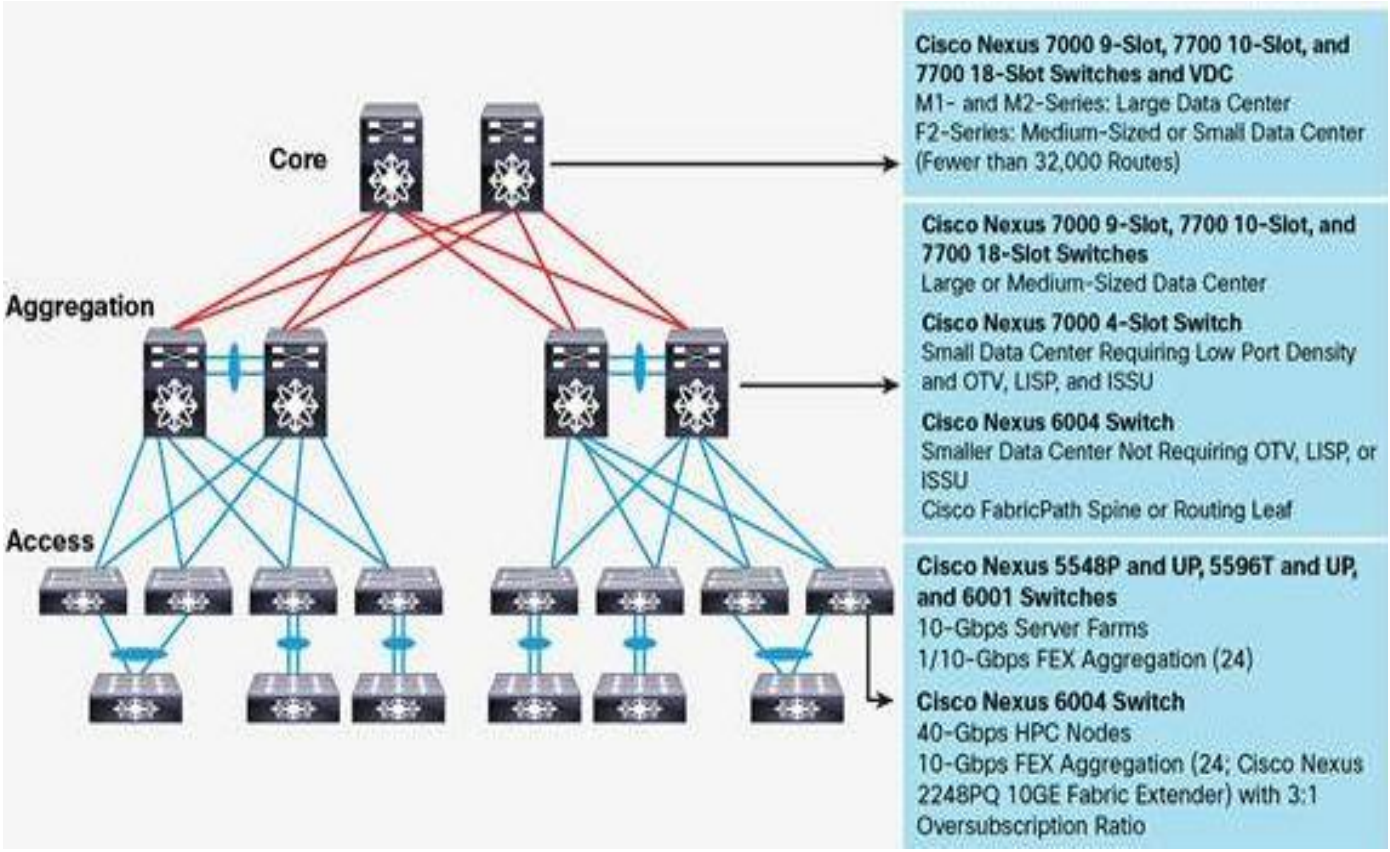
SDN подход к построению информационных систем

