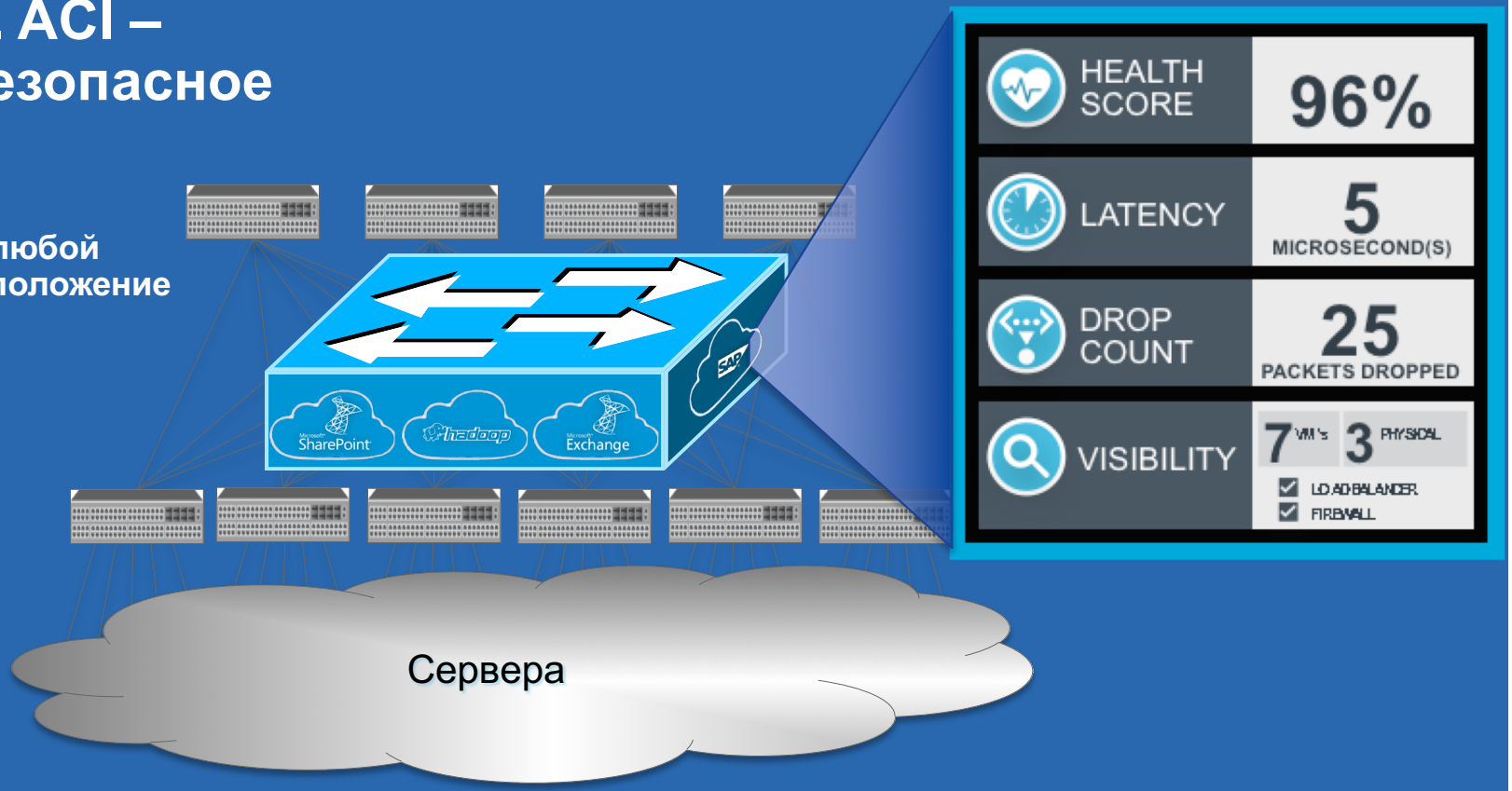
Cisco TechTalks. ACI – Современное безопасное ядро сети ЦОД

Любая рабочая нагрузка, любой гипервизор, любое местоположение



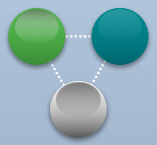
Виктор Подкорытов
Cisco SE

vpodkory@cisco.com

+38 044 3913600

Необходима НОВАЯ Операционная модель

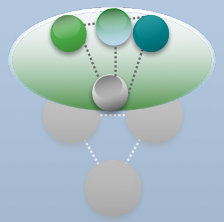
Традиционная СЕТЕВАЯ МОДЕЛЬ



СЕТЬ КОРОБОК

Существующая Модель

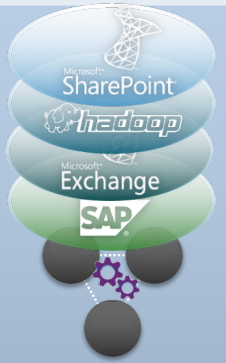
SDN МОДЕЛЬ



Software-Based Network Virtualization

2 Сети вместо 1…

НОВОЕ ПОКОЛЕНИЕ



APP-CENTRIC INFRASTRUCTURE

Едины Сеть и Автоматизация

Гибкость и HW производи-сть

Applications Drive Development Network

Cisco ACI на рынке

4,800+

ACI Customers

65+

Ecosystem Partners

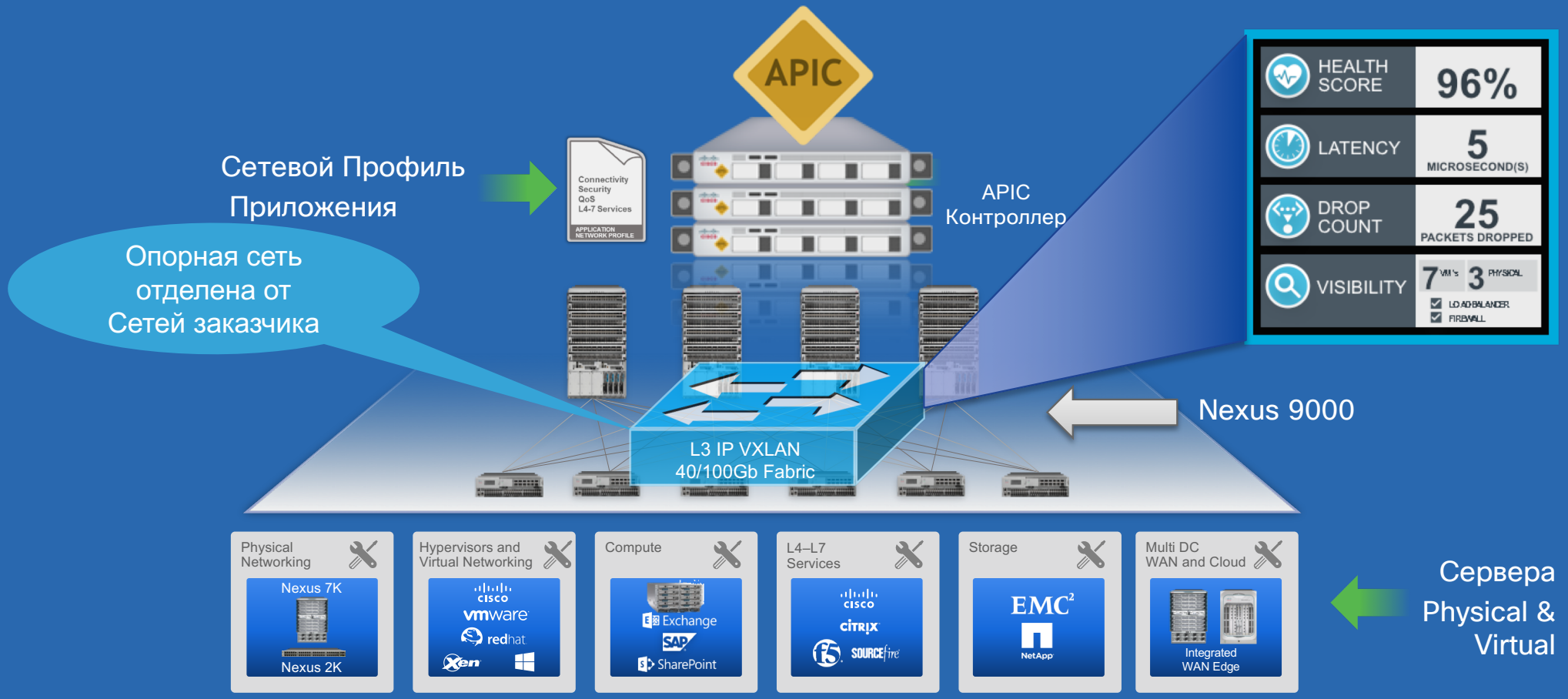
38+%

Quarterly Revenue Growth

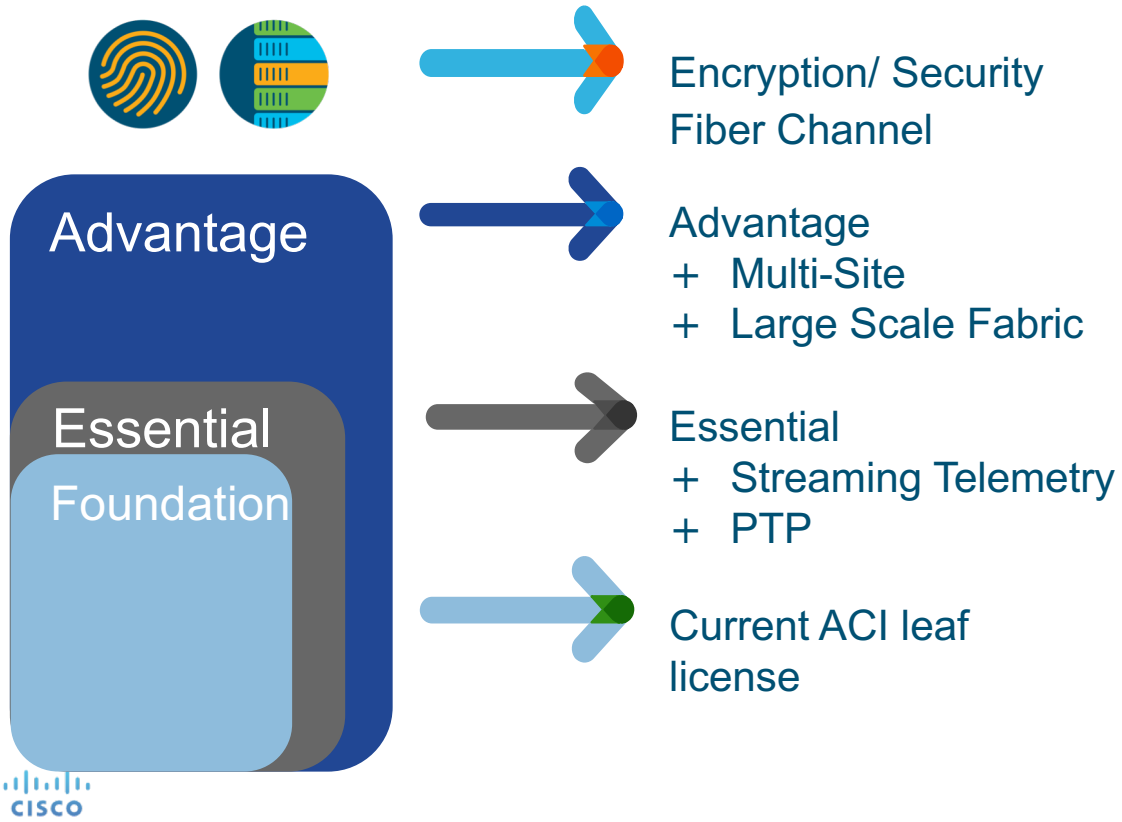
ECOSYSTEM PARTNERS

Заказчики по всему миру!

Ориентированная на Приложения Инфраструктура



Лицензирование ACI



ACI лицензируется на каждый leaf, без дополнительных лицензий для spines и APIC

Гибкость схем лицензирования

Традиционный подход:Traditional License Option

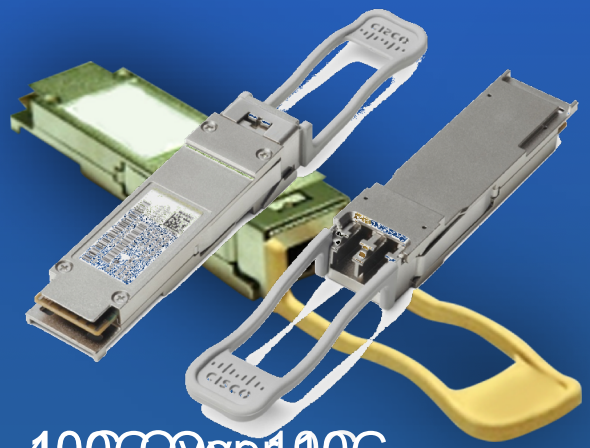
- «Вечные» лицензии
- Essential & Advantage Tier + Add-Ons

Временные Лицензии

- Те же уровни
- Стоимость на 1, 3, 5 лет

Инновации в Оптике: цена 40Gb ≈ 10Gb
Ре-использование обычной пары MM оптики

40G BiDi Optics



40G Over 10G
Multimode Fiber

100G

Экономия при
переходе на 40/100G

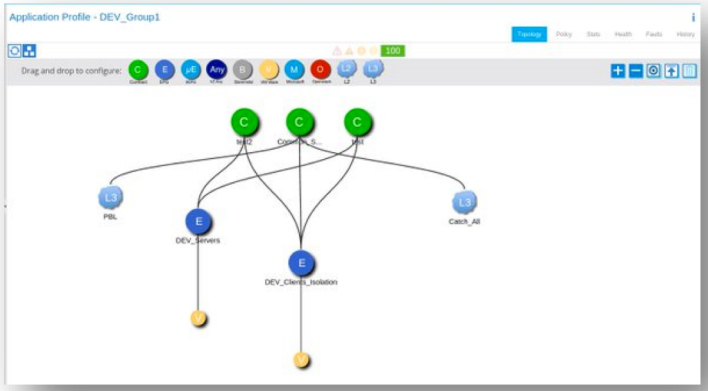
(99% DC)

Контроллер ACI

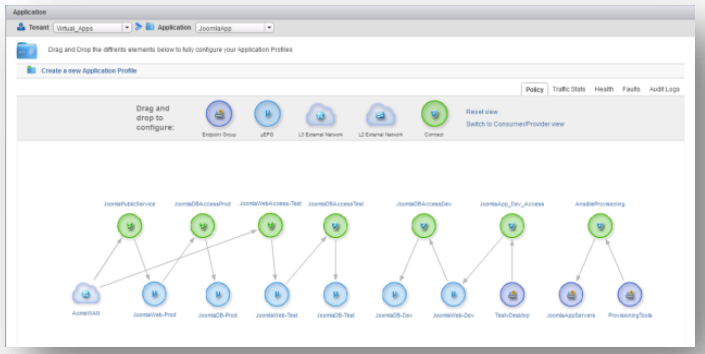
Централизованная автоматизация и управление фабрикой

