

Улучшенная аналитика

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)**

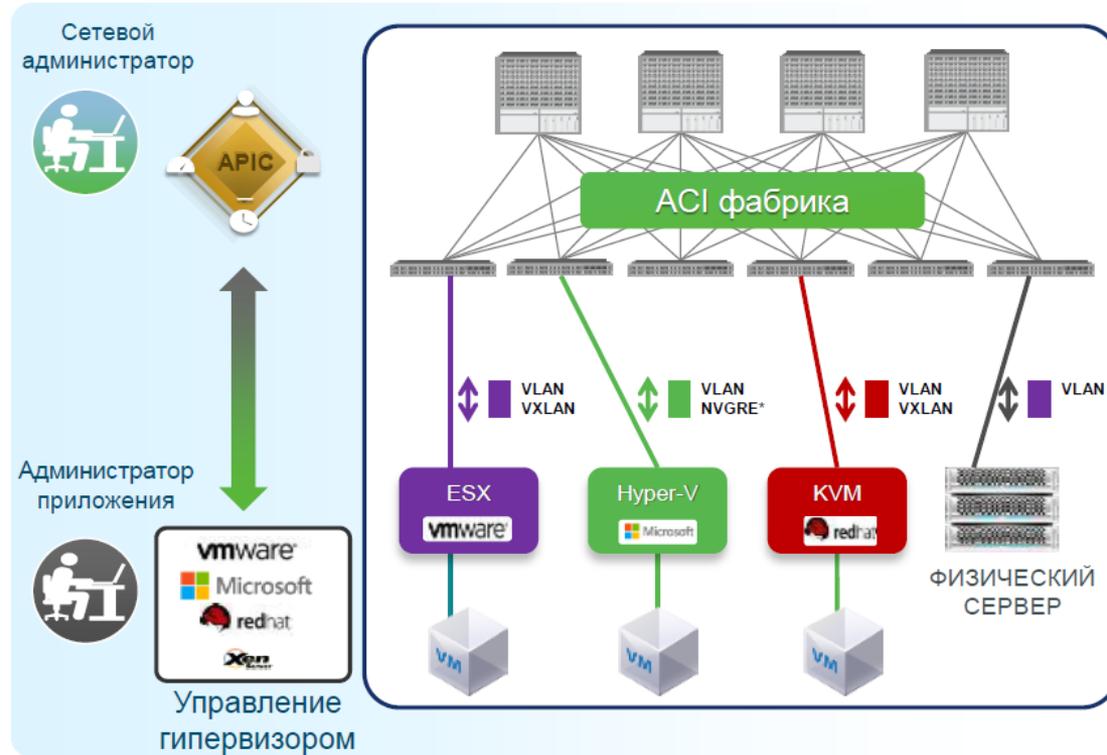


Фабрика с поддержкой нескольких гипервизоров

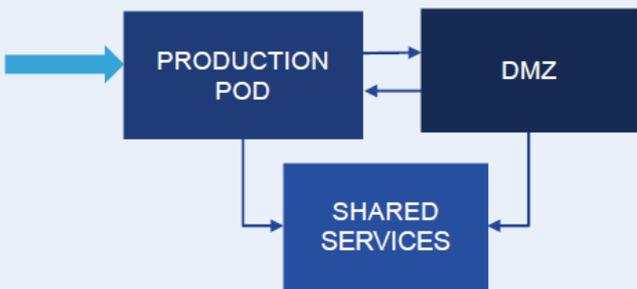
Интеграция с физическим и виртуальным миром



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



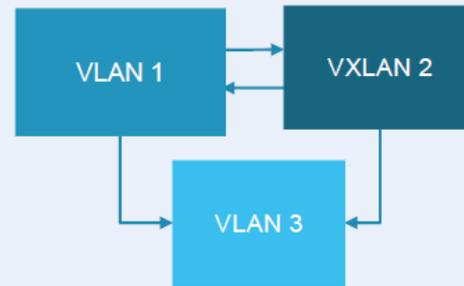
Cisco ACI – разнообразие методов сегментации



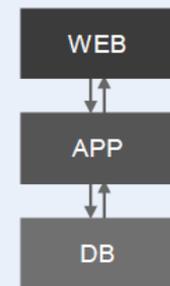
Сегментация контуров ЦОД



Сегментация жизненного цикла приложения



«Сетецентричная» сегментация на основе VLAN



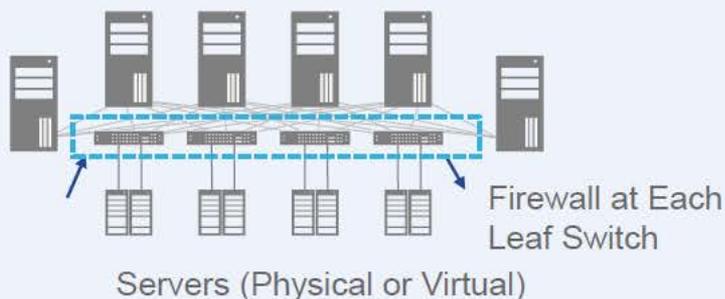
Сегментация на основе структуры приложения
Микросегментация



Уровень сегментации/изоляции/контроля

Cisco ACI – варианты применения политик безопасности

L4 Stateless Security



▶ L4 Distributed Stateless Firewall

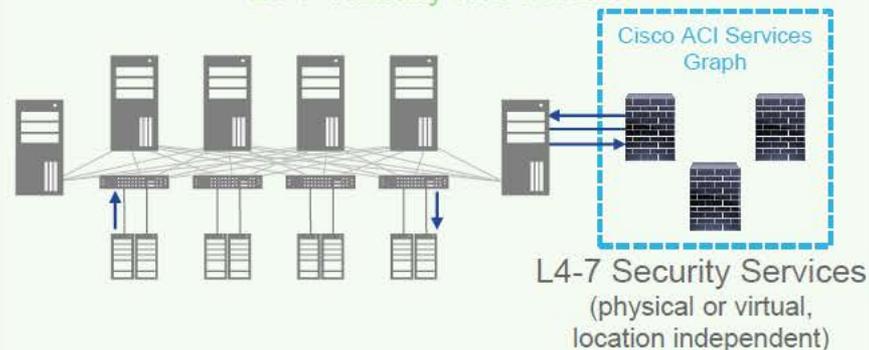
L4 Stateless Firewall Attached to Every Server Port