Евгений Лысенко
системный инженер
CCNP, CCDP, CCNP DC, CCNA Sec, CCNA Wireless

IT.Integrator

Ограничения классического дизайна ЦОДа

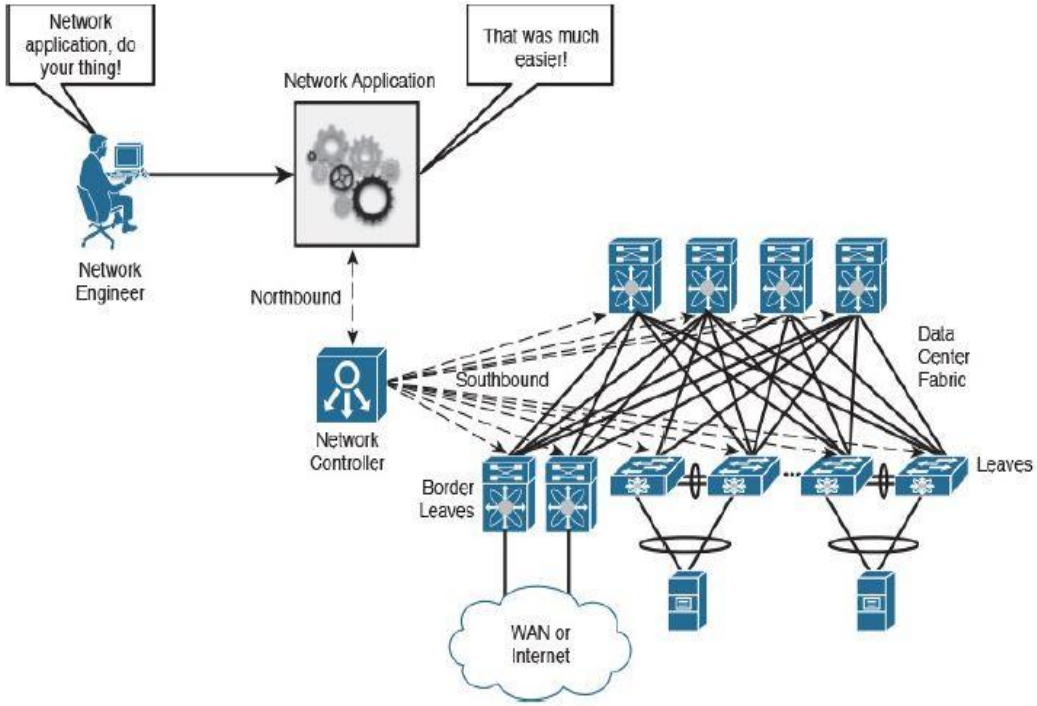
- Переподписка трафика
- Низкий уровень автоматизации процесса настройки
- Низкая степень адаптивности к изменениям в сети



- Трудоёмкость и подверженность ошибкам процесса настройки оборудования
- Необходимость перевода бизнес-требований на технический язык

Программно-определяемые сети (SDN)

- Контроллер – единая точка управления сетью
- Широкие возможности для автоматизации управления
- Повышение уровня управляемости и интеллектуальности сети, уменьшение затрат на администрирование