- **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)**

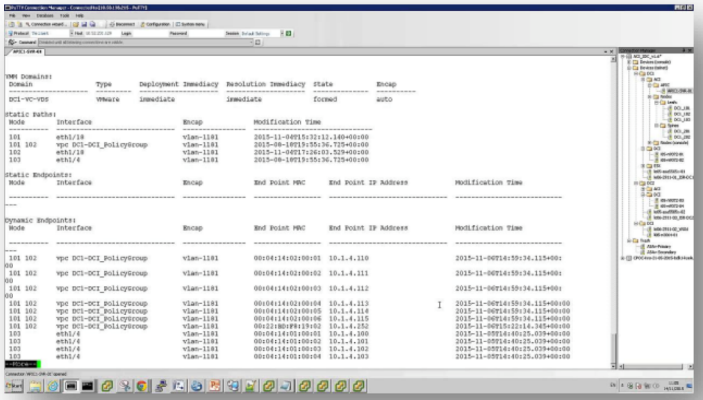
Разнообразие методов управления ACI



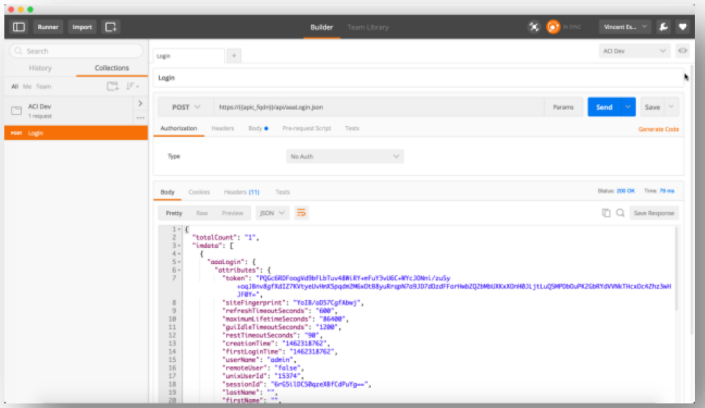
APIC GUI



Плагин для vCenter

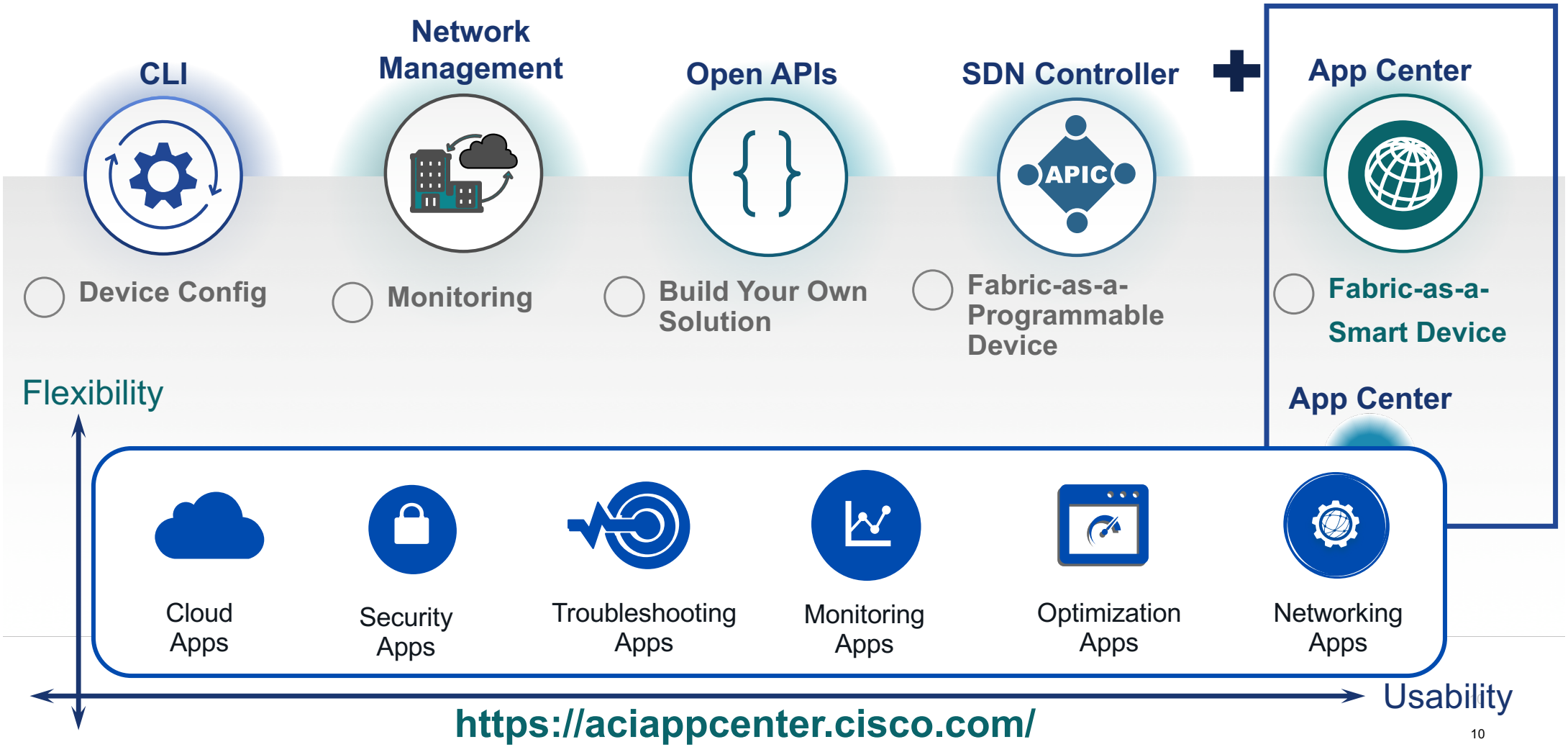


NX-OS-подобный CLI



API - автоматизация

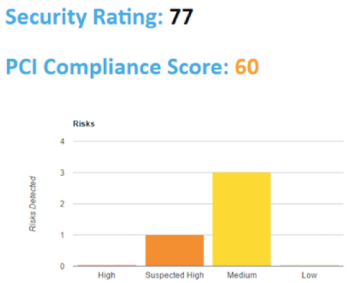
Представляем ACI App Center



App Center Apps

Programmable Infrastructure: Open APIs for Value Added Applications

AlgoSec



Get Your Fabric A Score On Security And Compliance.

Path Analysis

Connectivity and Compliance

Dimension Data

Route Visualizer

Tetration

Discover Application Dependencies and Define Application Network Profile

Smart Tenant Deployment

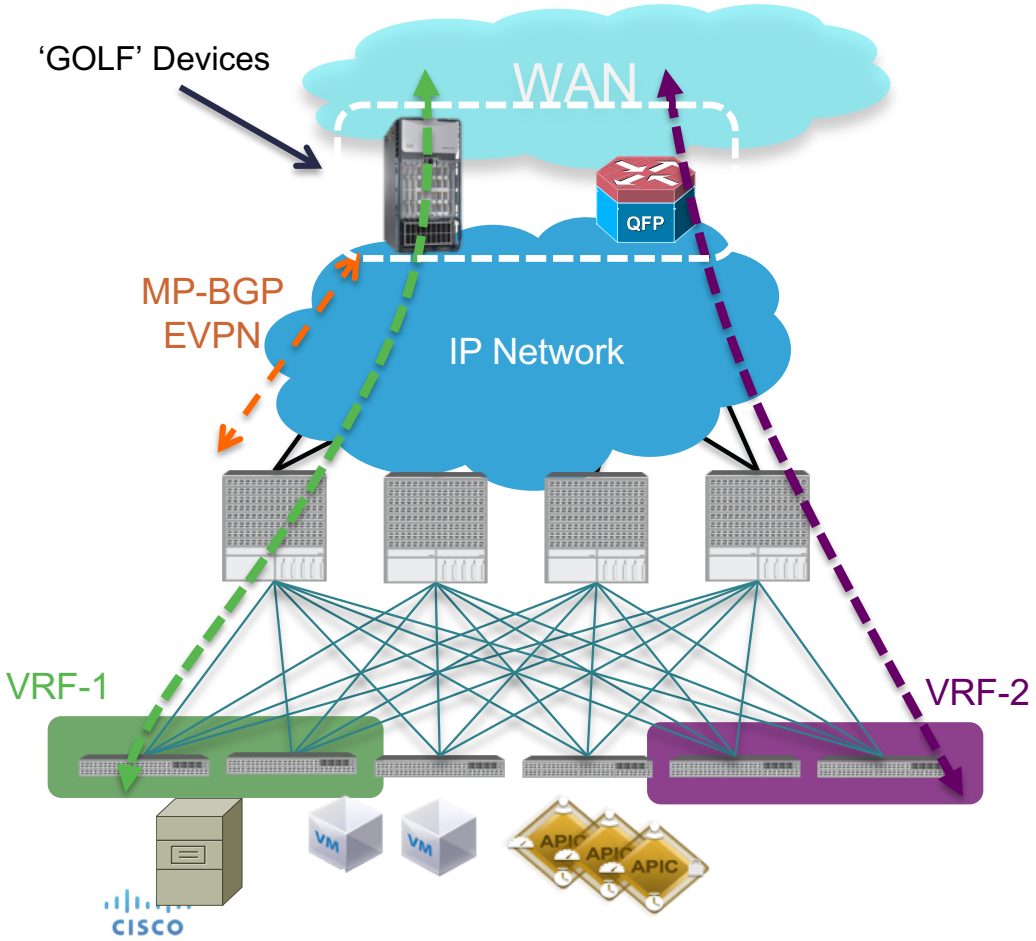
Cisco DevNet

Keep A Pulse On Your Network Hardware Resources (TCAM, Memory Etc.) Across The Fabric

Fabric Resource Inspector (NRI)

ECOSYSTEM splunk> puppet labs servicenow Infoblox **Sample Apps**

Масштабируемая интеграция ACI с WAN роутерами
Обзор проекта GOLF



- Масштабирование уровня передачи данных и управления
  - VXLAN инкапсуляция между ACI spines и WAN роутерами
  - BGP-EVPN control plane между ACI spines и WAN роутерами
  - OpFlex для обмена настройками (имена VRF, BGP Route-Targets и т.д.)
- Применение политик на ACI коммутаторах (в обоих направлениях)
- Поддержка маршрутизаторов :
  - Nexus 7k, ASR9000
  - ASR1000, CSR1000v

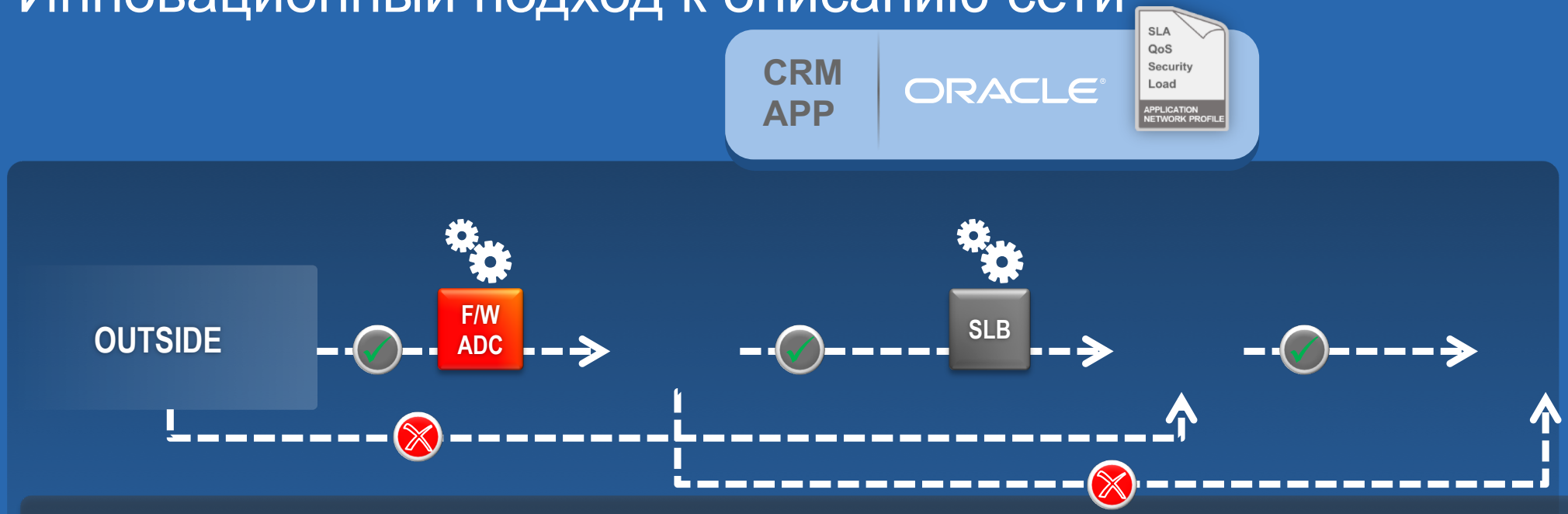
Политика ACI

Сетевой профиль приложения = сетевая политика в ACI

“Разрешить WEB серверам коммуникацию с APP серверами”

- Определяется разнообразные требования к инфраструктуре приложения: безопасность, QoS, SLA, L4-L7 сервисы, потоки в фабрике и т.д.
- Политика абстрактна и не привязана к моделям коммутаторов (логический уровень)
- Политика перемещаема, как и приложение она может применятся как внутри ЦОД так и в другом ЦОД

Инновационный подход к описанию сети



Что такое Политика Приложения?

1. Группа: Набор VM или физических серверов с одинаковой политикой
2. Контракт: Набор правил (ACL) взаимодействия между группами
3. Сервисная Цепочка: Набор сетевых сервисов между группами

Модель политик ACI
различные методы определения элементов EPG

Сервер

Виртуальные машины
или контейнеры

СХД

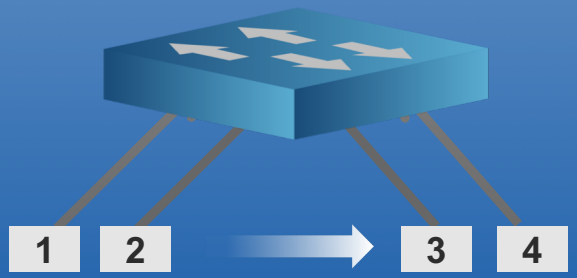
Клиенты

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

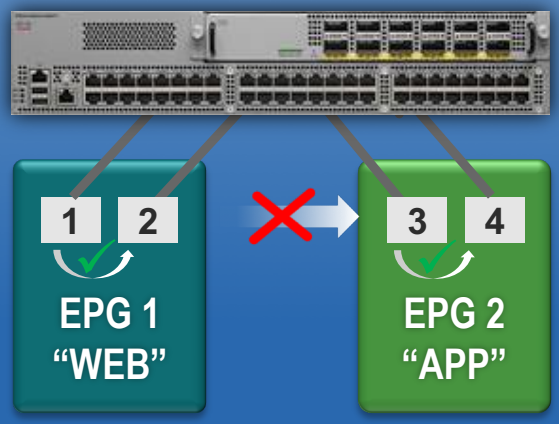
- Примеры критериев отнесения к EPG
  - Физический порт (на коммутаторе или FEX)
  - Логический порт (VM port group)
  - VLAN ID
  - Атрибуты виртуальных машин
  - IP адрес
  - MAC адрес
  - IP подсеть (применительно ко внешним подключениям)

ACI Политика по умолчанию “Zero Trust”

TRUST BASED ON LOCATION
(Traditional DC Switch)

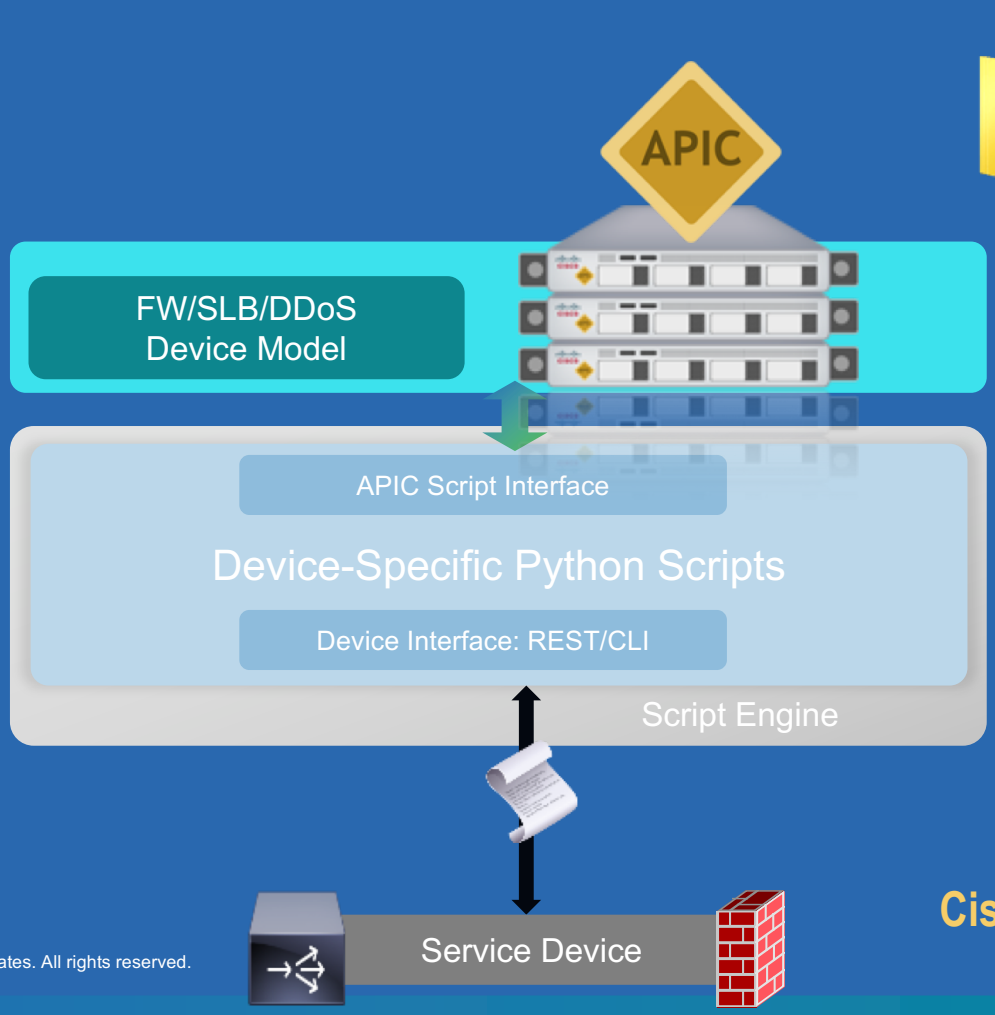


ZERO TRUST ARCHITECTURE
(Nexus 9000 with ACI)



Whitelist policy = Explicitly configured ACI contract between EPG 1 and EPG 2 allowing traffic between their members
ACI architecture allows flexible EPG membership, enabling wide range of security policies