Line Rate Policy Enforcement

Policy Follows Workloads

CISCO

L4-7 Visibility and Control



▶ L4-7 Security via Cisco ACI™ Service Graph

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

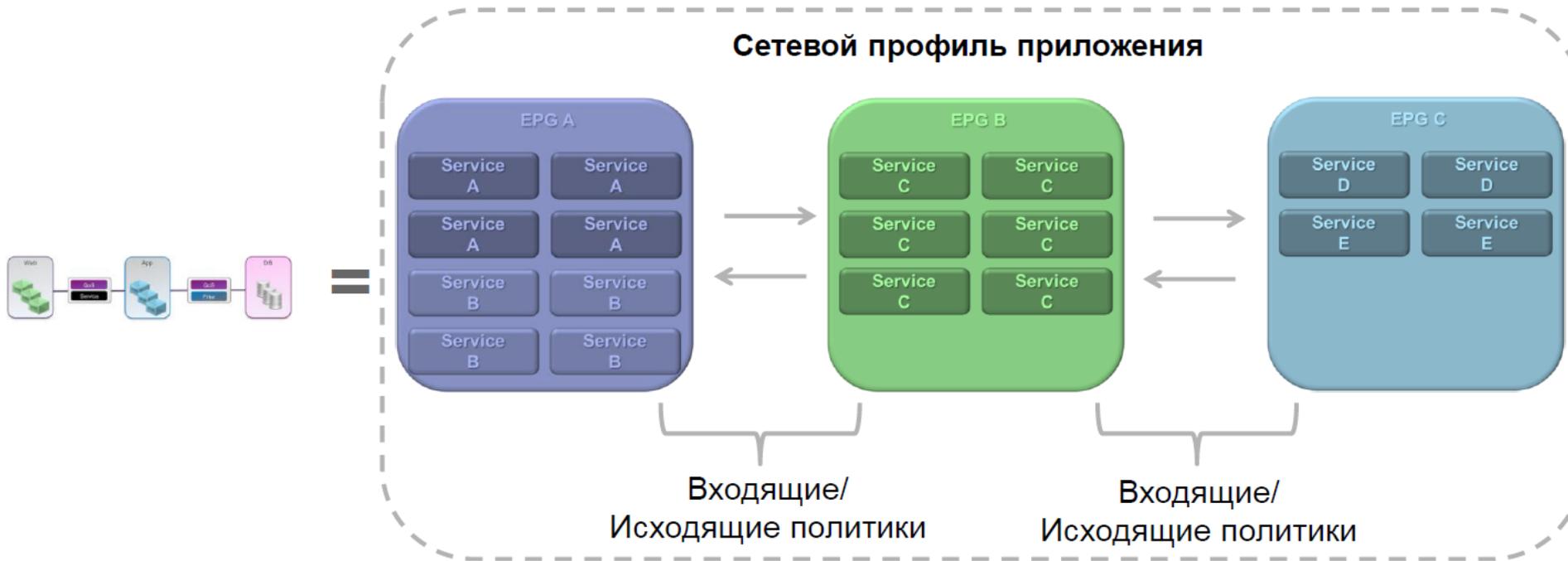
Sizing at Scale: Enabled via Pool and Cisco ACI Dynamic Redirection

L4-7 Security Policy Applied Consistently for Any Workload

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

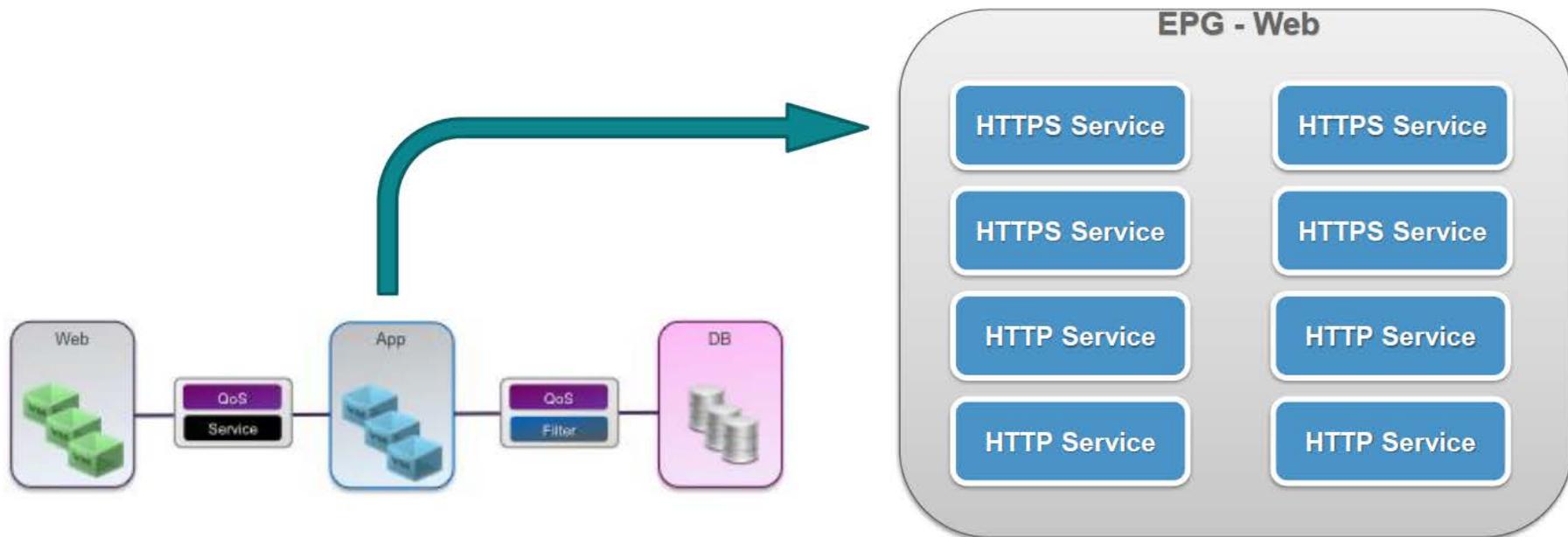
10

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 инкапсуляции и универсальные политики