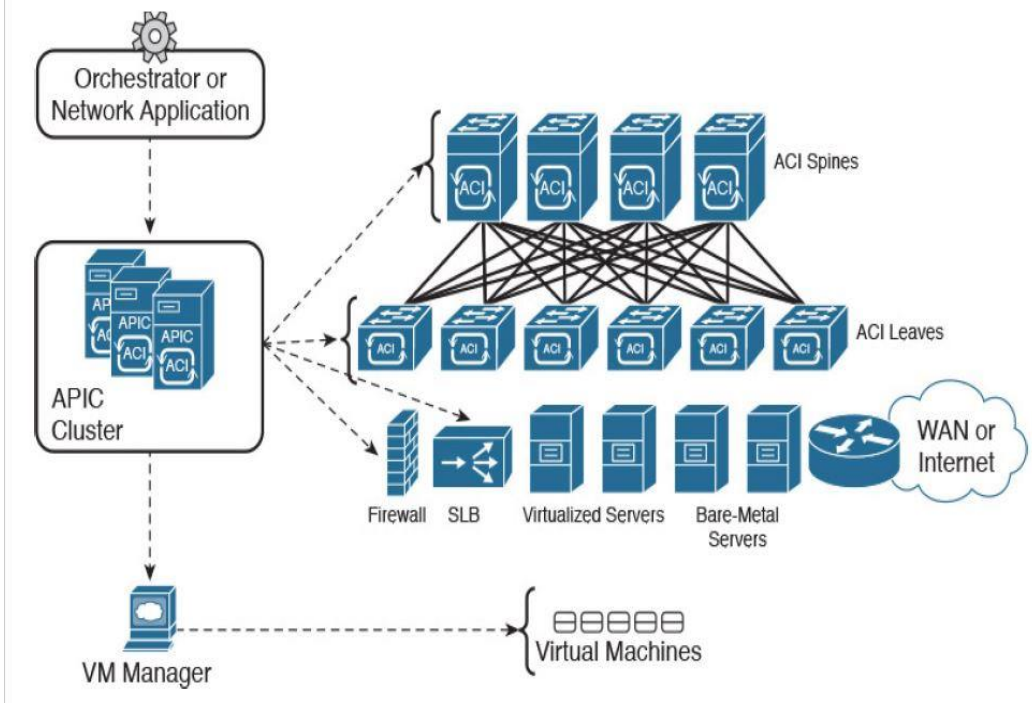


- Уменьшение рисков отказа сети и сервисов в результате ошибки при администрировании