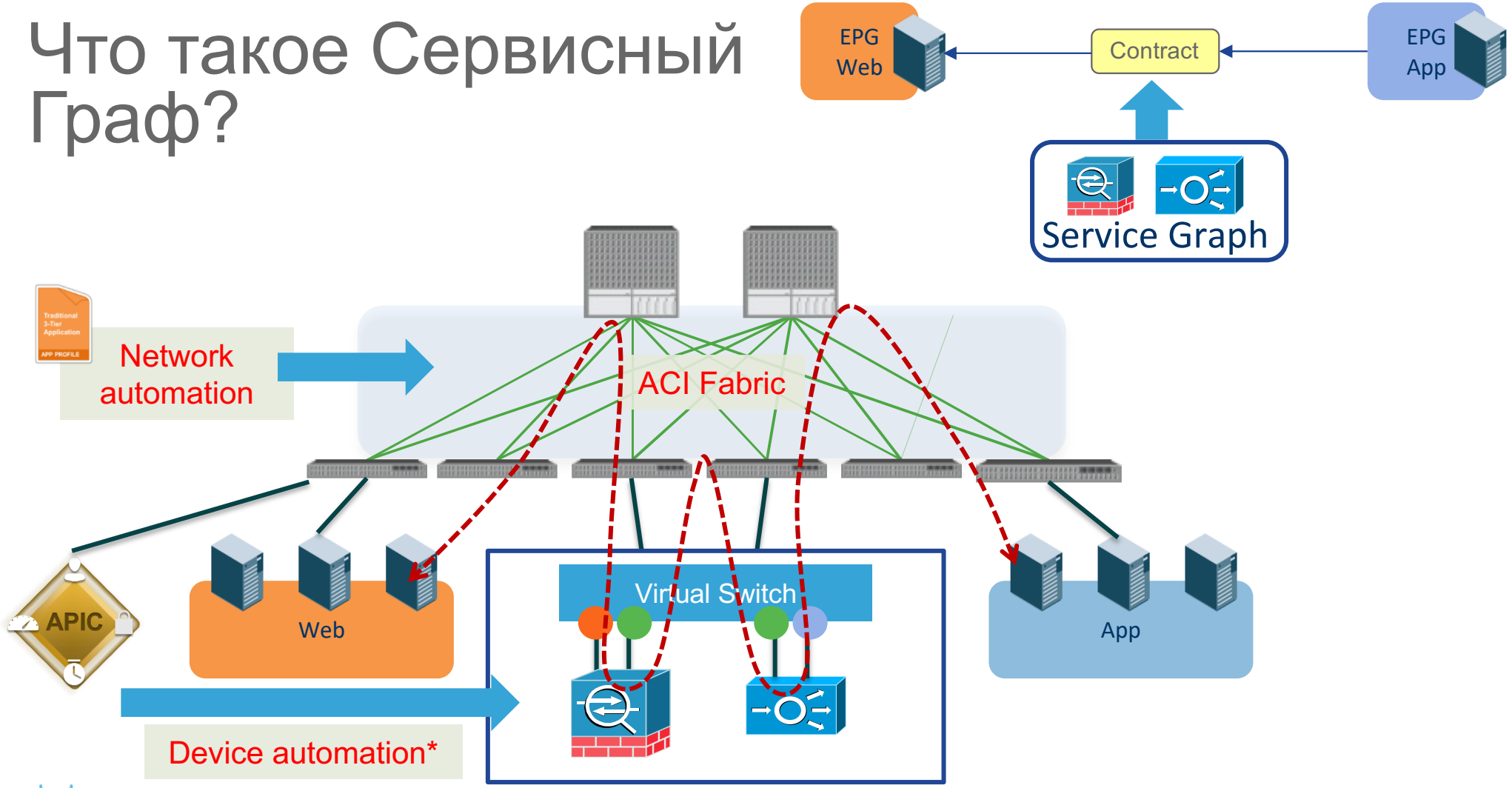
УПРОЩЕНИЕ ACL / интеграции сетевых сервисов



Файл с описанием Возможностей Устройства

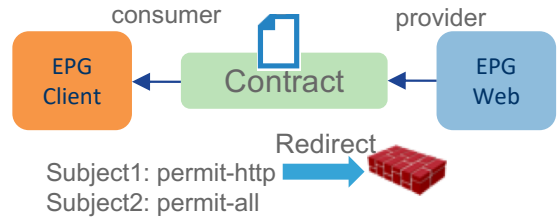
Cisco ASA / ASAv, SLB и т.п.

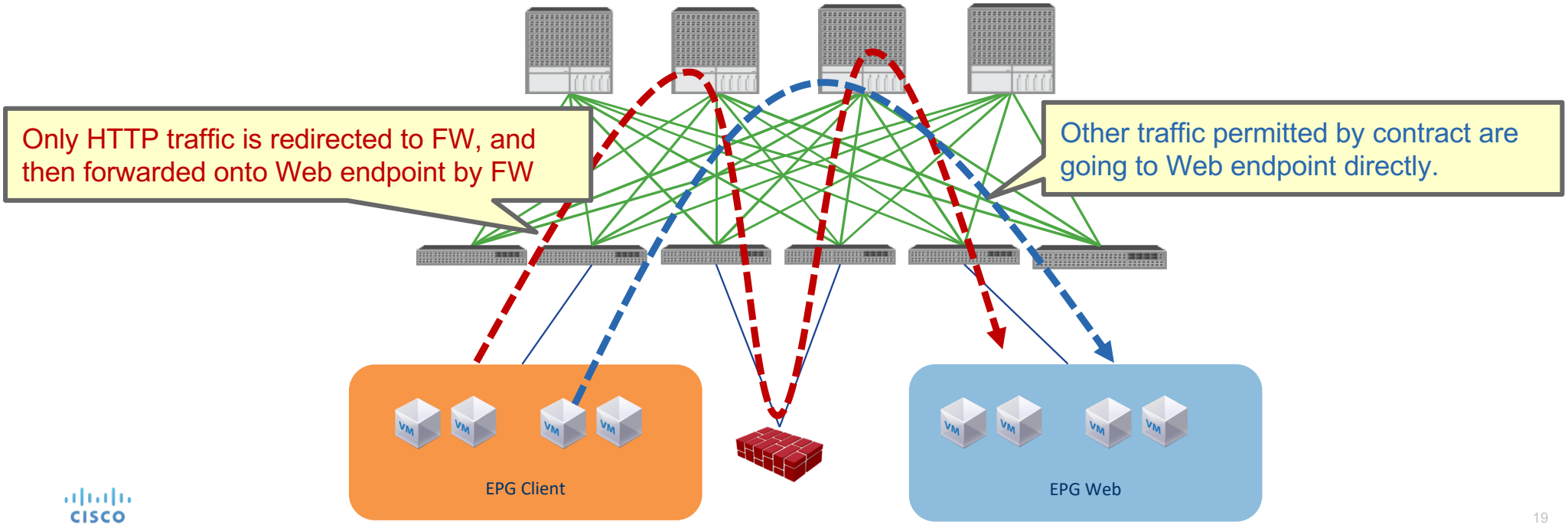
Что такое Сервисный Граф?



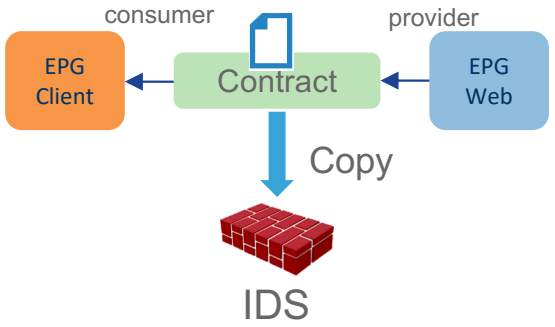
*Managed Mode/Hybrid Mode Only

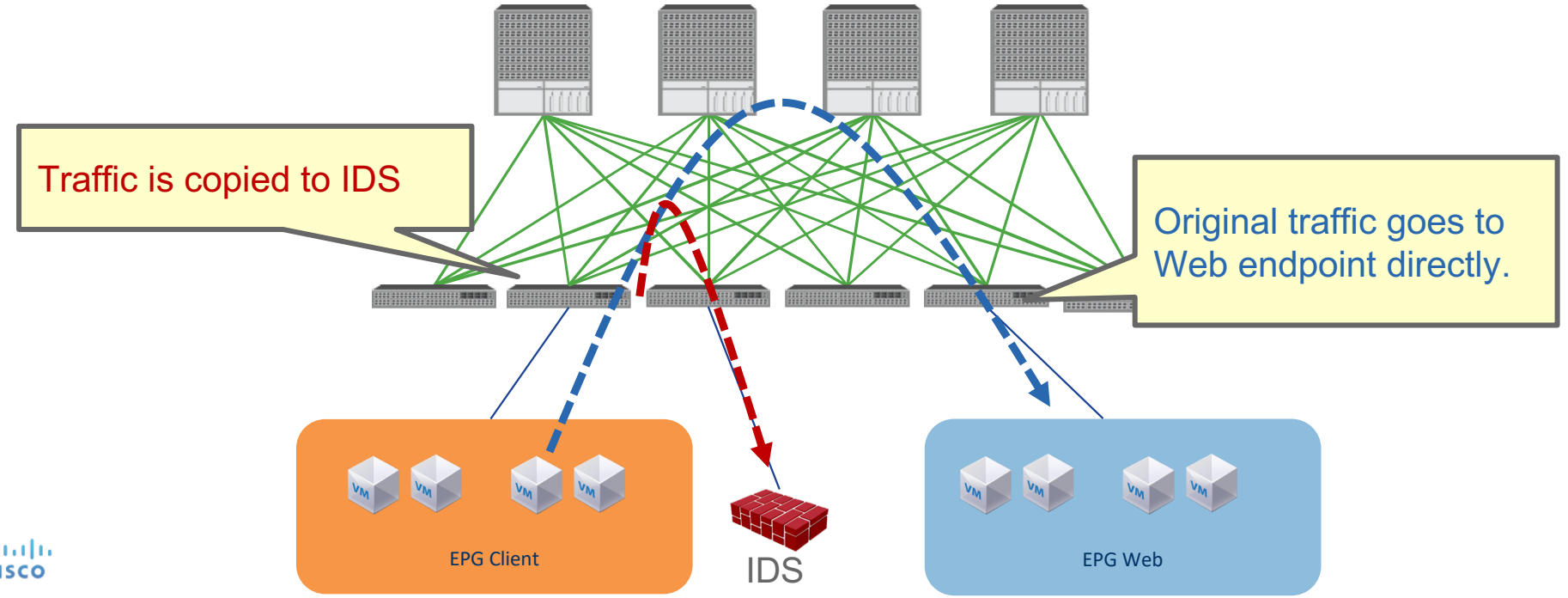
Обзор
Policy Based Redirect (PBR)



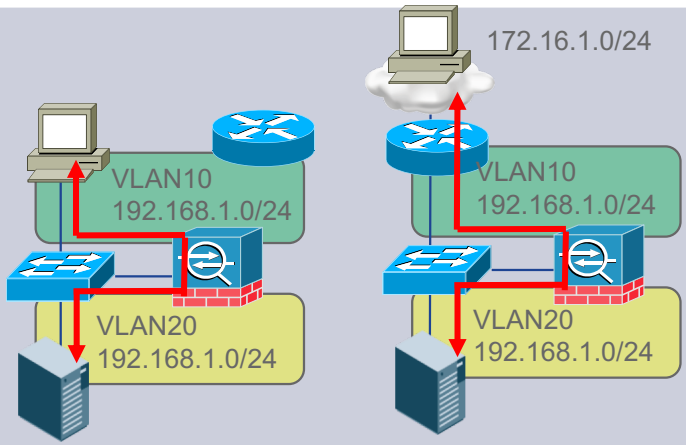
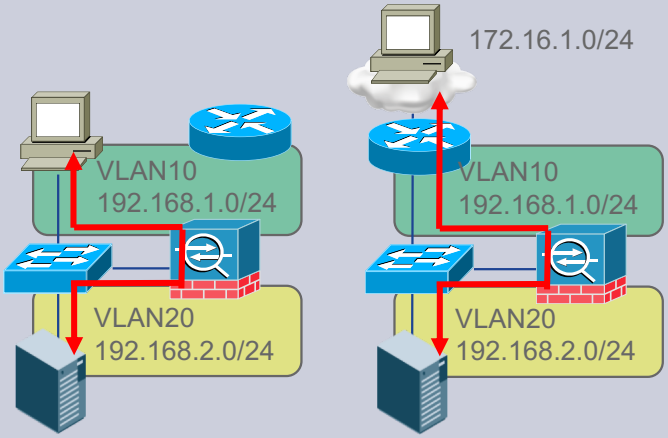


Обзор
Copy Service

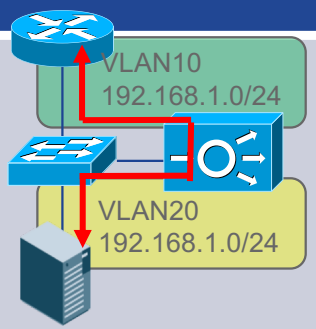
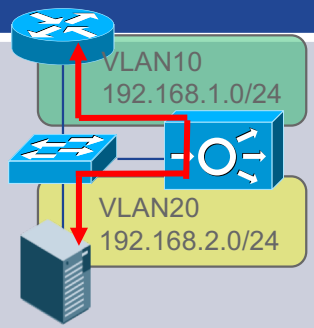
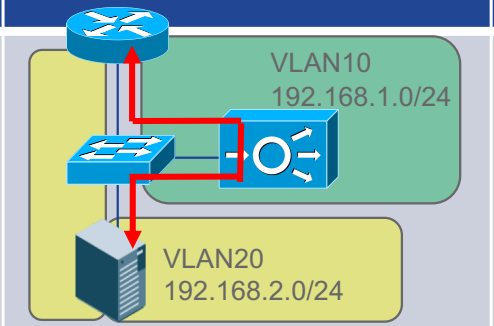
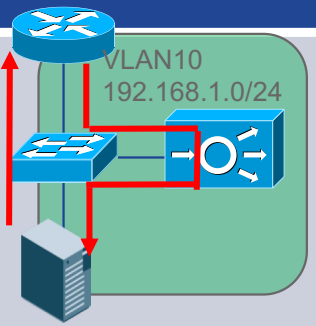




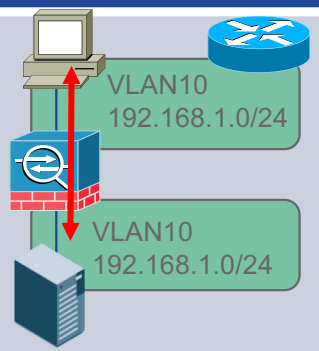
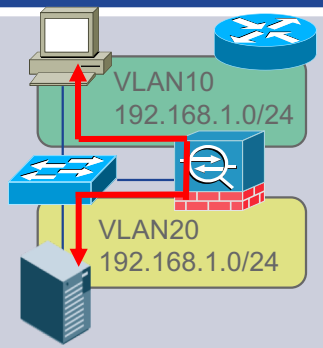
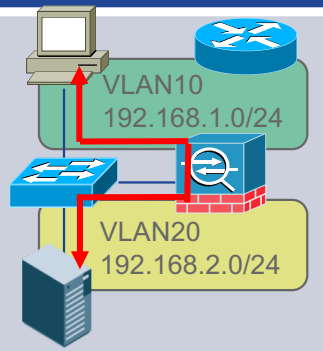
Firewall Mode Options

	L2 (Transparent)	L3 (Routed)
		
Default GW of servers	Router	Firewall alias IP of server-side (in case of ASA, active IP)
When to use	Want to use same subnet for client-side and server-side	Common case when we can have separate VLAN/subnet for client-side and server-side.

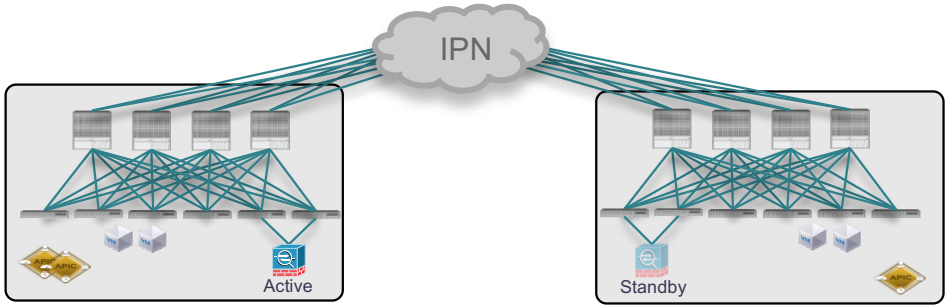
ADC Design Options

	L2 (Bridged)	L3 (Routed) Two-Arm	One-Arm	DSR
				
Default GW of server	Router	ADC alias IP (server side)	Router	Router
NAT	ADC does DNAT (VIP <-> real server IP)	ADC does DNAT (VIP <-> real server IP)	ADC does DNAT and SNAT (VIP <-> real server IP, client IP <-> ADC)	ADC doesn't do NAT
When we use	Want to use same subnet for client-side and server-side	Common case when we can have separate VLAN/subnet for client-side and server-side.	Don't want to insert new VLAN/subnet between router and server.	Return traffic is huge and want to reduce load of ADC (ex streaming server)
comment	Current ADC device package doesn't support it.			APIC version 1.2

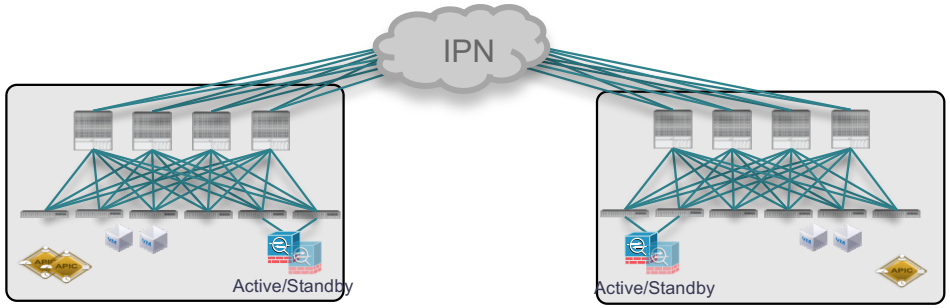
IPS Mode Options

	L1 (Fail-wire)	L2 (Transparent)	L3 (Routed)
			
Default GW of servers	Router	Router	IPS alias IP of server-side (in case of FirePOWER, active IP)
When to use	Want to insert IPS inline	Want to use same subnet for client-side and server-side	Common case when we can have separate VLAN/subnet for client-side and server-side.
comment	Firepower appliances support L1 bypass network modules		