Пример: 4 разных типа подключений в одной EPG

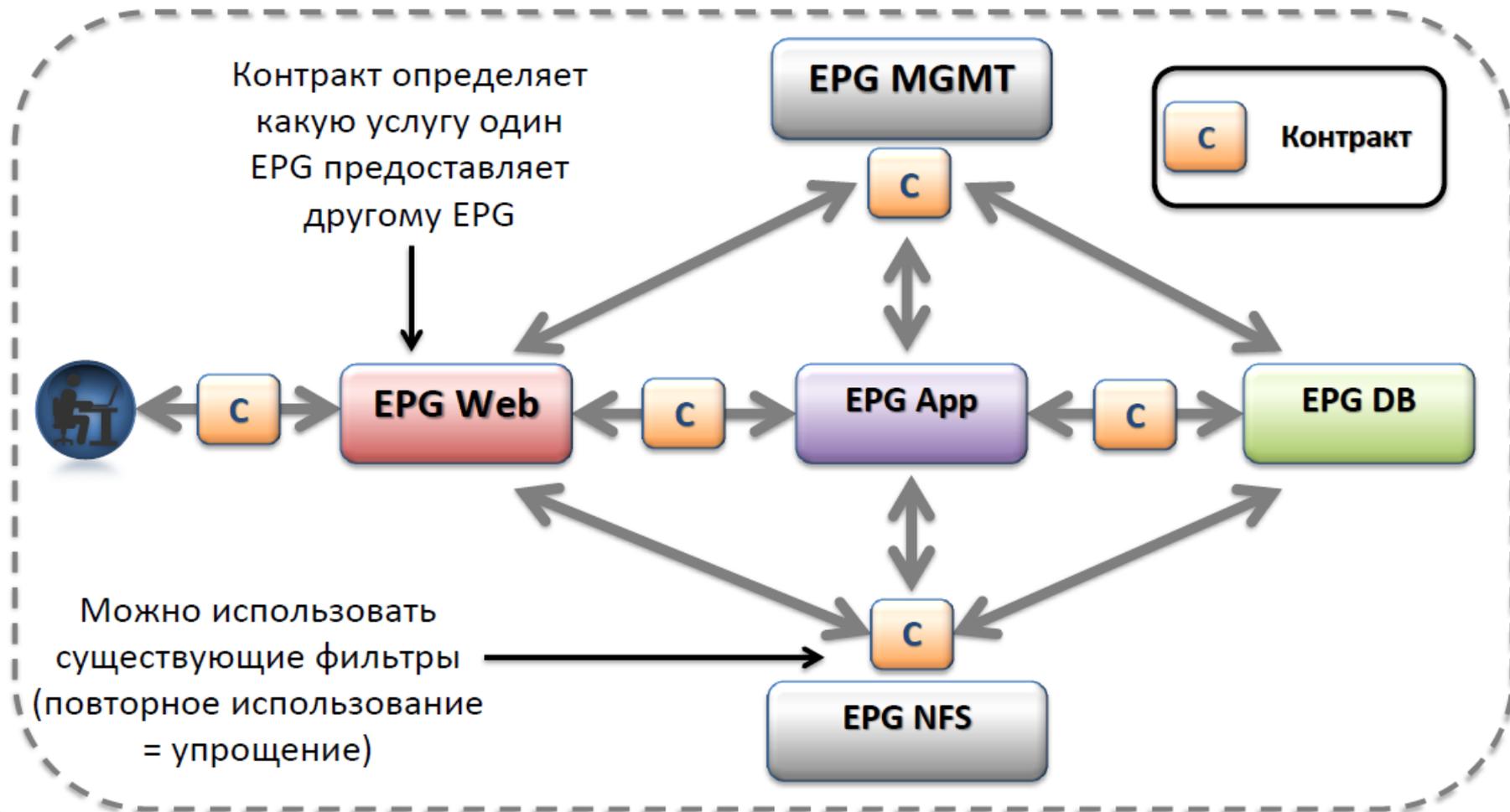
- ESX – распределенный коммутатор VMware (VLAN)
- ESX – коммутатор AVS от Cisco (VXLAN)
- Hyper-V – коммутатор от Microsoft (VLAN)
- Порт физического сервера (VLAN)

Application EPG - EPG One

| END POINT | MAC | IP | LEARNING SOURCE | HOSTING SERVER | REPORTING CONTROLLER NAME | INTERFACE | ENCAP | MULTICAST ADDRESS |
|---------------------|-------------------|---------------------|-----------------|-------------------------------|---------------------------|---|--------------|-------------------|
| WinXP-one | 00:15:50:4A:38:02 | 169.254.63.68, 1... | learned vmm | HYPERV-R2.ucslab.cisco.com | 10.48.82.69 | Node-101/eth1/43 (learned vmm) | vlan-334 | --- |
| VM1 | 00:50:56:B0:77:91 | 192.168.66.100 | learned vmm | esxi2-oci.ucslab.cisco.com | VC-DVS | 10.46.58.8 (vmm) 10.46.58.9 (vmm) Node-101-102/UCS-Mini_VPC-F1-A (learned) | vlan-500 | --- |
| VM4 | 00:50:58:88:98:86 | 192.168.66.200 | learned vmm | rackmount-r3.ucslab.cisco.com | AVS | Node-101-102/1-40_PoGrp (vmm) Node-101/tunnels (learned) Node-102/tunnels (learned) | vlan-8421376 | 235.1.1.1 |
| EP-AC-F2:CS:F8:3... | AC:F2:C5:F8:3D:01 | 192.168.66.244 | learned | | | Node-101-102/1-9_PoGrp (learned) | vlan-444 | --- |

Контракты в сетевом профиле приложения Разрешённые виды взаимодействия

Сетевой профиль приложения

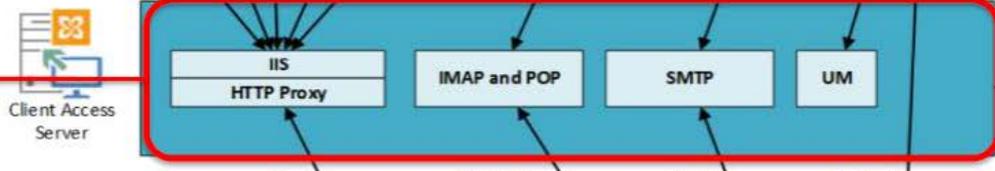


Внедрение традиционных приложений с Cisco ACI На примере Microsoft Exchange

EPG Outside

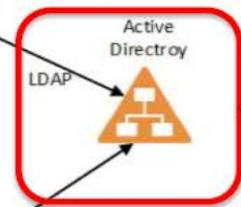
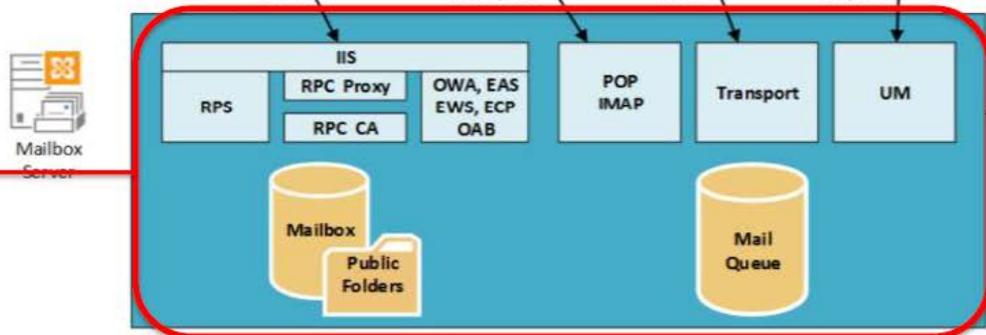