- Значительно ускоряет развёртывание новых сервисов

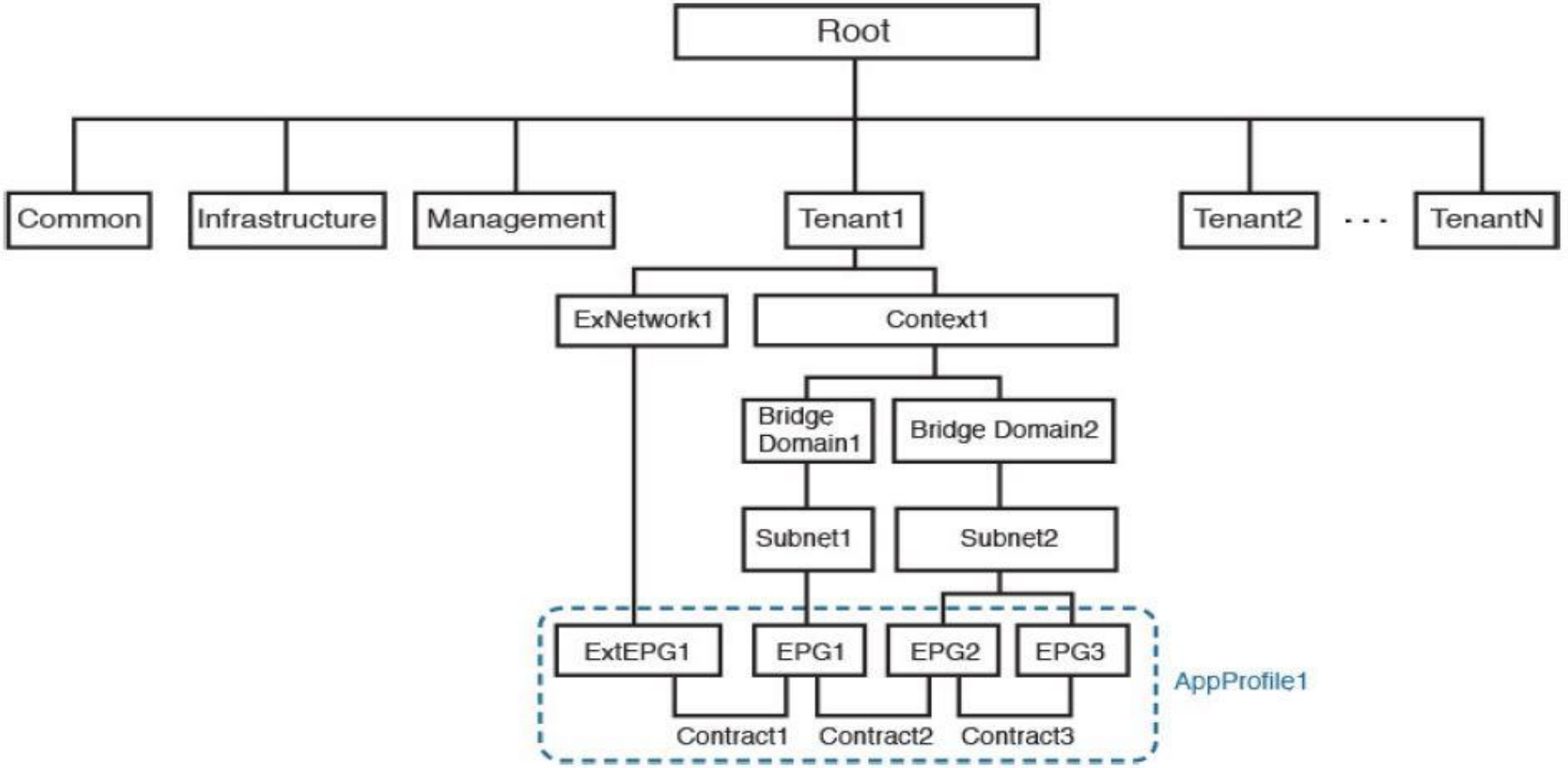
Cisco ACI: Application Centric Infrastructure