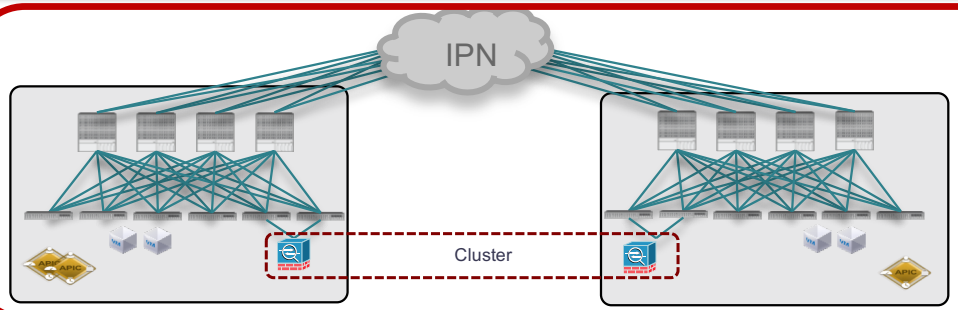
Что нового в ACI 3.2
FW Cluster Support across Pods



- Active and Standby pair deployed across Pods
- No issues with asymmetric flows



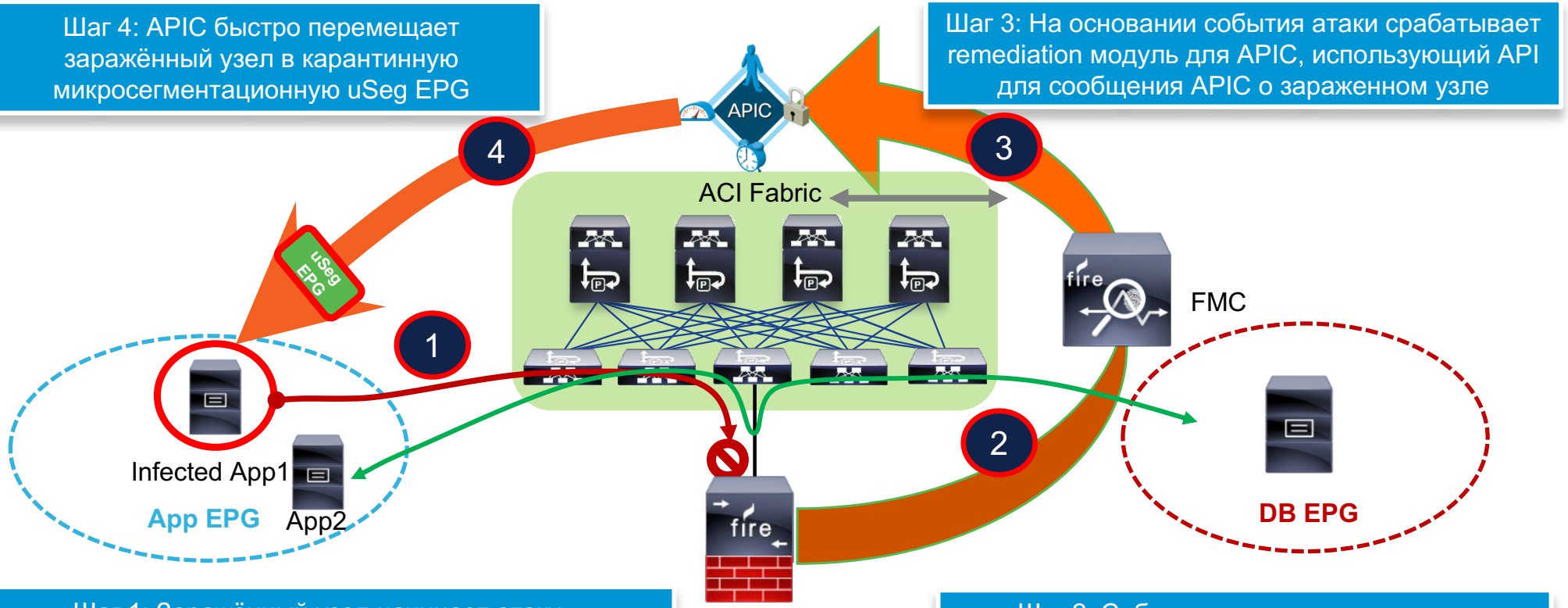
- Independent Active/Standby pairs deployed in separate Pods
- Need to avoid the creation of asymmetric paths crossing different active FW nodes



- **FW cluster deployed across Pods**
- **Supported from ACI release 3.2**
- **Requires the use of Service-Graph with PBR**

Интеграция FMC с APIC: Rapid Threat Containment

FMC Remediation Module для APIC

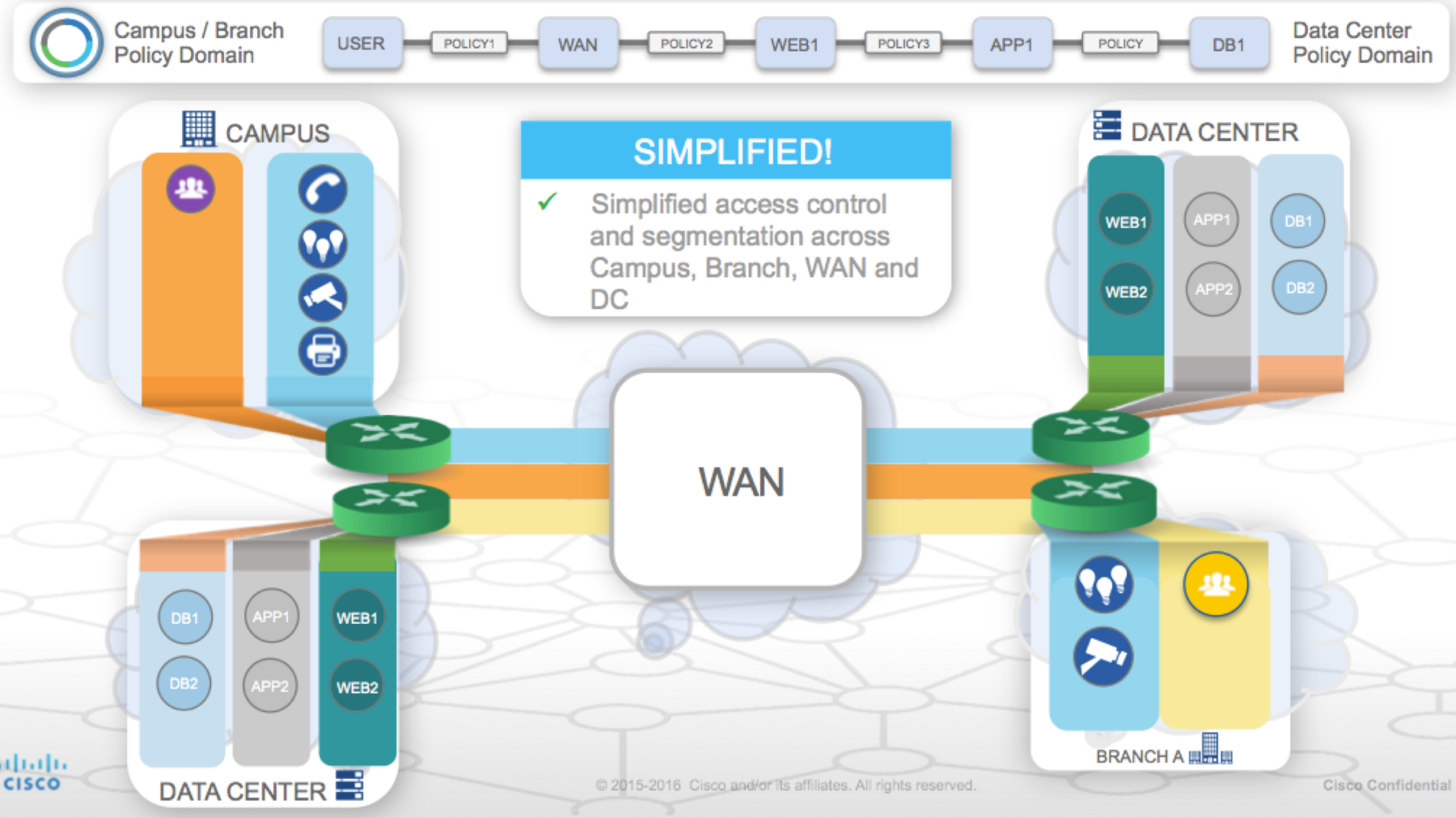


Security Certifications

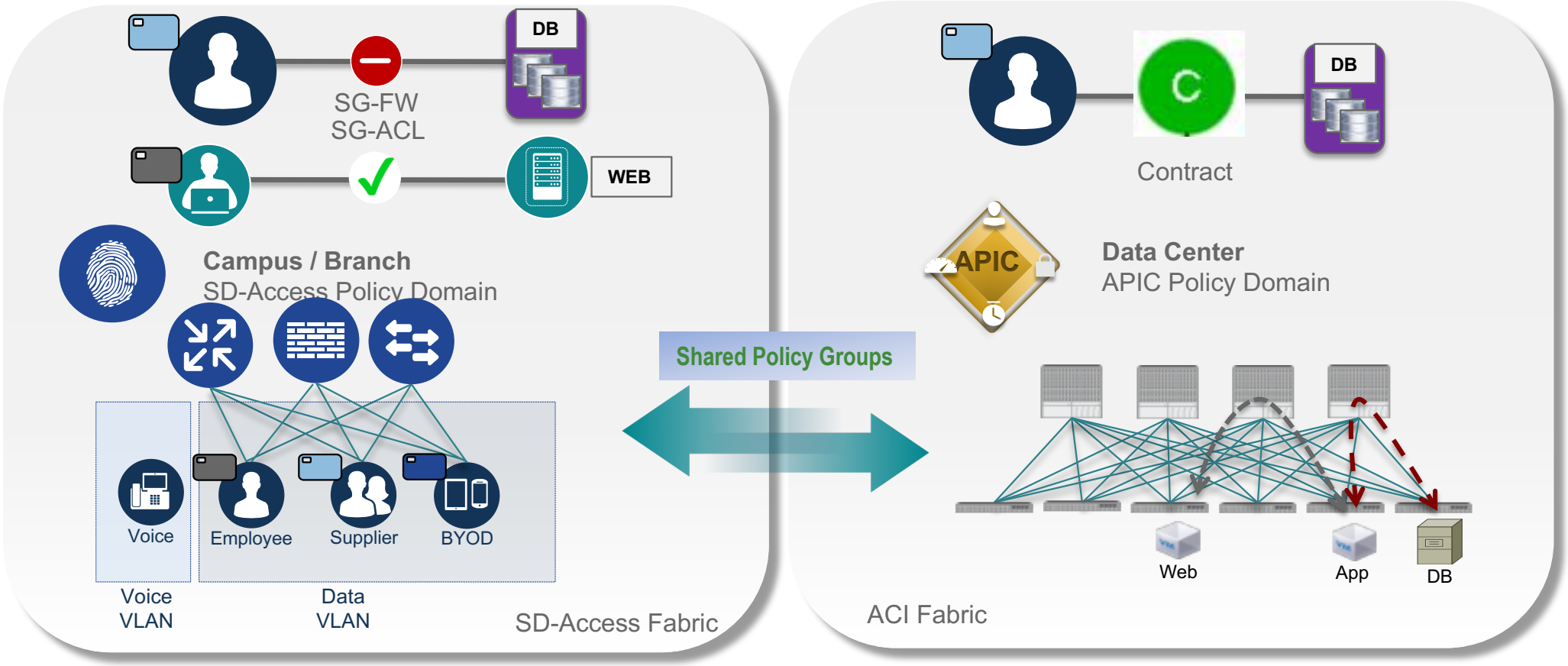
Certification	ACI
PCI Security Standards Council	Done
UC APL	Done
FIPS 140-2 CRYPTOGRAPHY	Done
Vulnerability Scanners • Nessus, Norad • Corona, AppScan	Done (Ran every release)
Common Criteria	Done

Fabric Integration

Campus, Branch, WAN and DC Integration

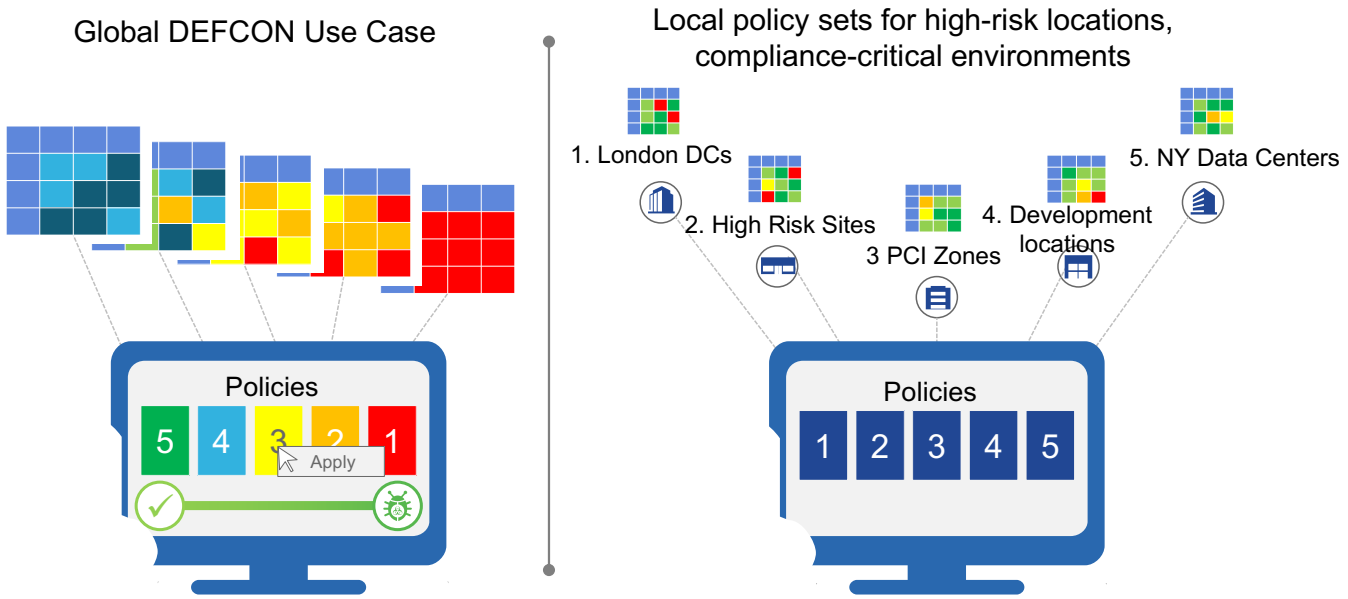


Enabling Group-based Policies in each Domain



Сегментация

Политики безопасности с учетом уровня угрозы



DEFCON (аббревиатура, англ. *DEFense readiness CONdition* — готовность обороны) — шкала готовности вооружённых сил Соединённых Штатов Америки. Стандартный протокол в мирное время — DEFCON 5. DEFCON 1 соответствует ожиданию немедленной полномасштабной атаки

Политики DefCon для сети

Multiple levels of policy sets
Applied globally

Standard Policy

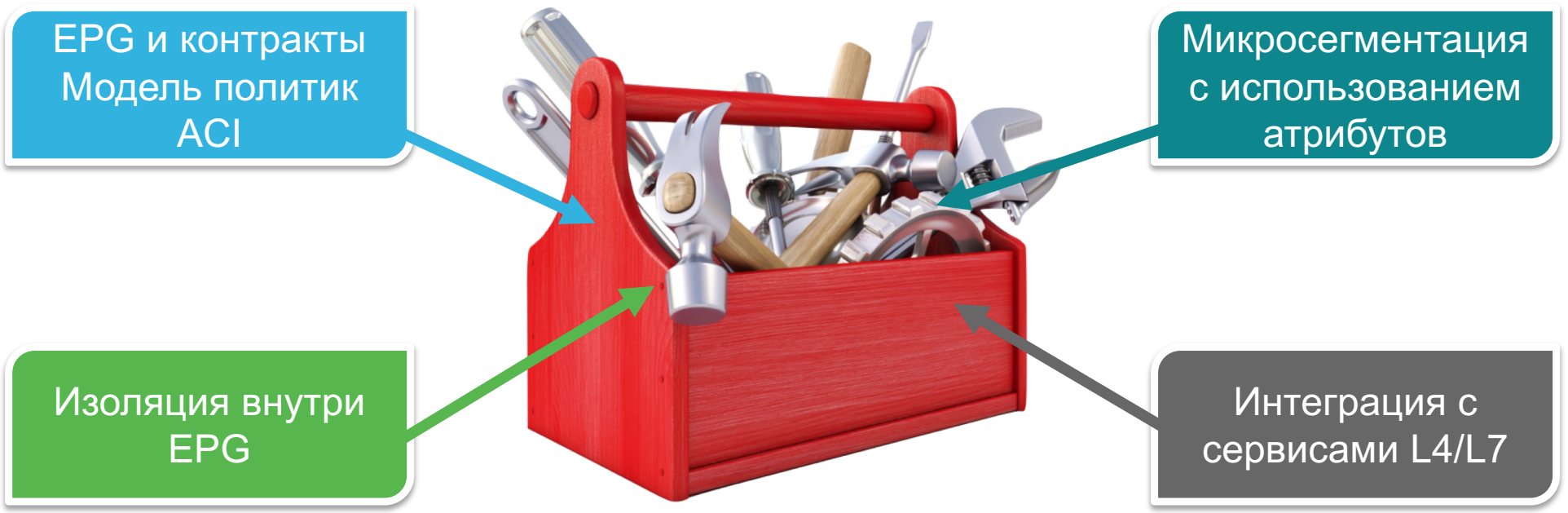
Source \ Destination	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	✓	–	–	–	–	✓	✓	–
LoB 2 Employee	–	✓	–	–	–	✓	–	✓
Partner 1	–	–	✓	–	–	✓	–	–
Partner 2	–	–	–	✓	–	✓	–	–
POS Terminal	–	–	–	–	✓	–	–	–