EPG CAS



Сервисное устройство SLB

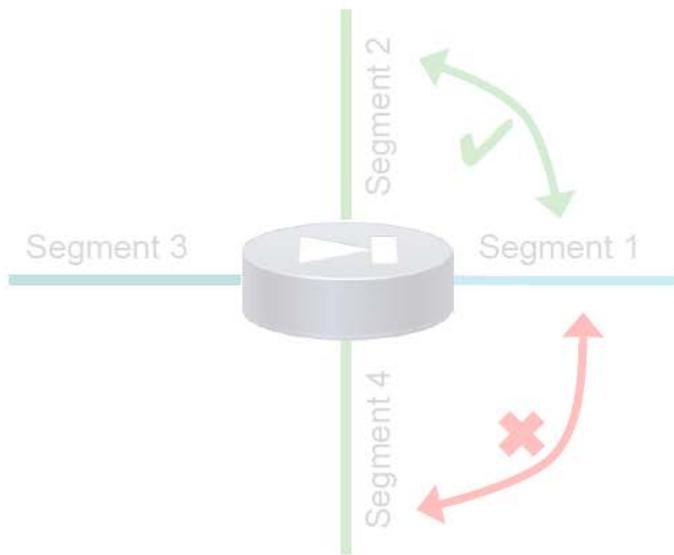
EPG Mail_Box



EPG AD

Микросегментация?

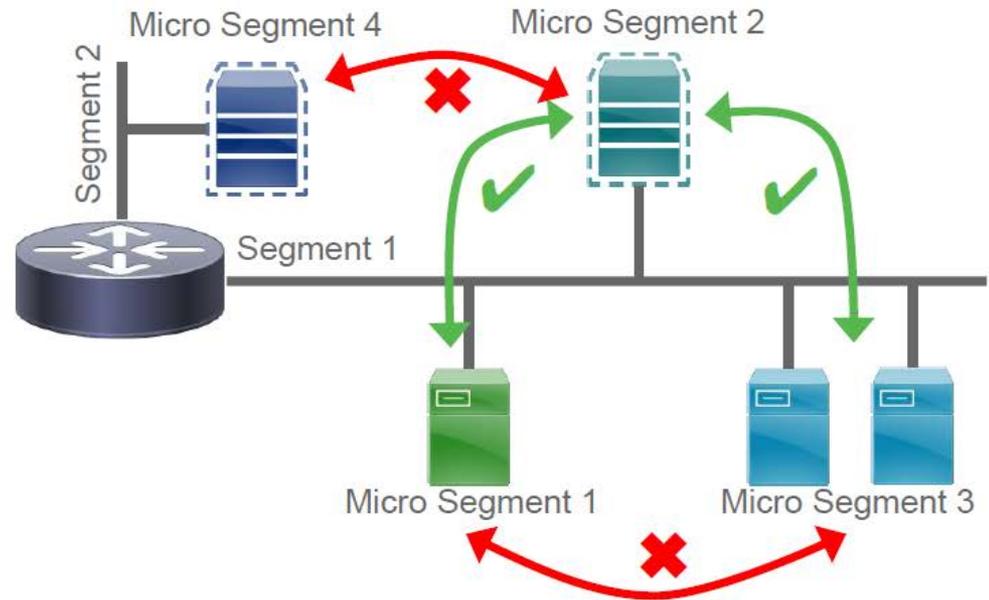
Сегментация



Сегмент = VLAN / подсеть



Микросегментация



Микросегмент = узел или группа узлов

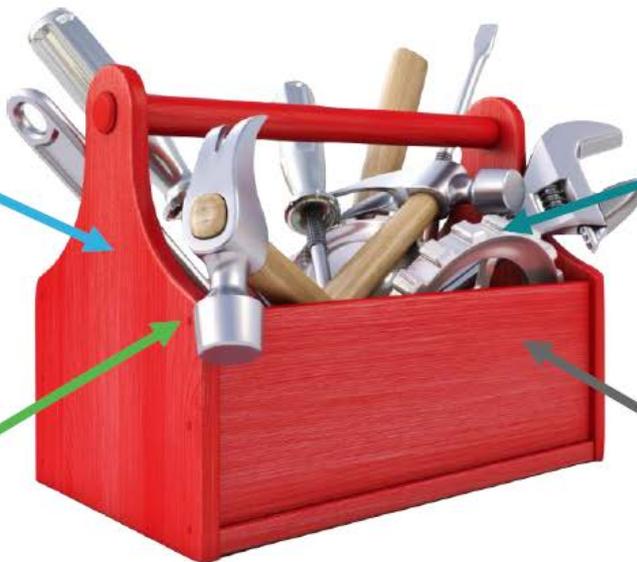
Инструментарий микросегментации Cisco ACI

EPG и контракты
Модель политик ACI

Микросегментация с
использованием
атрибутов

Изоляция внутри EPG

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 VM
- 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)

| Атрибуты VM | |
|------------------|-----------------------|
| Guest OS | vCenter VM Attributes |
| VM Name | |
| VM (id) | |
| VNIC (id) | |
| Hypervisor | |
| DVS port-group | |
| DVS | |
| Datacenter | |
| Custom Attribute | |
| MAC Address | |
| IP Address | VM Traffic Attributes |

«Распределенный межсетевой экран» на базе ACI

Коммутатор Leaf реализует stateless policy

| Src class | Src port | Dest Class | Dest port | Flag | Action |
|-----------|----------|------------|-----------|------|--------|
| A | * | B | 80 | * | Allow |
| B | 80 | A | * | ACK | Allow |

Аппаратная политика разрешает передачу пакета
 Reflexive policy на коммутаторе разрешает передачу обратного пакета

Применение политики на Leaf

Отслеживание состояния на AVS

- Создание новой записи внутри «flow table»
- Передача пакета на leaf коммутатор

| VLAN | Proto | Src ip | Src port | Dst IP | Dst port |
|------|-------|--------|----------|--------|----------|
| A | tcp | IP_A | 1234 | IP_B | 80 |
| A | tcp | IP_B | 80 | IP_A | 1234 |

- Получен пакет от VM
- Поиск внутри «flow table»

AVS

Consumer A

Если уже есть запись то пакет передается на коммутатор Leaf

При получении пакета TCP SYN создается новая запись

| VLAN | Proto | Src ip | Src port | Dst IP | Dst port |
|------|-------|--------|----------|--------|----------|
| B | tcp | IP_A | 1234 | IP_B | 80 |
| B | tcp | IP_B | 80 | IP_A | 1234 |