Компоненты Cisco ACI:

- Кластер APIC (Application Policy Infrastructure Controller)
- Spine Switches (Nexus 9500 Series, Nexus 9336PQ)
- Leaf Switches (Nexus 9300 Series)
- Серверы (физические и виртуальные)
- L4-L7 Services (Firewall, SLB…)
- VMM (VMWare vSphere, Microsoft SCVMM, RH KVM…)
- 3-Party приложение для управления и автоматизации

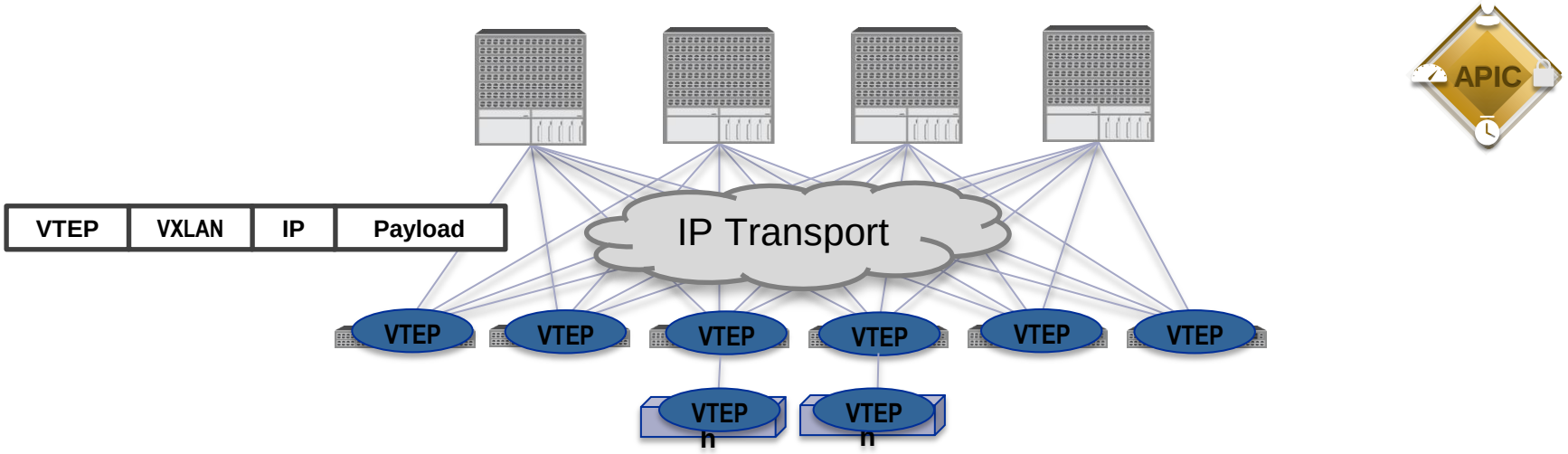


ACI Policy Model



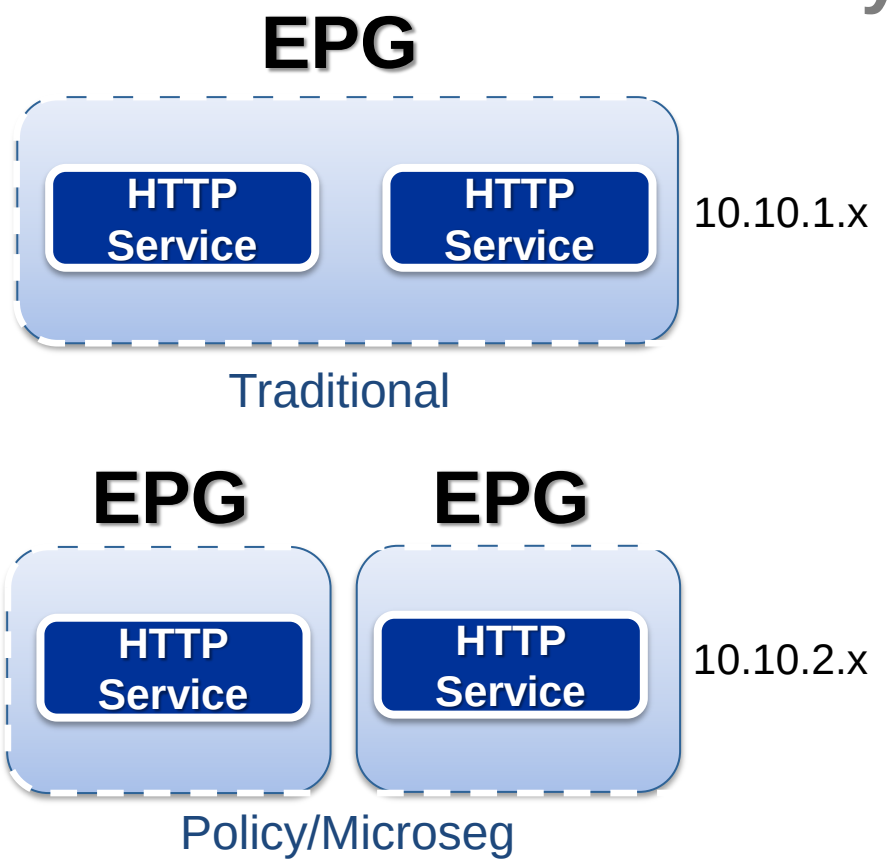
ACI Fabric – An IP network with an Integrated Overlay