Ограничение распространения

DEFCON3 Policy

Source \ Destination	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	–	–	–	–	–	✓	✓	–
LoB 2 Employee	–	–	–	–	–	✓	–	✓
Partner 1	–	–	✓	–	–	–	–	–
Partner 2	–	–	–	✓	–	✓	–	–
POS Terminal	–	–	–	–	✓	–	–	–

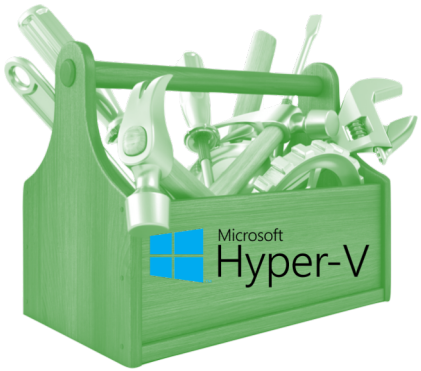
Инструментарий (микро)сегментации Cisco ACI



Для физических и виртуализованных серверов

Intra-EPG Изоляция:
- DVS
- AVS

µSeg EPG с Атрибутами:
- DVS
  9300-EX
- AVS

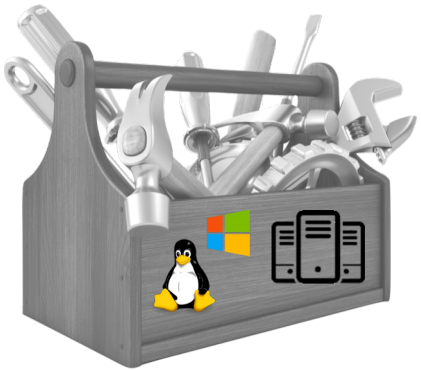


Intra-EPG Изоляция:
- Microsoft Virtual Switch

µSeg EPG с Атрибутами:
- Microsoft Virtual Switch

Intra-EPG Изоляция:
- Поддерживается

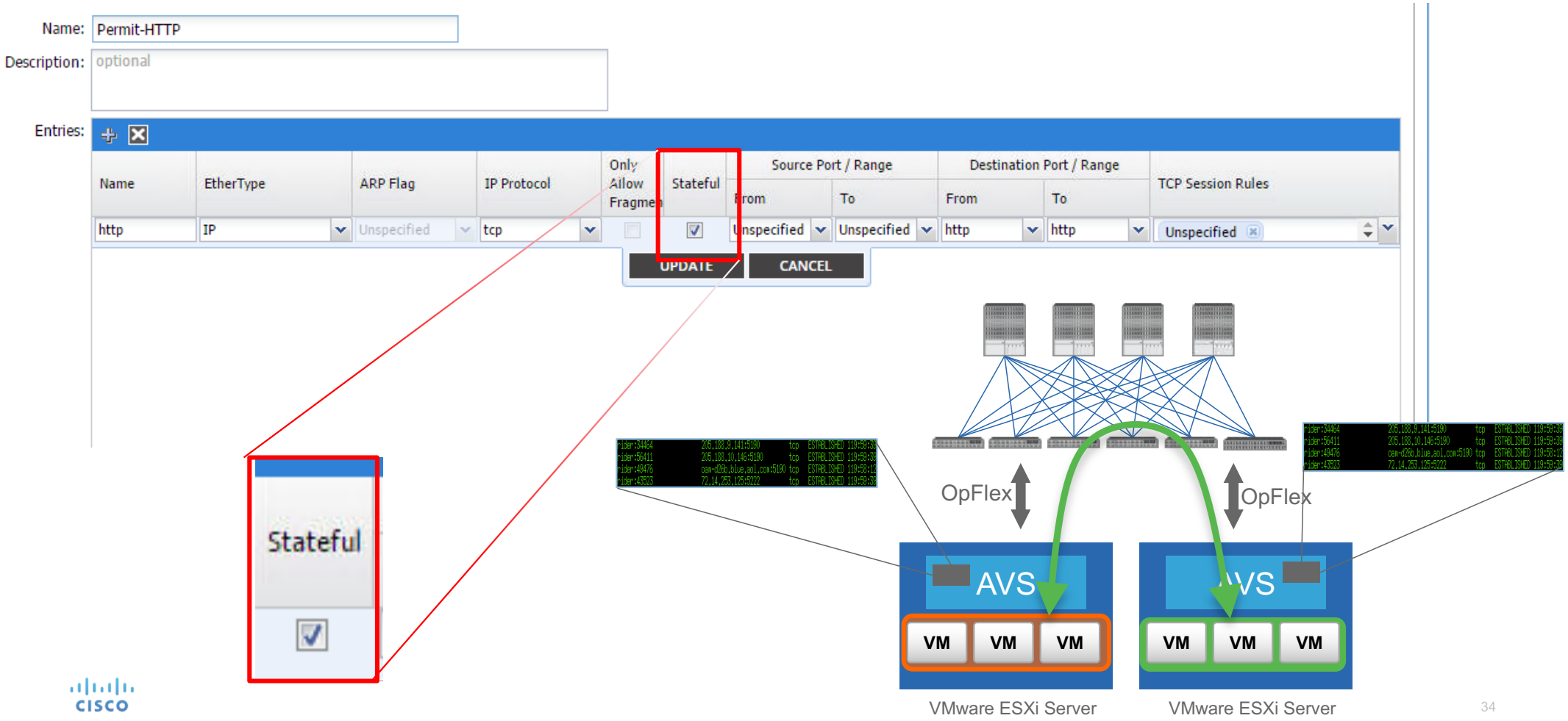
µSeg EPG с Атрибутами:
- Roadmap



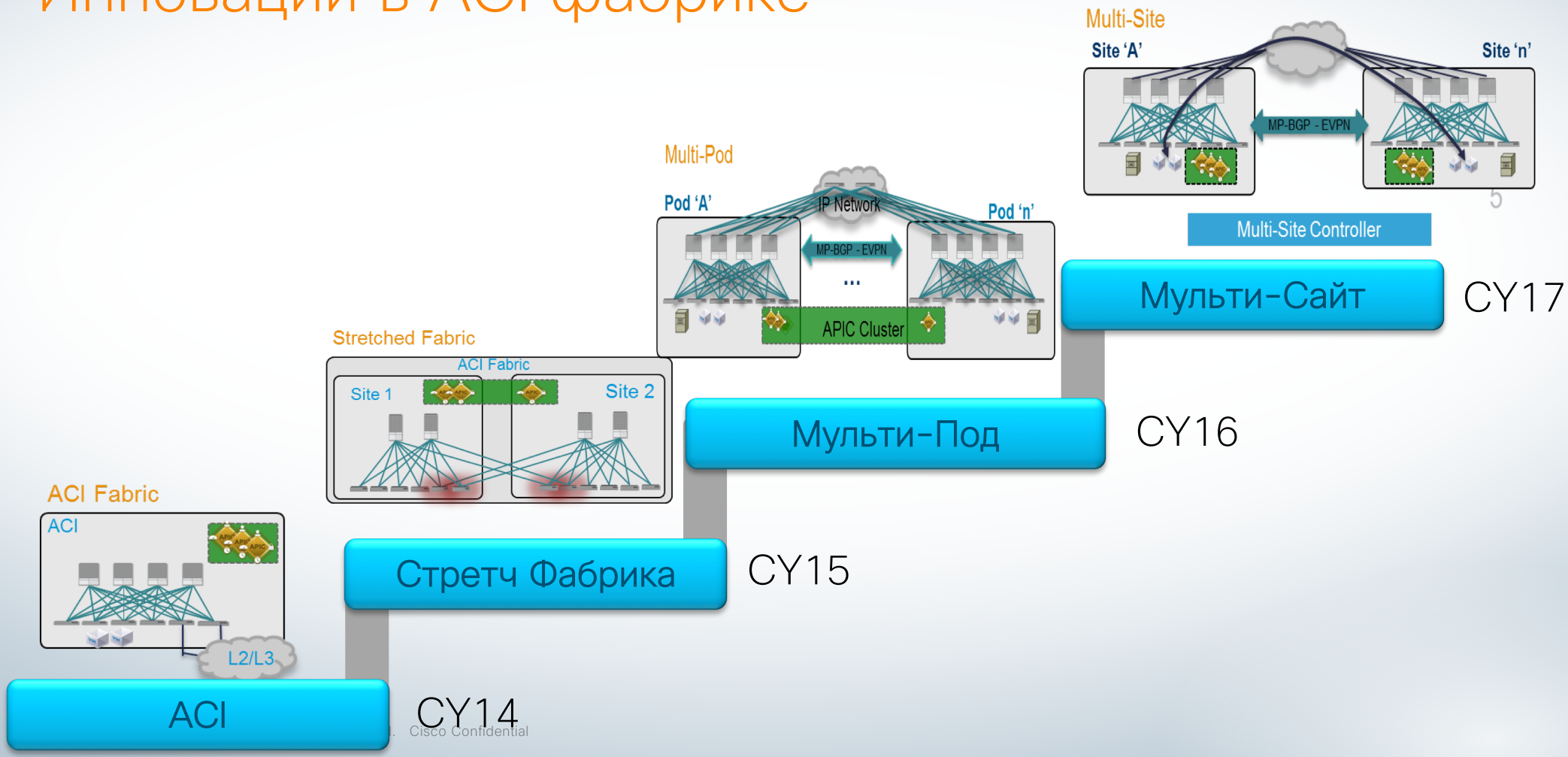
Intra-EPG Изоляция:
- Поддерживается

µSeg EPG с Атрибутами:
- IP EPG
  9300-EX
- MAC EPG планируется

ACI Stateful Distributed Firewall with AVS

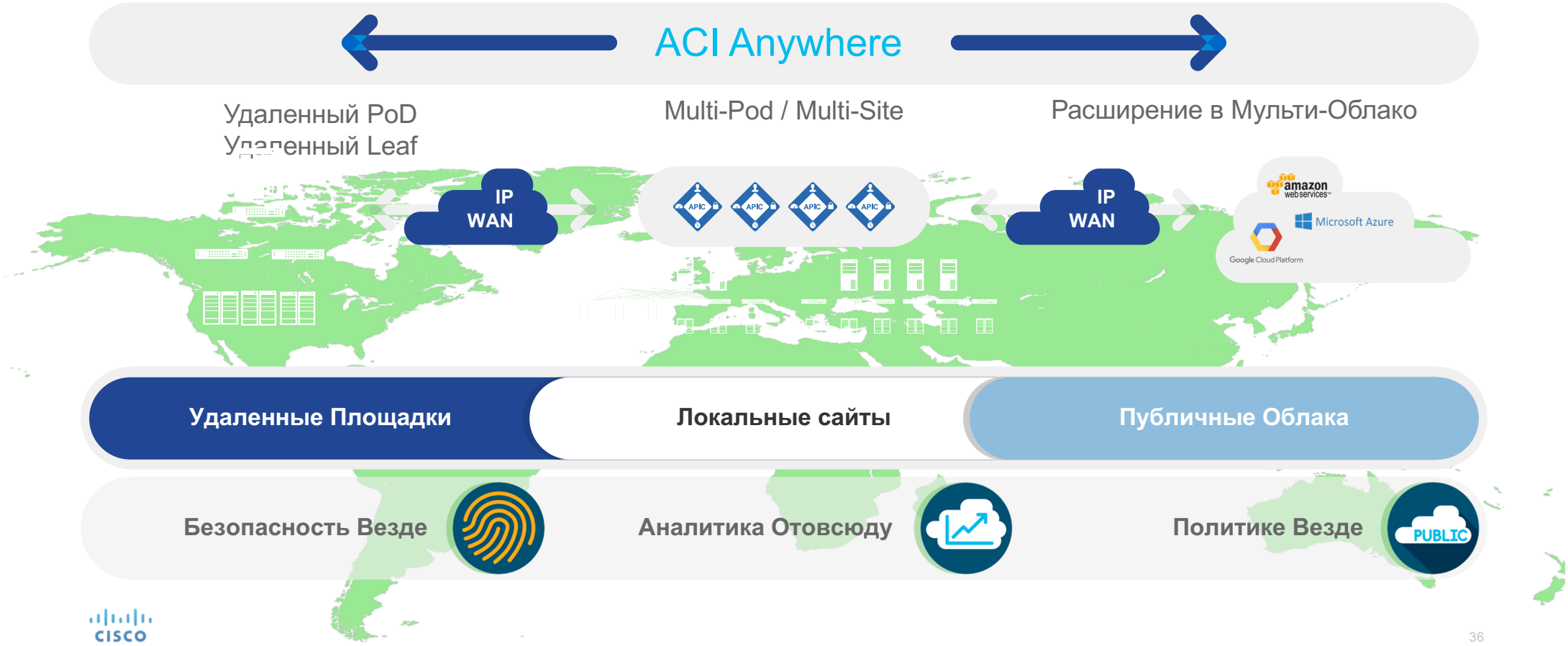


Инновации в ACI фабрике



ACI Vision

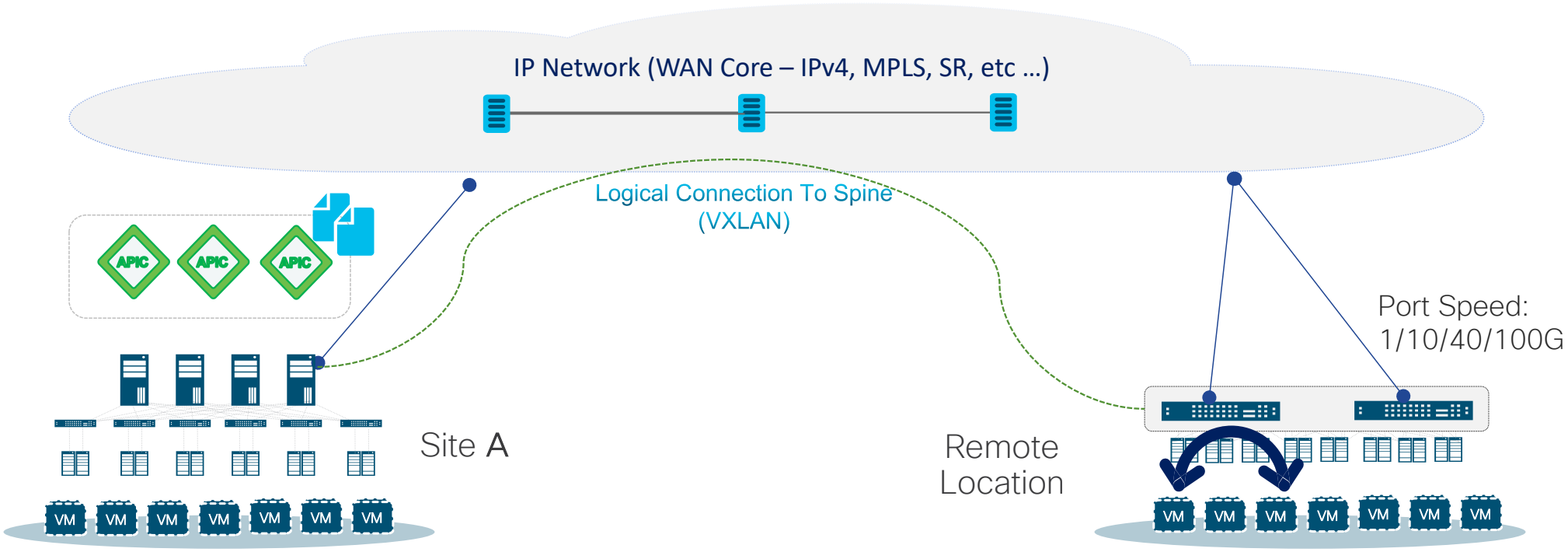
ONE Intent: Any Workload, Any Location, Any Cloud



Shipping Since Q1 CY '18

ACI: Physical Remote Leaf

Extend ACI to Satellite Data Centers



Zero Touch Auto Discovery of Remote Leaf

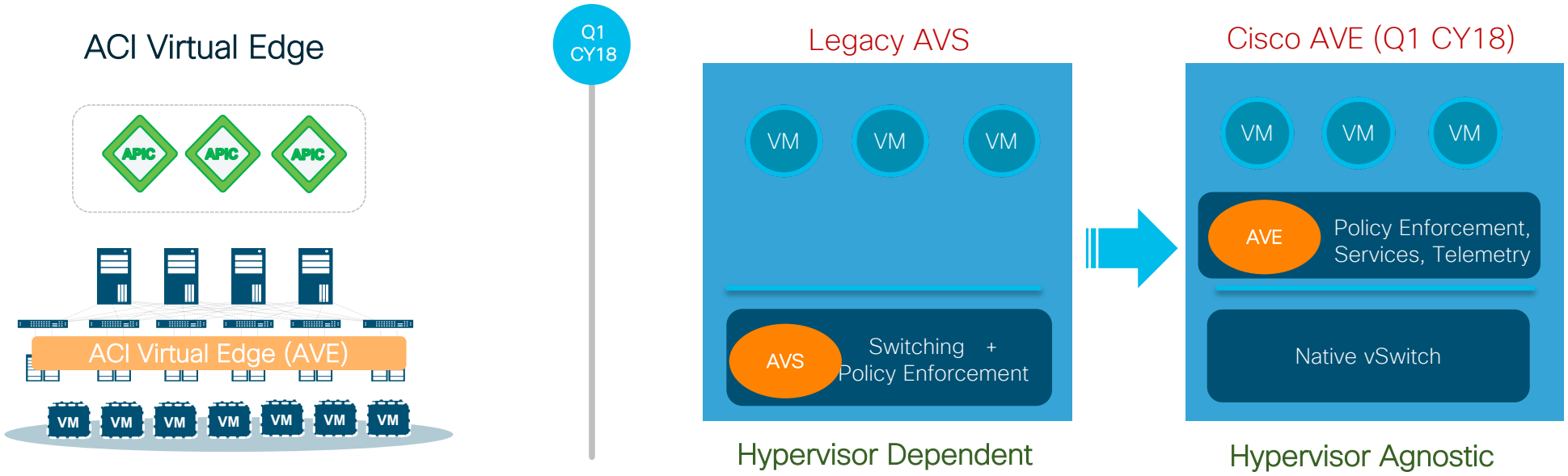
Pair Of Remote Leafs Per Location

Stretch EPG, BD, VRF, Tenant, Contract etc.