Ответ от VM
Поиск в таблице

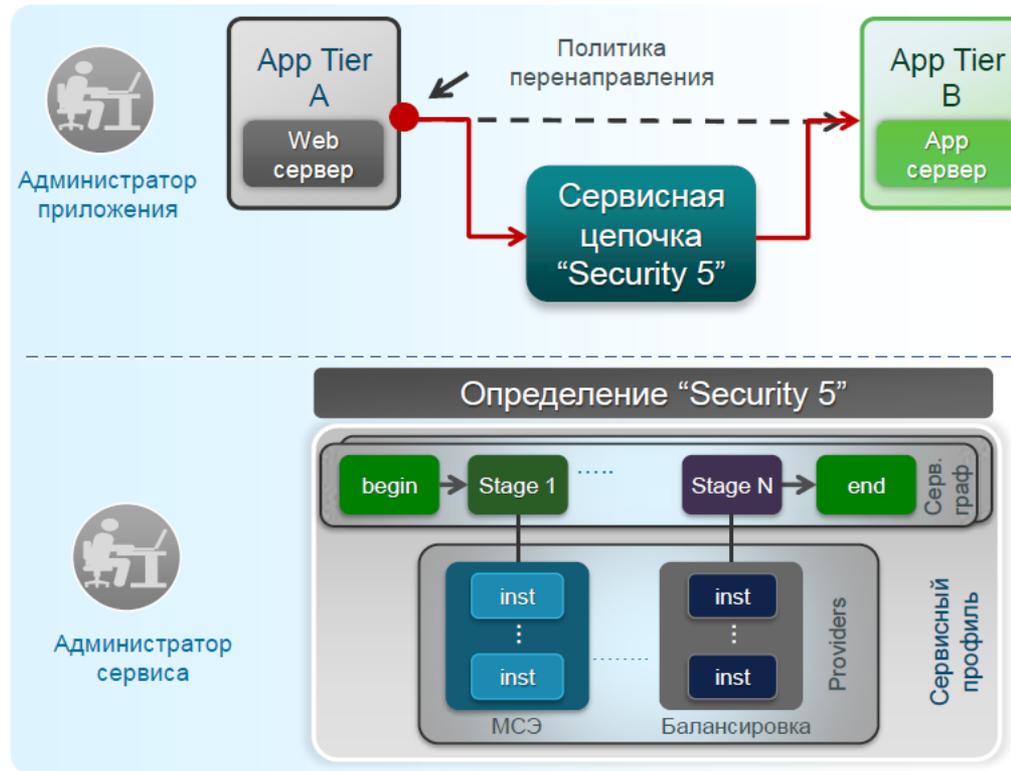
Provider B

Пакет передается VM

AVS

ACI: интеграция с сервисами 4 - 7 уровня

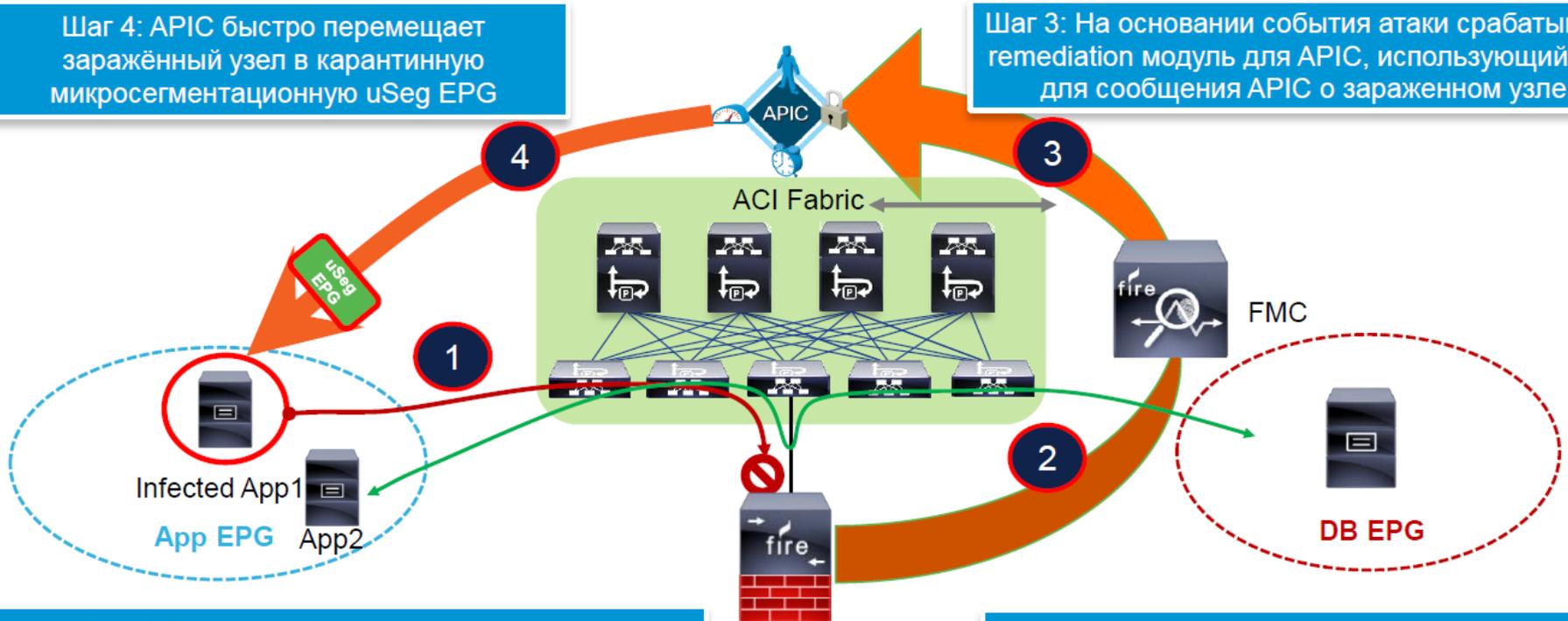
- Автоматизация вставки и настройки сервисов
- APIC – центральная точка контроля сети и согласования политик
- Безопасность (FW/IPS/...) и балансировка нагрузки
- От Cisco или от других компаний (включая российские)
- Физические или виртуальные сервисы
- Одиночные сервисы или цепочки
- Применение сервиса 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

Шаг 4: APIC быстро перемещает заражённый узел в карантинную микросегментационную uSeg EPG