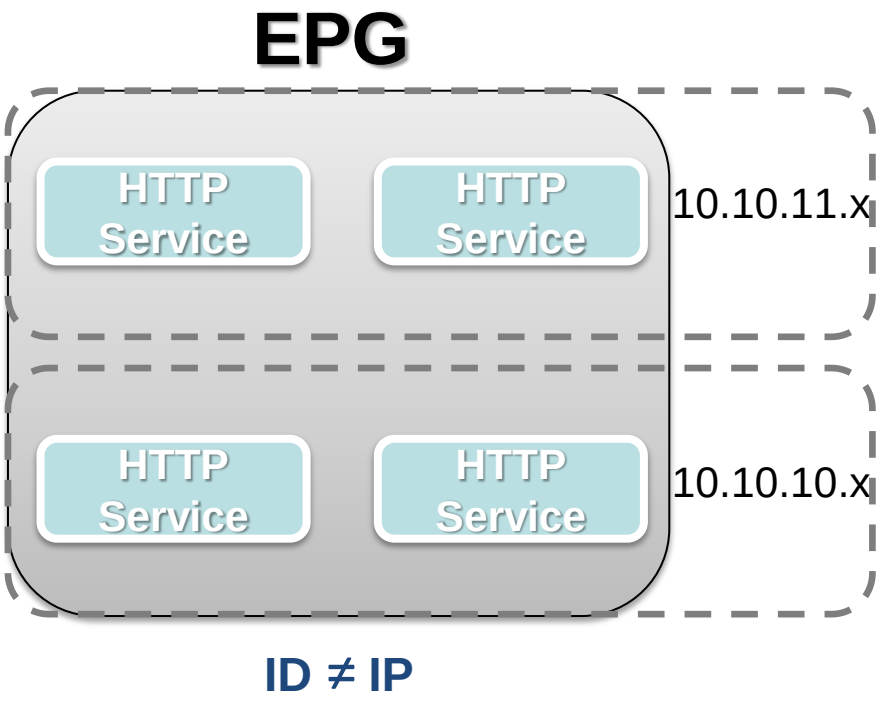
Virtual and Physical



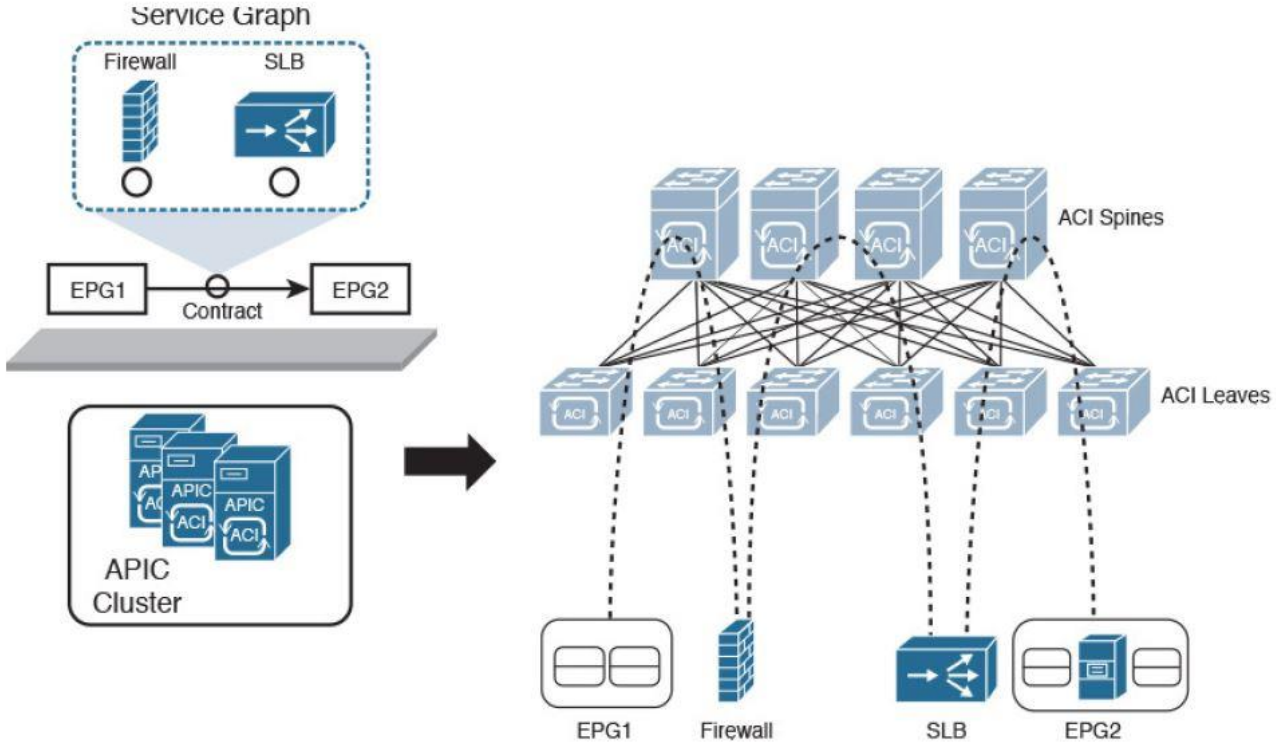
- Cisco ACI использует оверлейную сеть, основанную на технологии VXLAN
- IP-сеть для транспорта
- VXLAN based tunnel end points (VTEP)
- VTEP discovery via infrastructure routing

Why EPG's


EPG
HTTP Service
HTTP Service
10.10.1.x
Traditional
EPG
EPG
HTTP Service
HTTP Service
10.10.2.x
Policy/Microseg