Visibility & Troubleshooting

Shipping Since Q1 CY '18

Cisco ACI Virtual Edge
Decoupled From Hypervisor Kernel API Dependencies



Next Generation of Cisco AVS

Distributed Firewall & Micro-segmentation

AVS/AVE Feature Parity

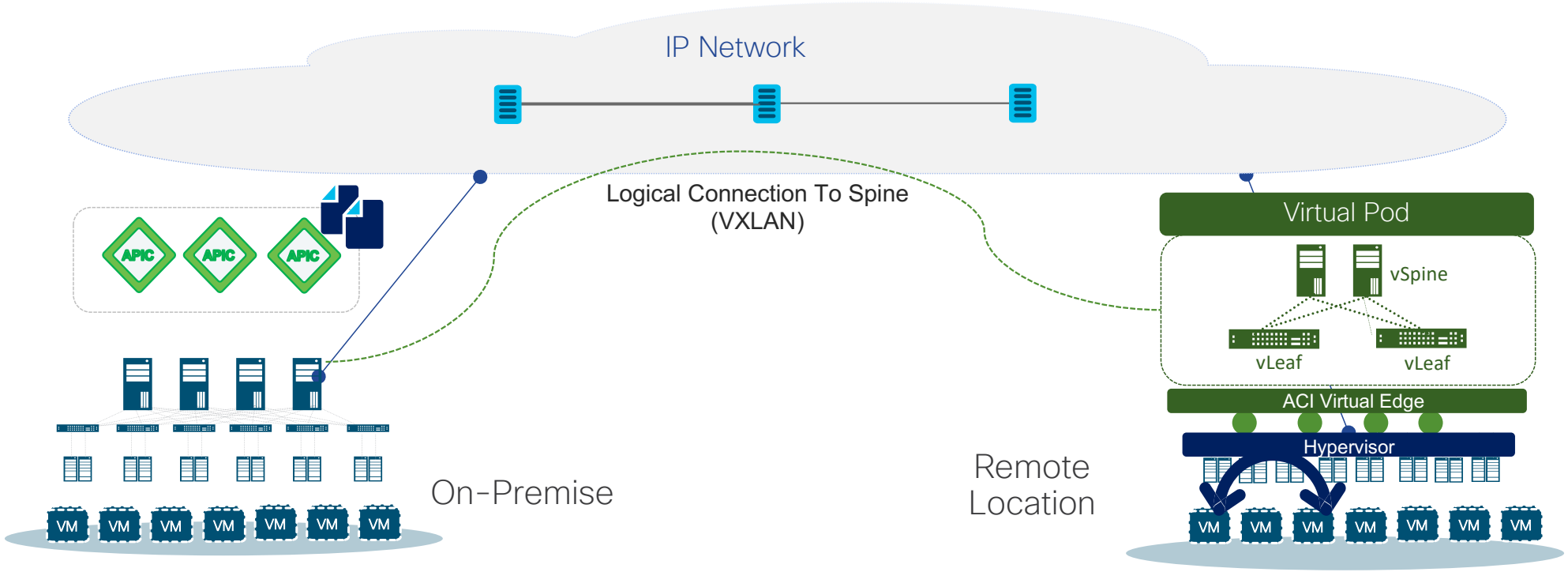
VXLAN Overlay

ACI: Virtual PoD

Extend ACI To Bare-metal Cloud

Beta: Q2 CY '18

GA: Q3 CY '18

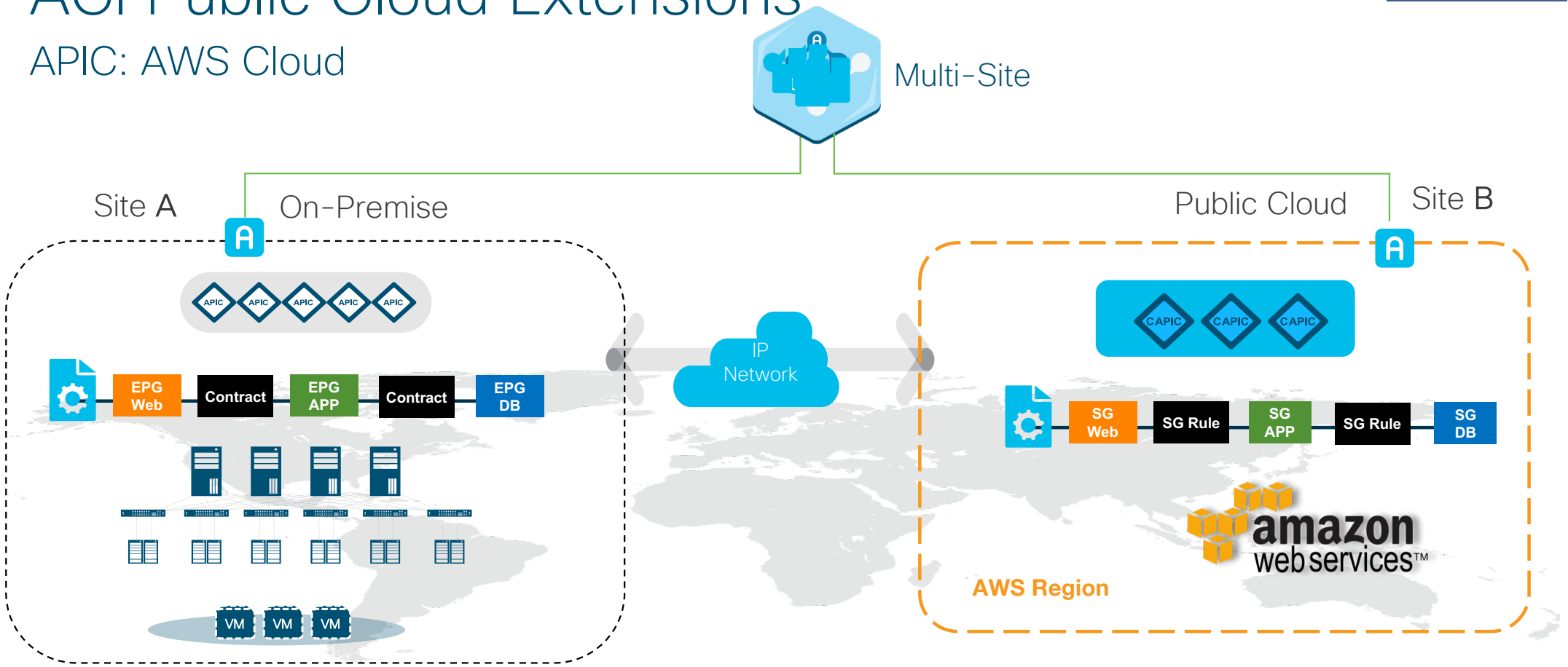


Bare Metal Clouds | Remote Data Centers | Colo Facilities | BrownField Deployments

ACI Public Cloud Extensions

APIC: AWS Cloud

Future

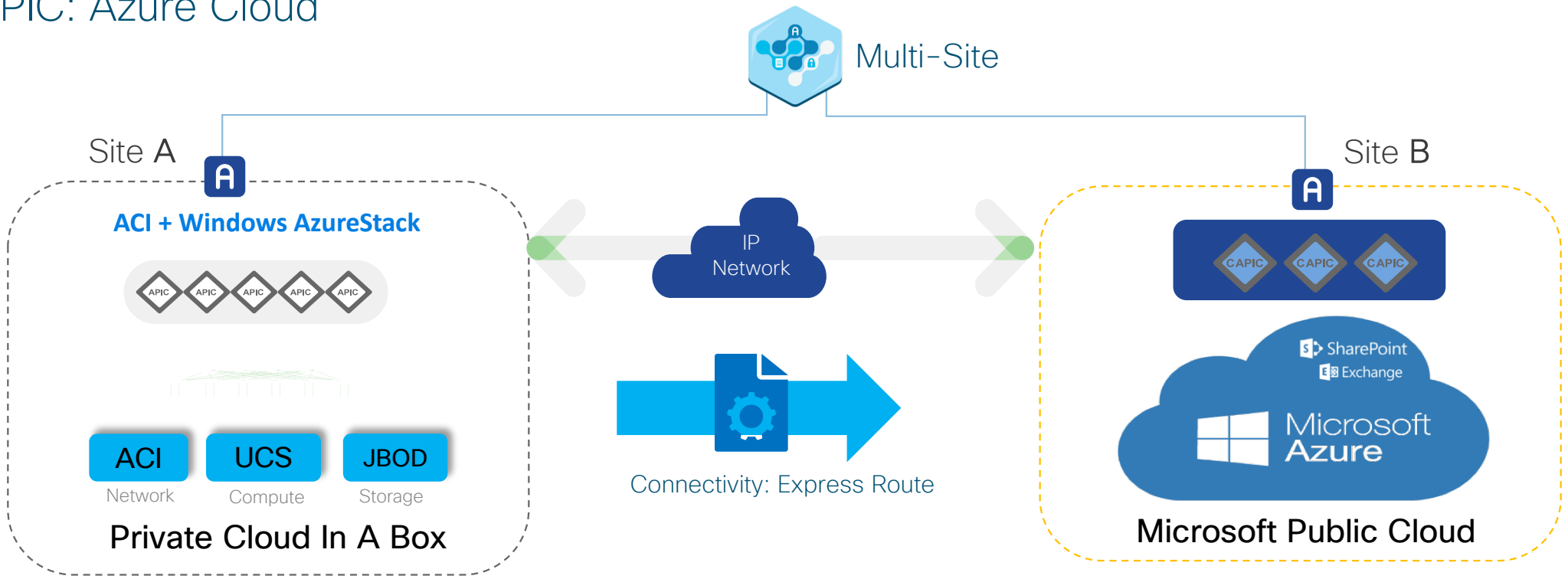


Common Governance | Discovery & Visibility | Policy Translation | Monitoring & Troubleshooting | Single Point Of Orchestration | Operational Consistency

Future

ACI Public Cloud Extensions

APIC: Azure Cloud



Azure Consistent Self-Service Portal Experience for Private & Public Cloud

Common Governance	Discovery	Policy Translation	Monitoring & Troubleshooting	Single Point Of Orchestration	Operational Consistency

ACI 3.2: Security

Connectivity

- PingFederate SSO and PingID 2-FA
- 64k scale ACI-SGT/IP binding scale
- 802.1x Multi-Domain/Host/Auth

Profiles

- Blacklist Contracts
- VM folder EPG

Services

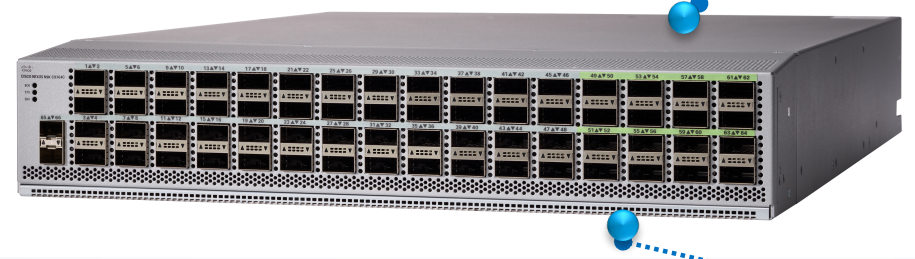
- Multisite L4-L7 Services
- Anycast MAC/IP for ASA Services
- Service Graph Wizard
- AVE L4-L7 routed mode

Nexus 9364C 64p 40/100G - ACI Фиксированный Spine

Идеально подходит для небольших фабрик

Поддержка смешанных конструкций Leaf 1-го и 2-го поколения

Поддержка смешанных 40/100G фабрик



100G линия MACSEC и VTEP-VTEP шифрования на 16 портах *

40 МБ интеллектуального буфера

Гибкие шаблоны TCAM
Маршруты 1M + IPv4

Маршрутизация VXLAN

QSFP28 - совместим с 40G QSFP +

Гибкая скорость
1,10,25,40,50,100G

6.4 Тб L2/3 ASIC

* future

Cisco Nexus 9000 Fixed 40/100G Switches

Nexus 9300

64p 40/100G QSFP
Nexus 9364C, NX-OS & ACI Spine

Shipping

32p 40/100G QSFP
Nexus 9332C, NX-OS & ACI Spine

Q2 CY18

Cisco Nexus 9300 Cloud Scale Access Switches

Q3 CY18

Nexus 9300 FX3

96p 1/10GT + 12p 40/100G QSFP
Nexus 93216TC-FX3, NX-OS/ACI Leaf

96p 10/25G SFP + 12p 40/100G QSFP
Nexus 93360YC-FX3, NX-OS/ACI Leaf

Shipping

Nexus 9300 FX2

48p 10/25G SFP + 12p 40/100G QSFP
Nexus 93240YC-FX2, NX-OS Leaf

36p 40/100G QSFP
Nexus 9336C-FX2, NX-OS/ACI Leaf

Shipping

Nexus 9300 FX

48p 100M/1GT + 4p 10/25G SFP + 2p 40/100G QSFP
Nexus 9348GC-FXP, NX-OS/ACI Leaf

48p 1/10GT + 6p 40/100G QSFP
Nexus 93108TC-FX, NX-OS/ACI Leaf

48p 10/25G SFP + 6p 40/100G QSFP
Nexus 93180YC-FX, NX-OS/ACI Leaf

Shipping

Nexus 9300 EX

48p 1/10GT + 6p 40/100G QSFP
Nexus 93108TC-EX, NX-OS/ACI Leaf

48p 10/25G SFP + 6p 40/100G QSFP
Nexus 93180YC-EX, NX-OS/ACI Leaf

32p QSFP
32p 40/50G | 24p 40G + 6p 100G
28p 40G + 4p 100G | 18p 100G
Nexus 93180LC-EX, NX-OS/ACI Leaf

Nexus 9348GC-FXP

ACI Leaf: 48p 100M/1G, 4p 10/25G, 2p 40/100G

Два блока питания

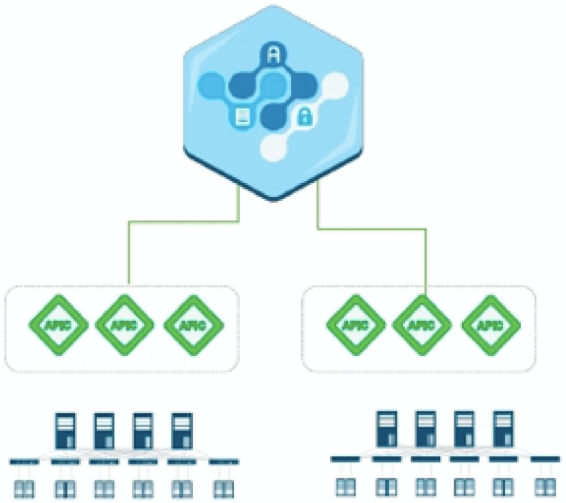
- Приложение для Gigabit Ethernet
- Ширина полосы пропускания
  696 Гбит/с
  250 Mpps

Гибкие скорости 100M, 1,10, 25, 40,100G

L2/L3 ASIC

40 MB 40 МБ интеллектуального буфера

ACI Multi-Site
Futures



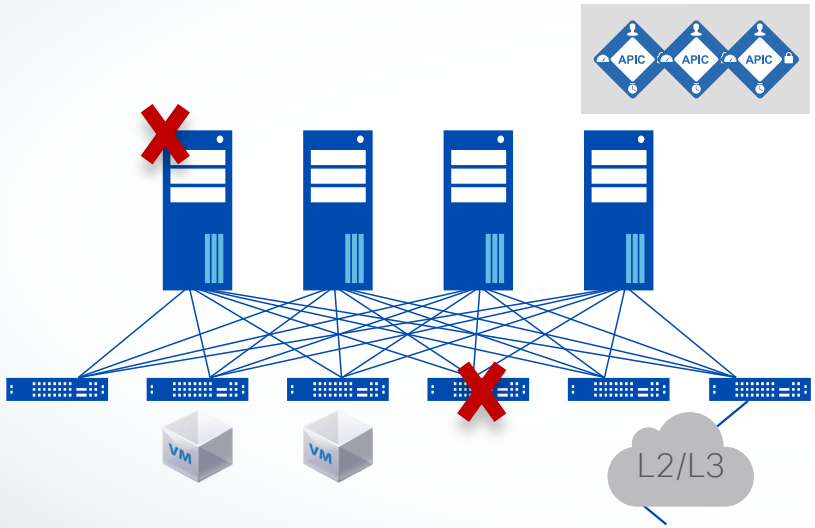
ACI 3.1 Release

- Nexus 9364C (Fixed Spine)
- Multi-Site Health Check
- External Authentication
- Audit / Accounting Logs
- Shared Golf
- Up To 8 Sites, 800 Leafs

ACI 3.2 Release

- Multi-Site + Multi-Pod
- L4-L7 Services Support
- Spine-Spine (Dark Fiber)
- Consistency Checker (Multi-Site, APIC, HW)
- UCS-D Orchestration (6.6)
- Up To 10 Sites