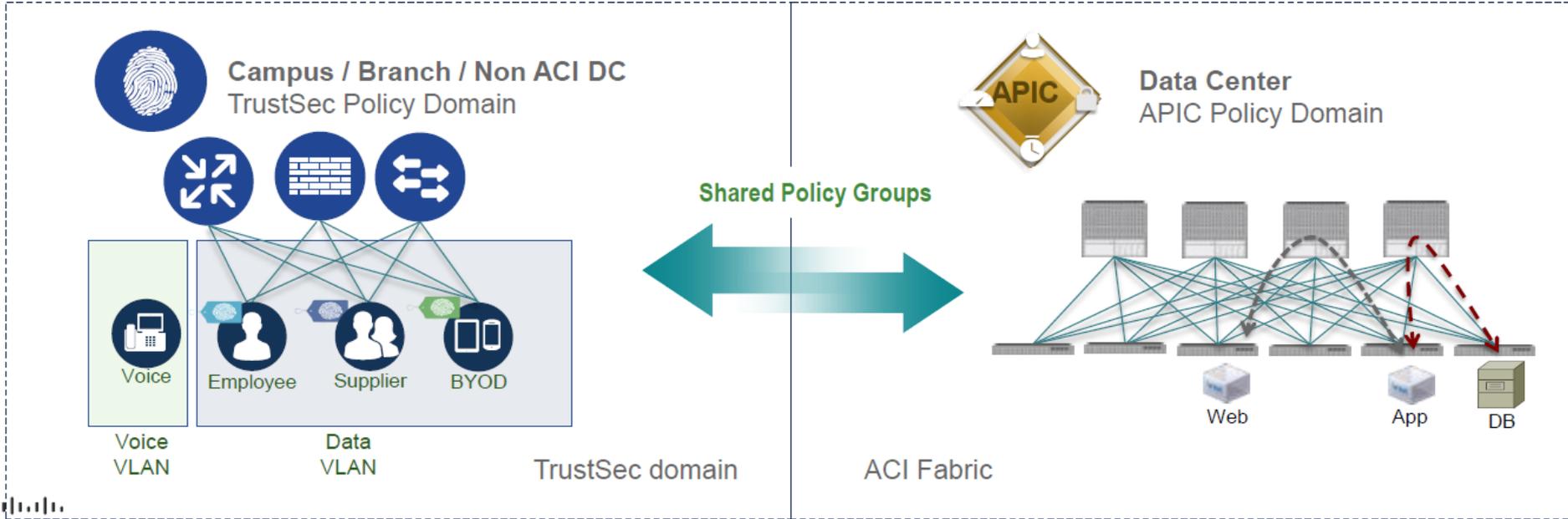
Шаг 3: На основании события атаки срабатывает remediation модуль для APIC, использующий API для сообщения APIC о зараженном узле



Шаг 1: Заражённый узел начинает атаку, обнаруживаемую и блокируемую NGFW(v), FirePOWER Services в ASA или FirePOWER appliance

Шаг 2: Событие о попытке вторжения генерируется и передается на FMC с информацией о заражённом хосте

Внедрение сквозных групповых политик в масштабах организации



Группы TrustSec и членство в них - представление в ACI

The screenshot shows the Cisco ACI GUI with the 'Networks' page selected. The left sidebar shows a tree view of the configuration, with 'L3_ROUTE_DEMO' expanded to show 'Networks'. The main content area displays a table of networks. A red box highlights the table, and another red box highlights the 'SUMMIT' column with the text 'Члены групп'.

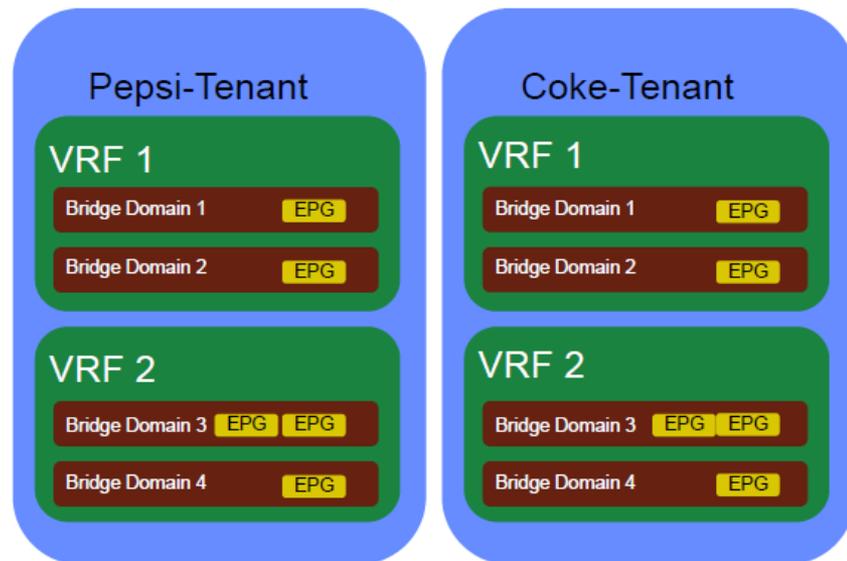
| NAME | QOS CLASS | DESCRIPTION | TARGET DISC | SUMMIT |
|---------------------------|-------------|-------------|-------------|--|
| Auditors_SGT | Unspecified | | Unspecified | 192.168.1.1/32, 192.168.1.3/32, 192.168.1.5/32 |
| BYOD_SGT | Unspecified | | Unspecified | 14.1.1.1/32, 192.168.1.2/32 |
| Contractors_SGT | Unspecified | | Unspecified | 192.168.1.4/32 |
| Developers_SGT | Unspecified | | Unspecified | 13.1.1.1/32 |
| Development_Servers_SGT | Unspecified | | Unspecified | |
| Employees_SGT | Unspecified | | Unspecified | 12.1.1.1/32 |
| Guests_SGT | Unspecified | | Unspecified | |
| Network_Services_SGT | Unspecified | | Unspecified | |
| PCI_Servers_SGT | Unspecified | | Unspecified | |
| Point_of_Sale_Systems_SGT | Unspecified | | Unspecified | |
| Production_Servers_SGT | Unspecified | | Unspecified | |
| Production_Users_SGT | Unspecified | | Unspecified | |
| Quarantined_Systems_SGT | Unspecified | | Unspecified | |
| Test_Servers_SGT | Unspecified | | Unspecified | |
| TrustSec_Devices_SGT | Unspecified | | Unspecified | |

SGTs видны как External EPG

Члены групп

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

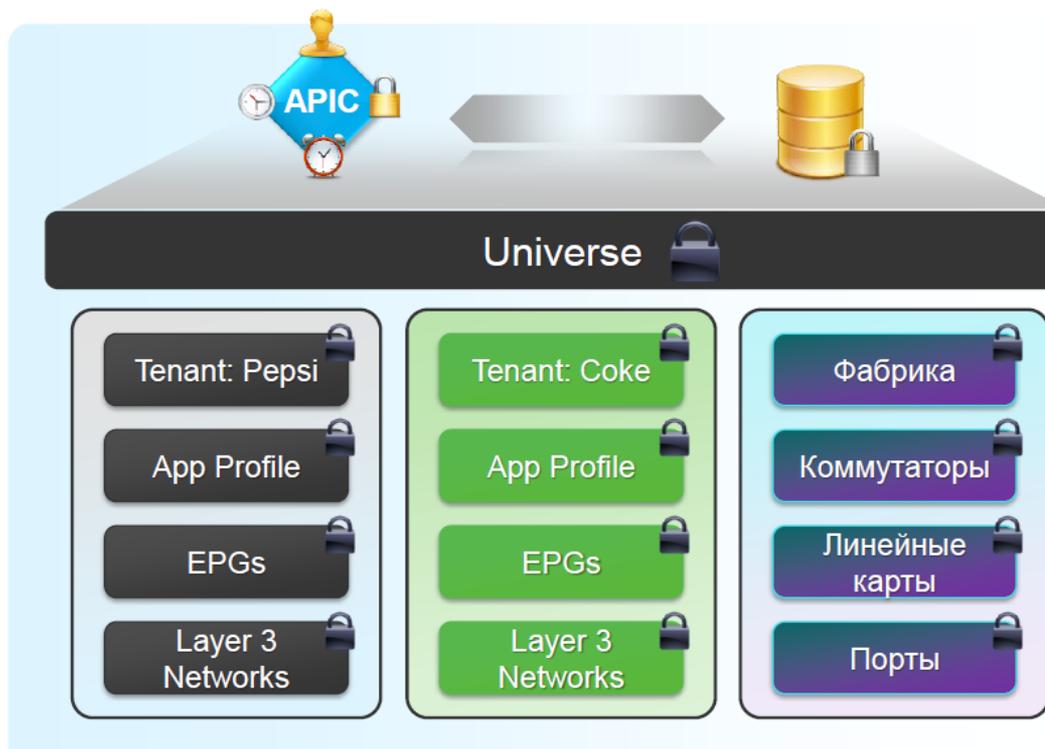
Доступ ко всем объектам управления после аутентификации и по защищенному каналу