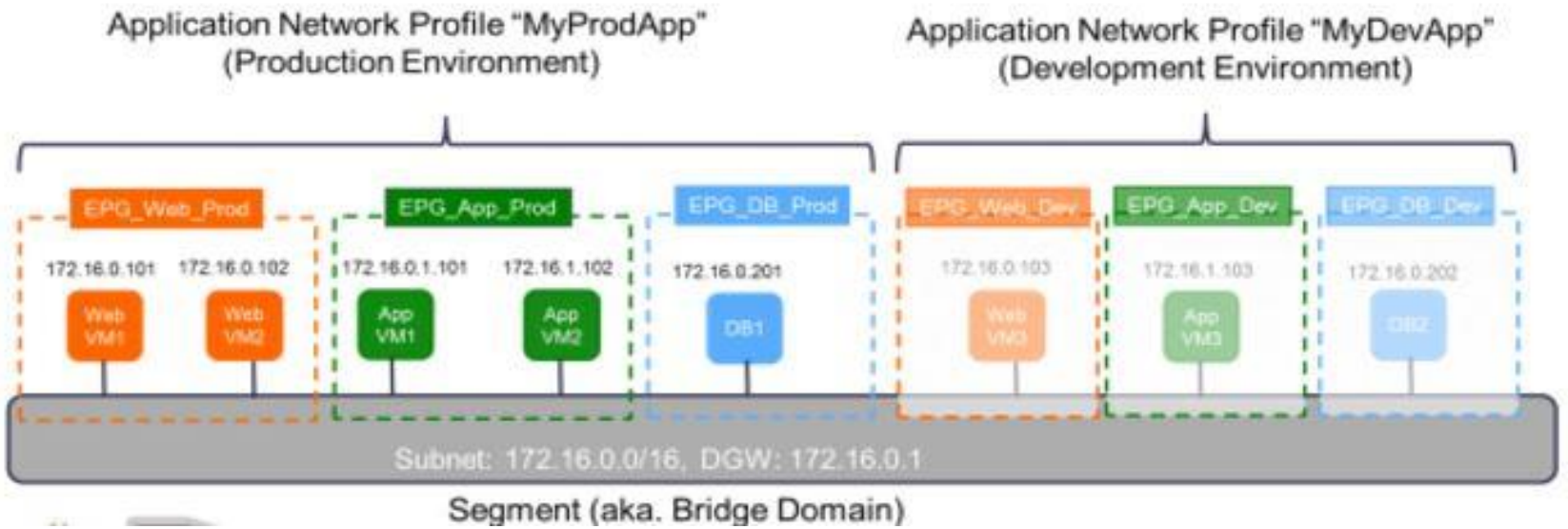

EPG
HTTP Service
HTTP Service
10.10.11.x
HTTP Service
HTTP Service
10.10.10.x
ID ≠ IP

Service Graphs (Service Chaining)



В контракте мы можем указывать PBR (Policy Based Routing) правила для перенаправления трафика в различные сервисные (L4-L7) устройства (например Firewall, SLB, WAF…). Таким образом, мы можем образовывать целые сервисные цепочки.