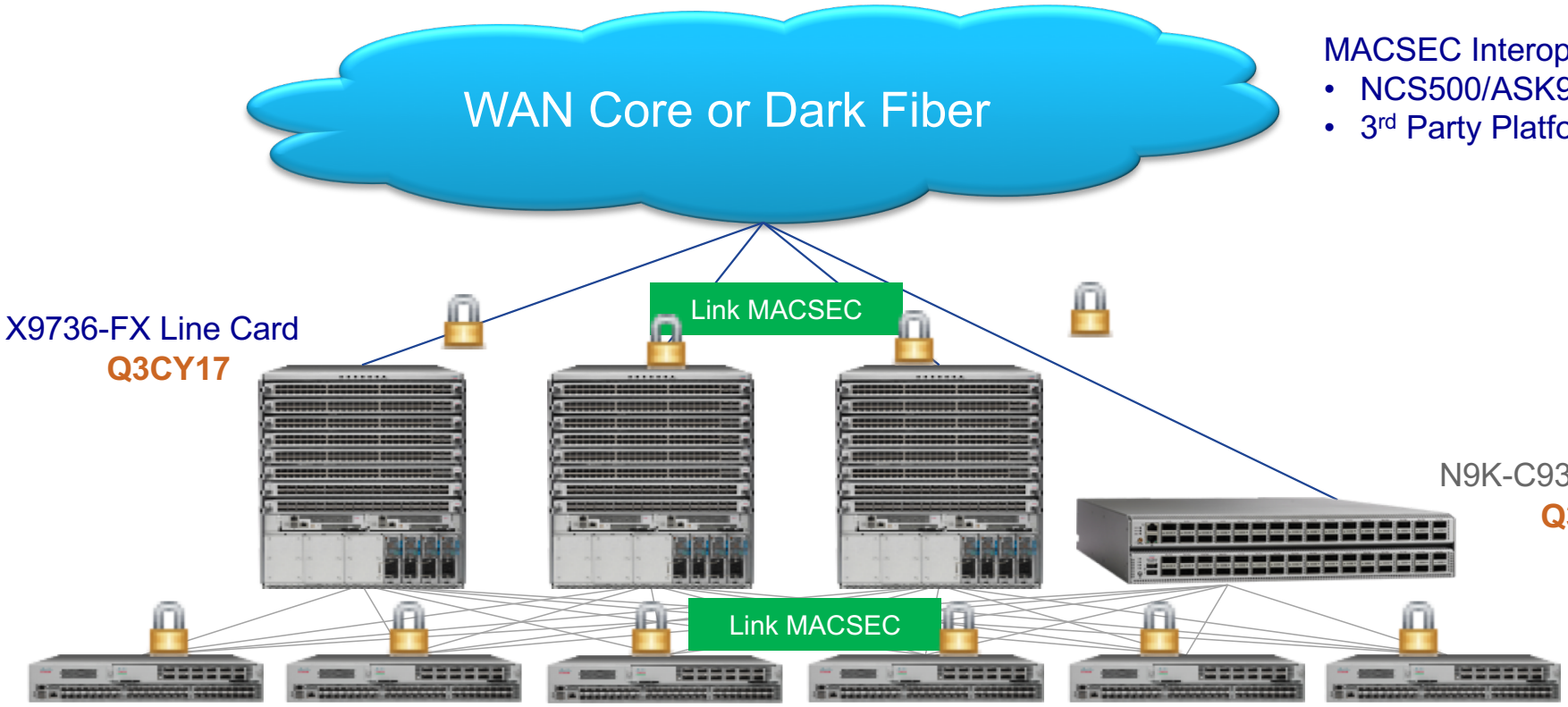
Упрощенная вставка и удаление (GIR)



1. Де-комиссия узела от фабрики
2. Устранение проблем
3. Ре-комиссия узла

GIR перенаправляет трафик данных на альтернативные пути и позволяет устранять неполадки, обслуживание и обновление узла.

Nexus 9000 MACSEC Encryption Portfolio



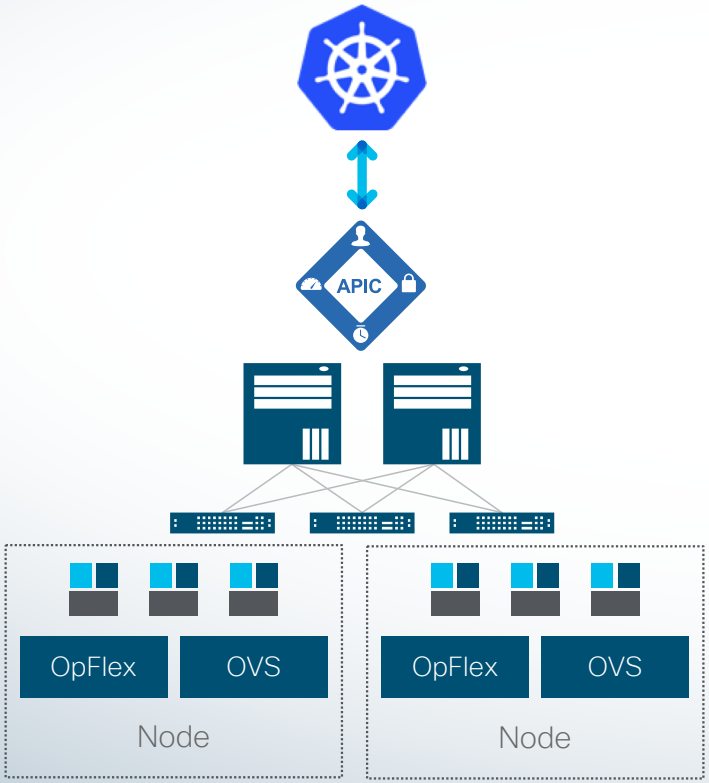
MACSEC Interoperability
- NCS500/ASK9K
- 3rd Party Platforms

X9736-FX Line Card
Q3CY17

N9K-C9364C Switch
Q3CY17

Nexus 9300-FX Access Series **Mid CY17**

Интеграция Контейнеров



ACI и Контейнеры

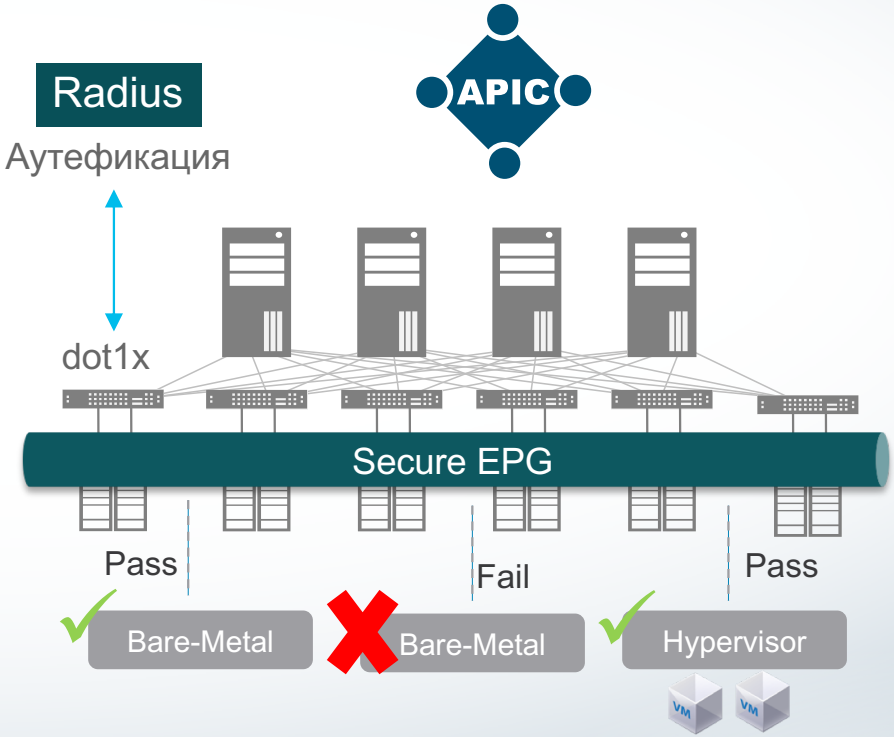
Унифицированная сеть: «Контейнеры, виртуальные машины и физические сервера

Интеграция сетевых политик Kubernetes и политик ACI

Видимость: статистика в реальном времени в APIC для каждого контейнера и показатели здоровья

Zero Trust Security
Dot1X Аутентификация

- ✓ End Point Аутентификация для классификации EPG
- ACI 3.0 — Поддерживается только на физических хостах
- ACI 3.0 — Поддержка на ‘-EX’ и ‘-FX’
- Развитие — Гипервизоры и Контейнеры



Функции безопасности первого хопа

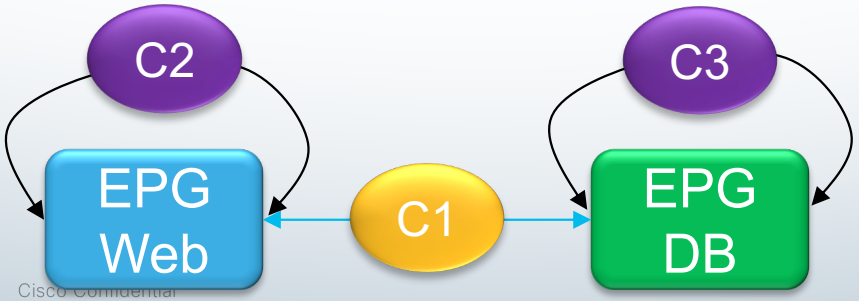
- 5 поддерживаемых функций IPv4/v6
  - Уровень BD
    1. DHCP Snooping/Inspection
    2. Dynamic ARP/ND Inspection
    3. IP Source Guard
    4. RA Guard v6
  - Уровень EPG
    1. Trusted EPG
- FHS политики только для Leaf
- ACI 3.0 поддерживает только PhyDoms
- VMM поддержка в будущем

2-х факторная аутентификация

- Внешняя аутентификация APIC
  - SAML
  - IDP support Microsoft ADFS and Okta
- Локальная аутентификация APIC
  - TOTP используя Google Authenticator для 2ro фактора pin/баркод

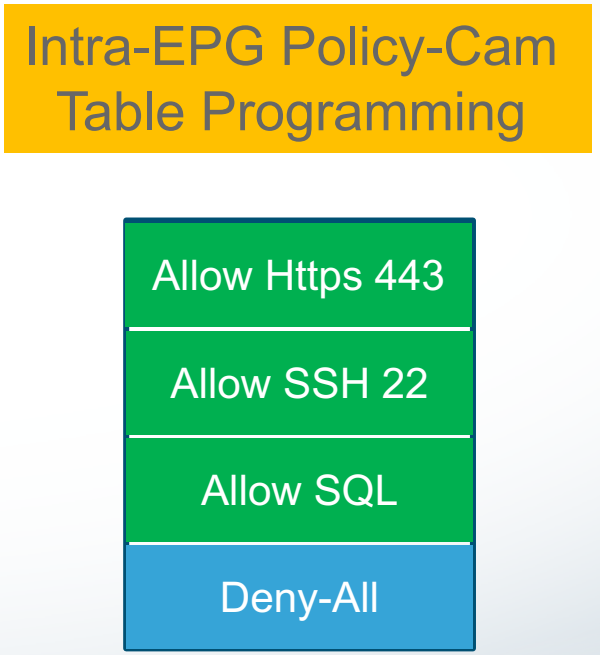
Контракты внутри EPG

- ACI 3.0 поддерживает“Intra-EPG Контракты”
  - Позволяет использовать политики «белого» трафика внутри EPG
  - Может сосуществовать с контрактами между EPG
  - Устраняет необходимость создания микро-EPG или развертывания внешних FW для сегментации внутри EPG
  - Применяется на Leaf (EX или выше)
  - Поддерживается для VMWare vDS и Физических серверов

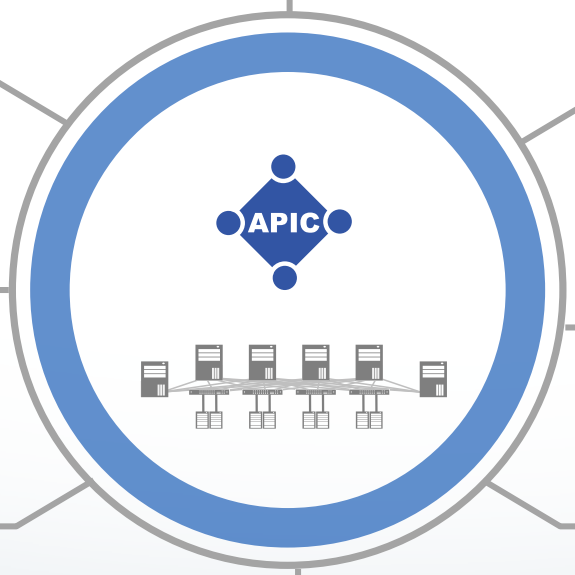


Реализация контракта Intra-EPG

- vDS реализация:
  - Intra-EPG Isolation + Contract allow rules (PVLAN + Proxy-ARP + Deny-All + Allow rule)
- Физические хосты:
  - Intra-EPG Isolation + Contract allow rules (Proxy-ARP + Deny-All + Allow rule)



Улучшение Масштабируемости



Layer-3
50 VRFs Per Tenant , 1k Ips/MAC

Leafs
До 400 на Фабрику
8 Border Leafs per L3 Out

Tenants
До 3000

EPGs
До 15000
До1k L3 EPGs/EX-Leaf
4k L3 EPGs for one tenant
и one context
250 Isolated EPGs

FEX
До 650 / Fabric
До 20 / Leaf

Bridge Domains
До 21,000 (L2), 15,000 (L3)
До 1750 Bridge Domains/VRF
3967 VLANs per leaf
3967 VLANs + BDs

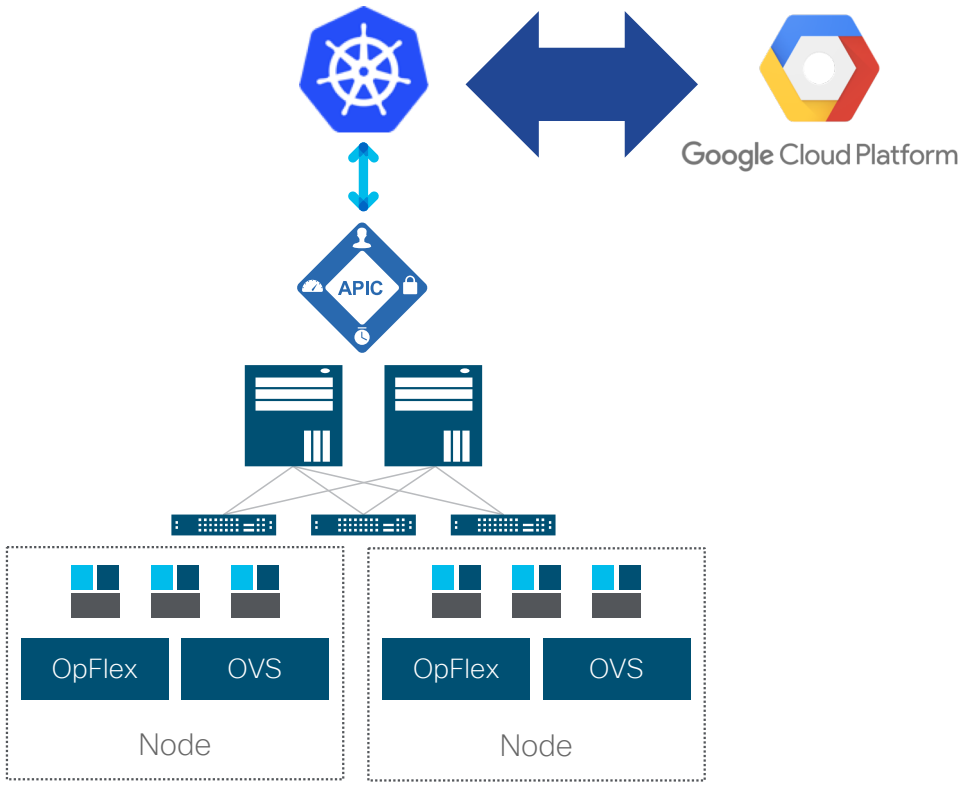
Multicast Groups
До 8,000 (S,G) routes with
Convergence of 5 seconds

Other
До 200 vCenters
До 2,000 Contracts
До 61k TCAM Rules
500 Service Graphs Per Cluster
До 12 Pods in Multi-Pod