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 выполнения (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

| TIME STAMP | USER | ACTION | AFFECTED OBJECT | DESCRIPTION | |
|-------------------------------|-----------|----------|--|---|------------------------|
| 2015-03-04T01:03:50.288+00:00 | admin | deletion | uni/tn-Customer/acEpToEp-yong_67_dst_src | EpToEp yong_67_dst_src deleted | |
| 2015-03-04T01:03:50.288+00:00 | admin | deletion | uni/tn-Customer/acEpToEp-yong_67_dst_src/rstoEpForEpToEp-[uni/tn-Customer/ap-DB/epg-SQLServerPool-1/cep-00:00:1F:FB:01:11] | RstoEpForEpToEp uni/tn-Customer/ap-DB/epg-SQLServerPool-1/cep-00:00:1F:FB:01:11 deleted | |
| 2015-03-04T01:03:50.288+00:00 | admin | deletion | uni/tn-Customer/acEpToEp-yong_67_dst_src/rfromEp-[uni/tn-Customer/ap-Apps/epg-AppServerPool-1/cep-00:00:20:03:9D:4F] | RrFromEp uni/tn-Customer/ap-Apps/epg-AppServerPool-1/cep-00:00:20:03:9D:4F deleted | |
| 2015-03-04T01:03:50.228+00:00 | admin | deletion | uni/tn-Customer/acEpToEp-yong_67_dst_src | EpToEp yong_67_dst_src deleted | |
| 2015-03-04T01:03:50.228+00:00 | admin | deletion | uni/tn-Customer/acEpToEp-yong_67_dst_src/rstoEpForEpToEp-[uni/tn-Customer/ap-Apps/epg-AppServerPool-1/cep-00:00:20:03:9D:4F] | RstoEpForEpToEp uni/tn-Customer/ap-Apps/epg-AppServerPool-1/cep-00:00:20:03:9D:4F deleted | |
| 2015-03-04T01:03:50.228+00:00 | admin | deletion | uni/tn-Customer/acEpToEp-yong_67_dst_src/rfromEp-[uni/tn-Customer/ap-DB/epg-SQLServerPool-1/cep-00:00:1F:FB:01:11] | RrFromEp uni/tn-Customer/ap-DB/epg-SQLServerPool-1/cep-00:00:1F:FB:01:11 deleted | |
| 2015-03-04T01:01:27.905+00:00 | admin | creation | uni/tn-Customer/acEpToEp-yong_67_dst_src | EpToEp yong_67_dst_src created | |
| 2015-03-04T01:01:27.905+00:00 | admin | creation | uni/tn-Customer/acEpToEp-yong_67_dst_src/rstoEpForEpToEp-[uni/tn-Customer/ap-DB/epg-SQLServerPool-1/cep-00:00:1F:FB:01:11] | RstoEpForEpToEp uni/tn-Customer/ap-DB/epg-SQLServerPool-1/cep-00:00:1F:FB:01:11 created | |
| 2015-03-04T01:01:27.905+00:00 | | | | | |
| 2015-03-04T01:01:27.834+00:00 | | | | | |
| 2015-03-04T01:01:27.834+00:00 | 589939999 | admin | modification | uni/fabric/tsod-ts | TechSupOnD ts modified |
| 2015-03-04T01:01:27.833+00:00 | | | | | |
| 2015-03-04T01:01:20.705+00:00 | | | | | |

MODIFICATION LOG RECORD - 85...

PROPERTIES

ID: 8589939999

Description: TechSupOnD ts modified

Affected Object: uni/fabric/tsod-ts

Time Stamp: 2014-11-10T10:10:37.152+00:00

Cause: transition

Change Set: adminSt (Old: untriggered, New: untriggered)

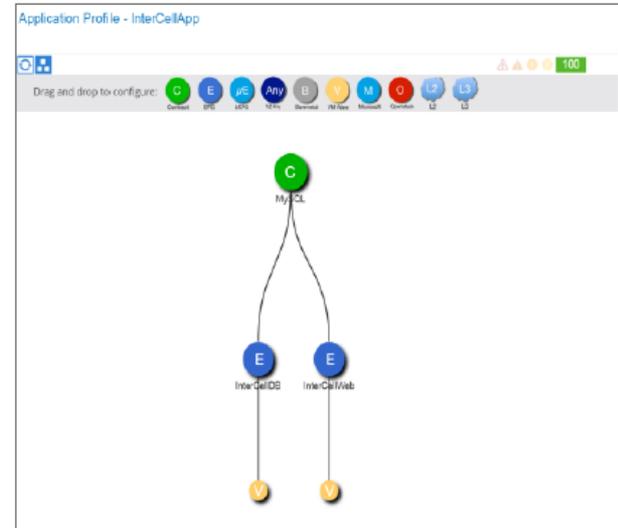
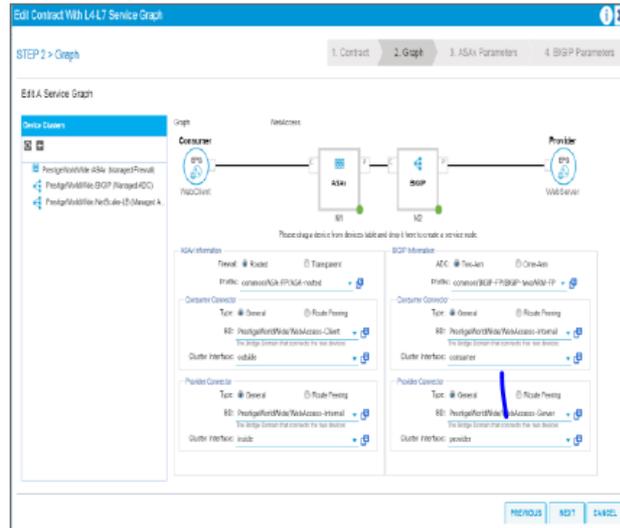
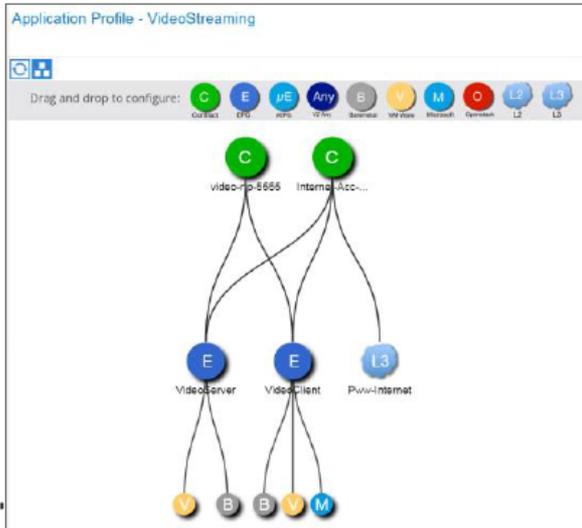
Action Performed: modification