Future

ACI Public Cloud Extensions

Google Cloud : Kubernetes Integration



ACI and Containers

Unified networking: Containers, VMs, and bare-metal

Integration of Kubernetes network policies and ACI policies

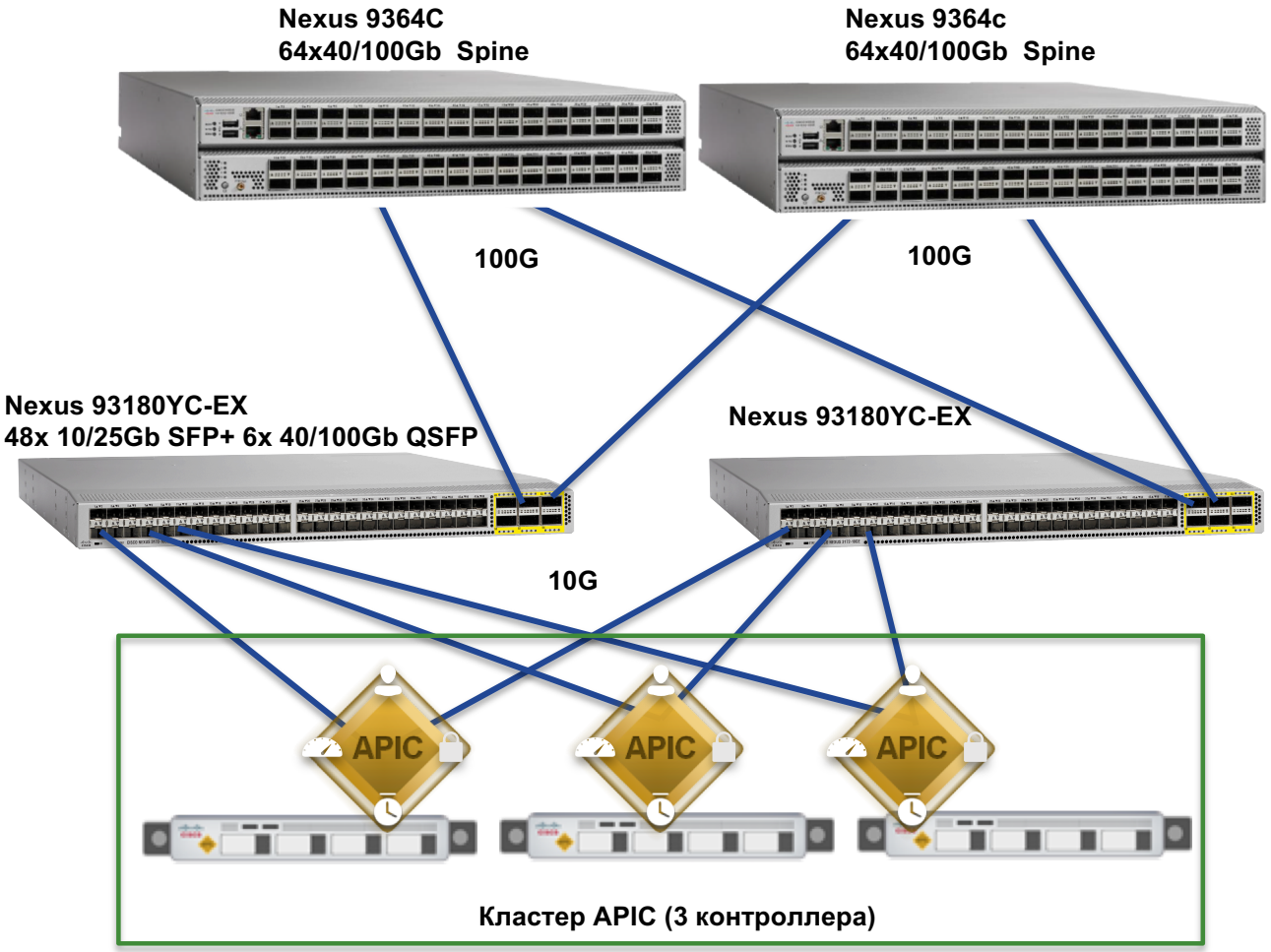
Visibility: Live statistics in APIC per container and health metrics

Эволюция Сети ACI

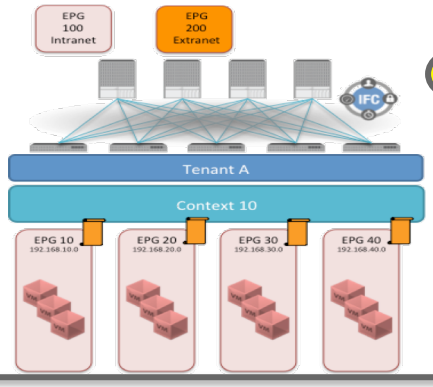
	ACI 1.0(2m)	ACI 1.2(1i)	ACI 2.0(1m)	ACI 2.2	ACI 3.0 Target
Leafs per APIC Cluster	50	200	200	400	800 (with msite)
Tenants	50	3k	3k	3k	3k
Contracts/Filters	1k/10k	1k/10k	1k/10k	2k/10k	2k/10k
Policy CAM per Leaf	4k	32k	32k	61k	61k
EPGs/Endpoints	4k/100k	15k/180k	15k/180k	15k/180k	15k/180k
vCenters per Fabric	5	10	50	200	200
Number of PODs in Multi-POD	-	-	4	6	12
Number of Sites	-	-	-	-	4

С чего можно начать?
Минимальная конфигурация инфраструктуры ACI

GPL
$194k

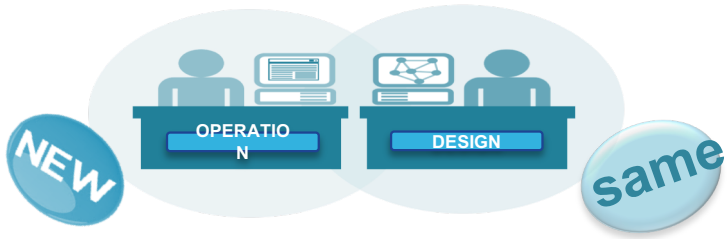


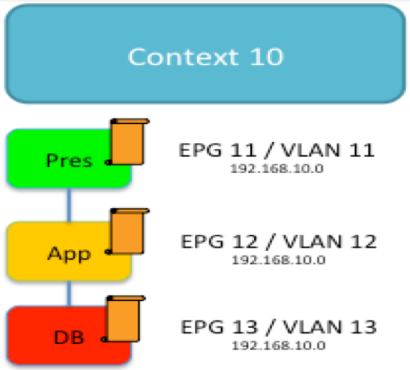
Миграция в новую модель EPG



1

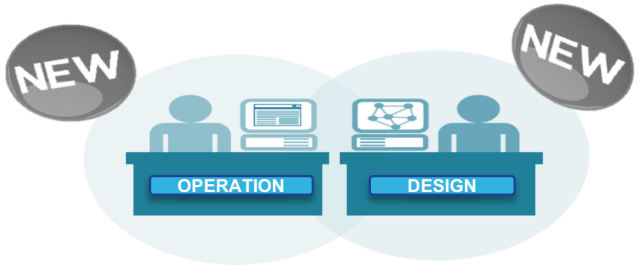
VLAN / Подсети в EPG

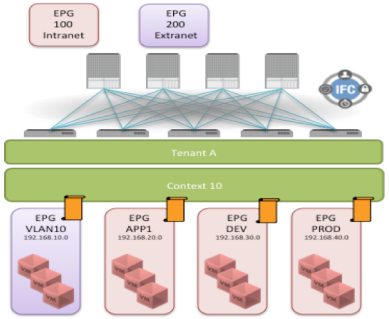




2

Знания о Приложениях/ Безопасность/ Жизненный цикл…



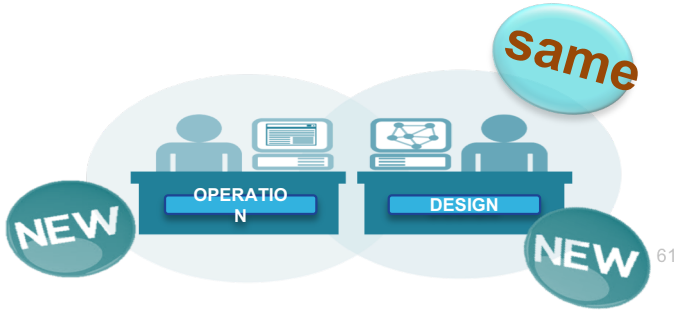


3

VLAN / Подсети в EPG

Гибридный дизайн

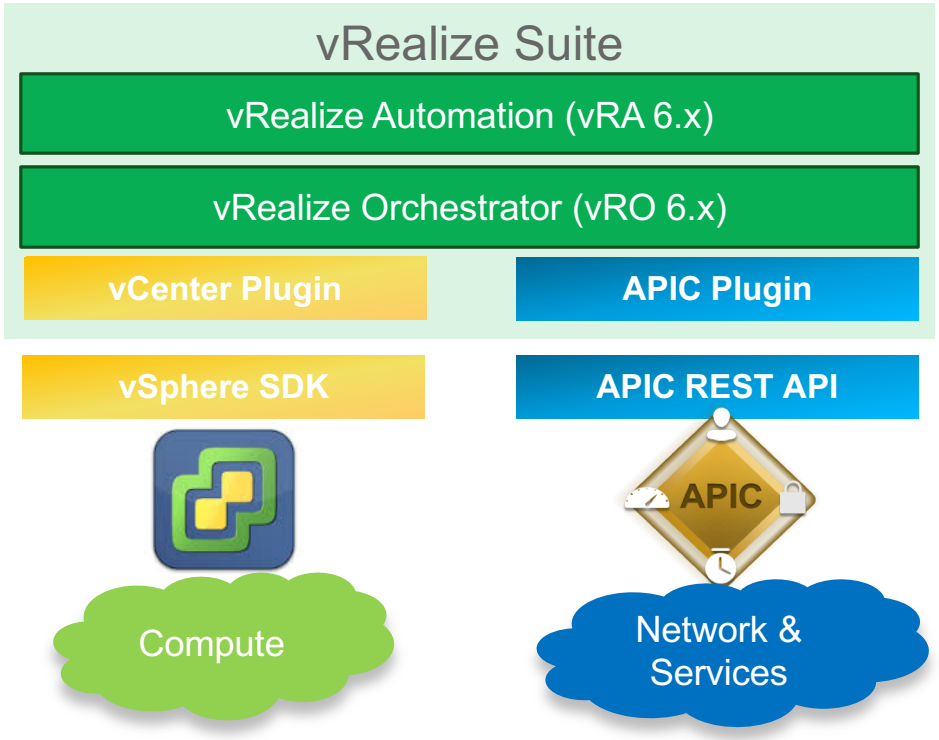
Знания о Приложениях/ Безопасность/ Жизненный цикл…



Облачная автоматизация - ACI с vRealize

Интеграция ACI с vRealize для внедрений под vSphere

С релиза 1.2



Day Zero Operations

Инициализация фабрики

Развёртывание инфраструктуры

Домены безопасности

Day 1/ Day 2 Operations

Shared Services Plans

Virtual Private Cloud

Сети, подсети, безопасность

ACI Policy Driven vRealize Automation Blueprints to Accelerate Application Deployment

Интеграция решений Microsoft и ACI
Два режима интеграции

Интеграция с SCVMM

- Управление политиками: посредством APIC
- Software / License: Windows Server с HyperV, SCVMM
- Обнаружение виртуальных машин: OpFlex
- Инкапсуляция: VLAN, NVGRE (План)
- Установка plugin-а: в ручную

Интеграция с Azure Pack

- Расширение возможностей SCVMM
- Управление политиками: посредством APIC или через Azure Pack
- Software / License: Windows Server с HyperV, SCVMM, Azure Pack (бесплатно)
- Обнаружение виртуальных машин: OpFlex
- Инкапсуляция: VLAN, NVGRE (План)
- Установка plugin-а: интегрирована

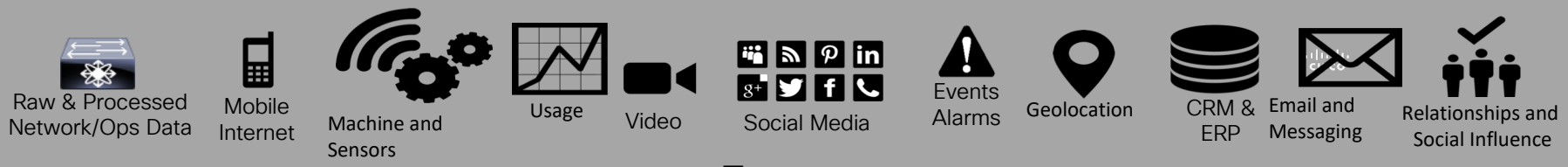
Cisco Tetration Analytics

Аналитика позволяет принимать правильные решения

Объяснить	Диагностировать	Предсказать	Подсказать
Что происходит?	Почему это произошло?	Что скорее всего может произойти?	Что следует делать по этому поводу?

Анализ

Технологии Больших Данных
собрать, объединить, обработать, обобщить, визуализировать



Данные

Это аналитическая платформа на базе машинного самообучения

Она может использоваться разными департаментами, для разных целей.

Приложения и автоматизация политик

Традиционный

1. Нанять консультанта
2. Собрать логи, побеседовать с командами …
3. Выявить зависимости приложения
4. Проверить с каждой группой пользователей
5. Статичная карта, запросы на изменения
6. Применить политику, убедиться, что приложения после этого работают

Стоимость $1M-$5M; несколько мес

TETRATION

Разворачивается за несколько часов; автоматически предложенная политика на основе данных в реальном времени менее чем через неделю

Возможность промоделировать результат применения политики на реальном историческом трафике до внедрения

70% сокращения расходов и времени (Cisco IT)

Tetration Analytics: варианты развертывания

Варианты размещения на месте

Cisco Tetration Analytics (Large Form Factor)

- Подходит для внедрений с более чем 1000 серверов
- Встроенная отказоустойчивость
- Масштабируется до 10 000 серверов

Включает в себя:

- 36 серверов UCS C-220
- 3 коммутатора Nexus 9300

Cisco Tetration-M (Small Form Factor)

- Подходит для внедрений с не более чем 1000 серверов

Включает в себя:

- 6 серверов UCS C-220
- 2 коммутатора Nexus 9300

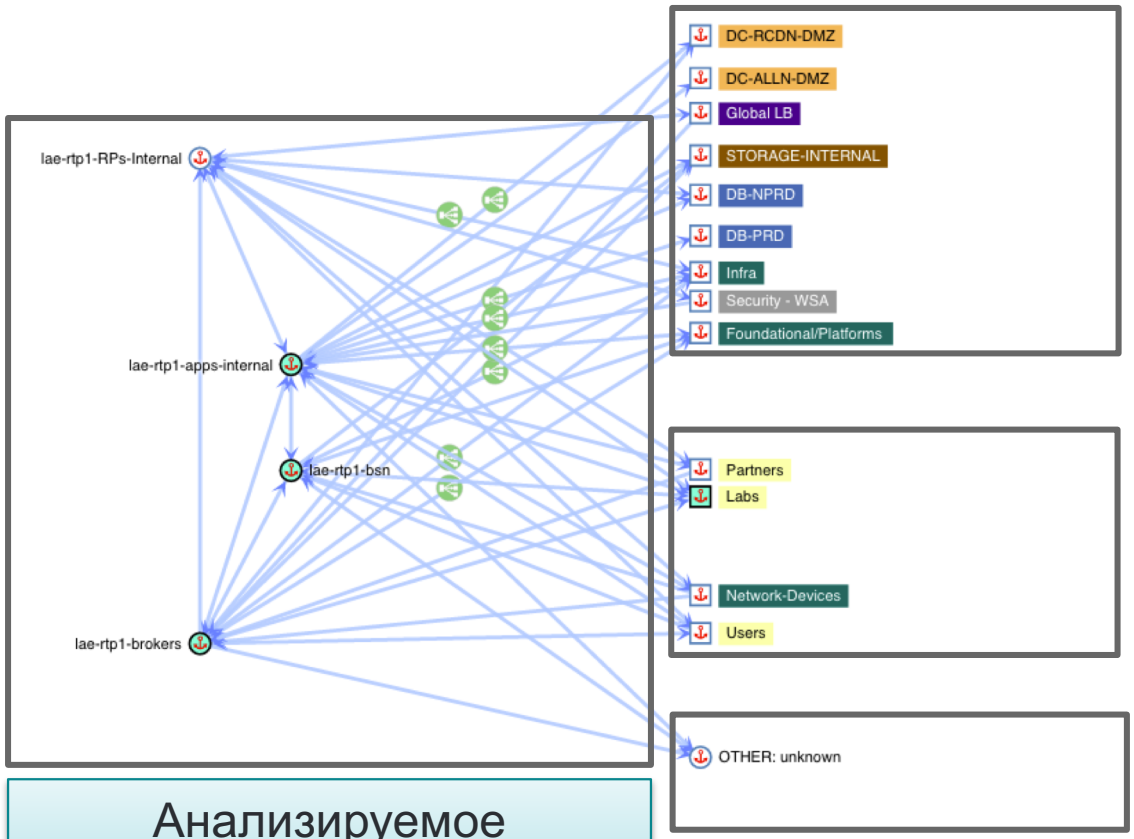
В публичном облаке

Cisco Tetration Cloud

- Платформа располагается в облаке Amazon AWS
- Подходит для внедрений с менее чем 1000 серверов
- Ресурсы используемые в облаке AWS принадлежат заказчику

amazon web services

Обзор зависимостей - с точки зрения потоков



Анализируемое приложение

Потоки к другим приложениям (внутри ЦОД)

Потоки в пределах внутренней сети

Потоки в / из Интернета

Практические примеры использования

- Высокая наглядность
  - Миграция ЦОД
  - Переход на услуги предоставляемые из облака
  - Слияния, поглощения и отчуждения
- Безопасность
  - Микросегментация с контролем применения
  - Проверка соответствия
  - Изоляция устаревших приложений
- Поиск
  - Проверка потоков

Картографирование зависимостей приложений

Автоматическое создание политик «белого списка»

Проверка соответствия политиками и моделирование

Расследование событий (пример: поиск потока и аномалии потока)

Обеспечение соблюдения политик

Cisco Tetration Analytics™

Real-time Network Analytics for Your Data Center

200x
faster application behavior insight

10s of Billions
of events searchable in seconds

100%
visibility across every packet

70%
higher operational efficiency

5x
reduction in attack surface

0
trust operational model

Learn more at www.cisco.com/go/tetration

С помощью Cisco ACI вы можете создать лучшую сеть ...

anywhere.

Thank you.