CLOSE

Автоматический отчёт о политиках безопасности

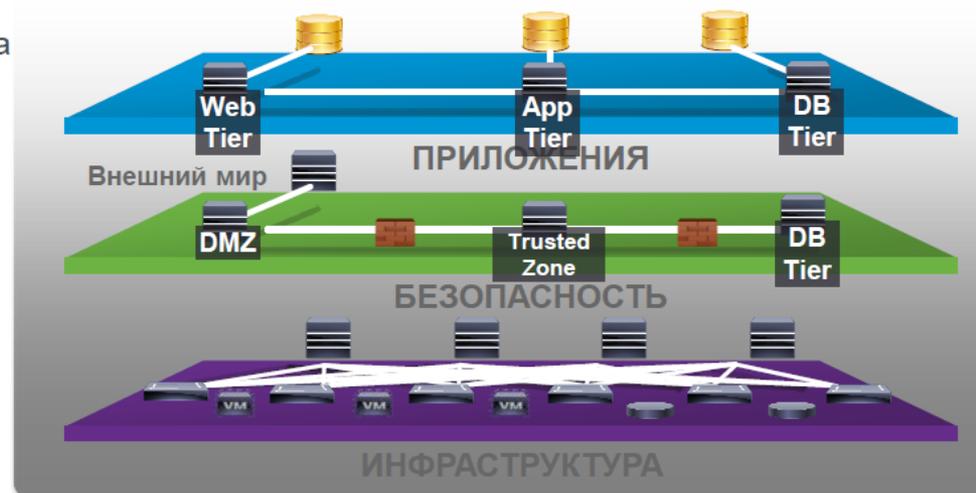
| No | Tenant | VRF | BD | Application | Consumer EPG/Endpoints | Provider EPG/Endpoints | Contract | Filter Protocol | Filter Source Ports | Filter Destination Ports | Service Graph ID | Service Node | Service Node | Permit Hits | Deny Hits |
|----|----------|------|------|----------------|------------------------|------------------------|-----------|-----------------|---------------------|--------------------------|------------------|--------------|--------------|-------------|-----------|
| 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 разработки
- **Полная изоляция организаций (tenants)**
- **Интегрированные возможности аудита**
 - Протоколирование 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>

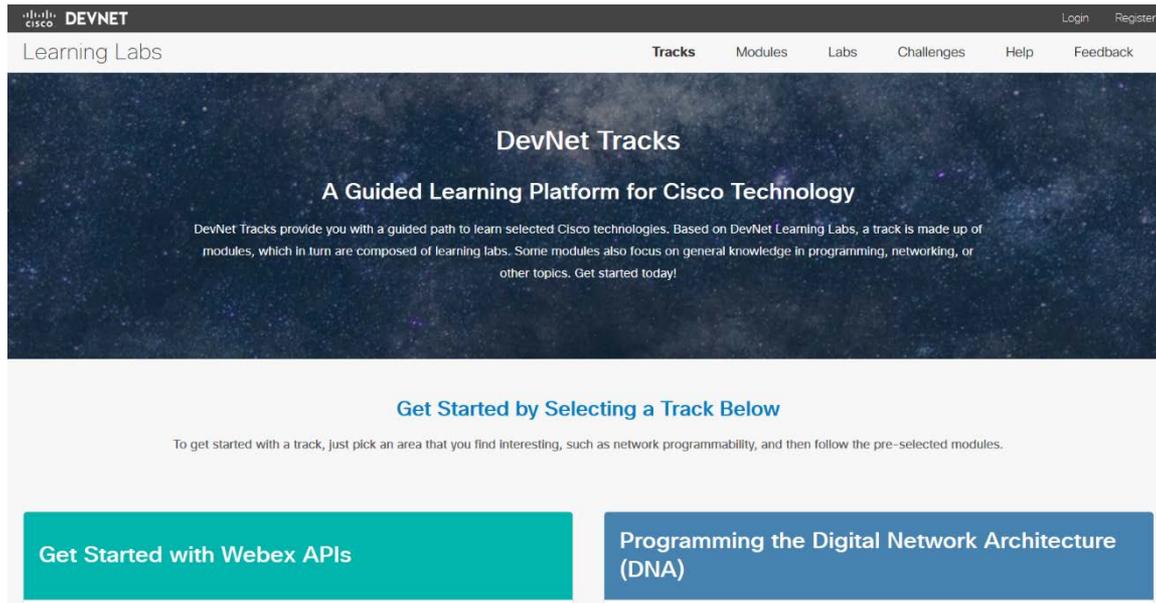
<https://ciscolive.cisco.com/>

<https://vk.com/cisco>

<http://blogs.cisco.com/>

<https://learninglabs.cisco.com/>

<https://dcloud.cisco.com/>



The screenshot shows the DevNet Tracks website. At the top, there is a navigation bar with the Cisco logo, 'DEVNET', and links for 'Login' and 'Register'. Below the navigation bar, there is a 'Learning Labs' section with a menu of 'Tracks', 'Modules', 'Labs', 'Challenges', 'Help', and 'Feedback'. The main content area features a dark background with the text 'DevNet Tracks' and 'A Guided Learning Platform for Cisco Technology'. Below this, there is a paragraph explaining that DevNet Tracks provide a guided path to learn selected Cisco technologies. At the bottom, there is a section titled 'Get Started by Selecting a Track Below' with a sub-paragraph explaining how to get started. Two buttons are visible: 'Get Started with Webex APIs' and 'Programming the Digital Network Architecture (DNA)'.



dCloud