Микросегментация

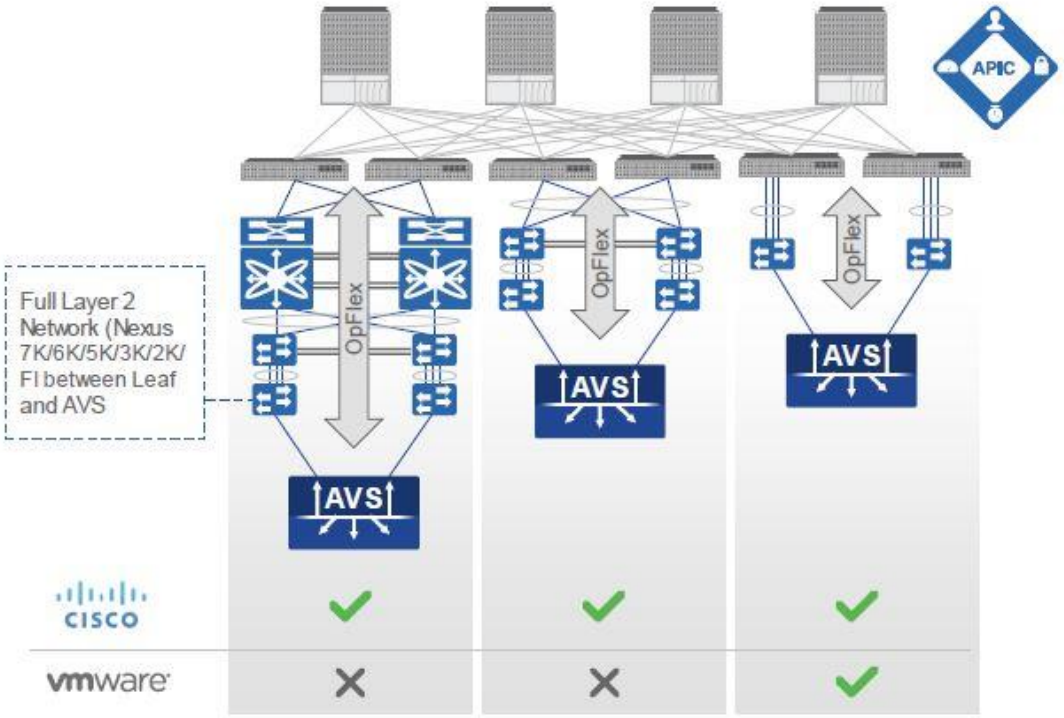


Предоставляет возможность динамически ассоциировать и перемещать виртуальную машину из одного микро-сегмента в другой на основе атрибутов этой ВМ, а также на основе IP и MAC адресов.

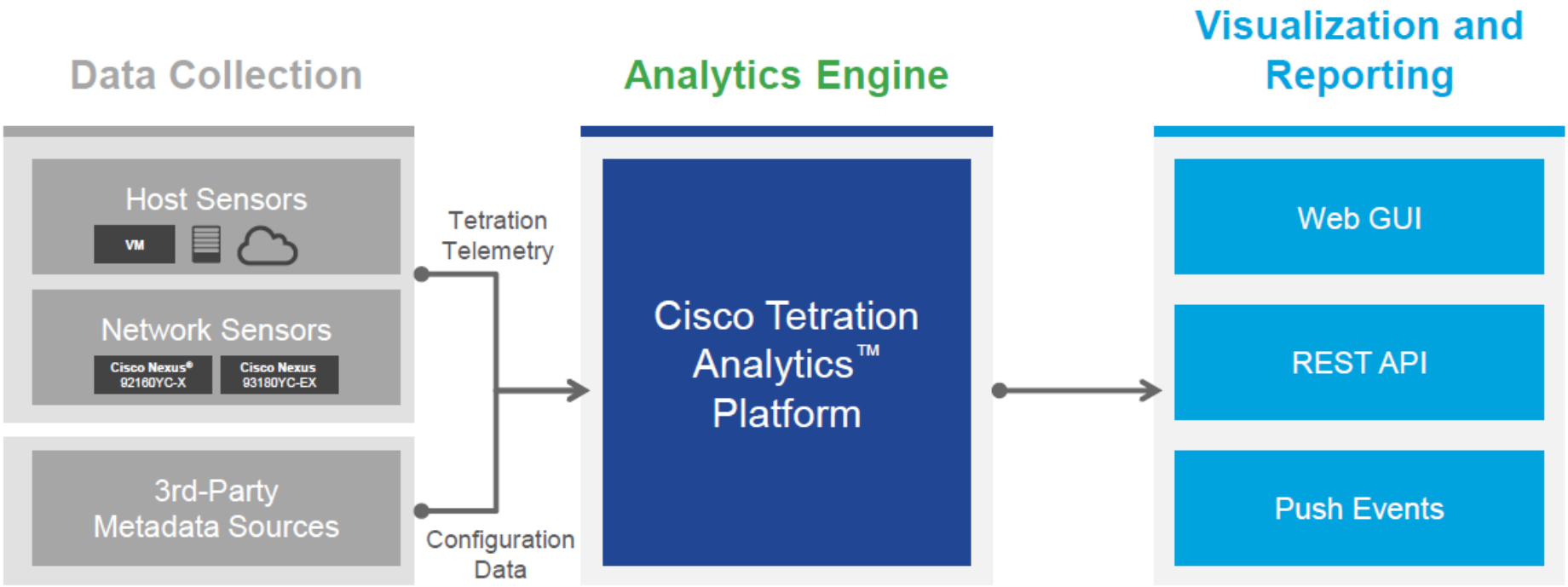
Cisco AVS (Application Virtual Switch)

Сценарии использования:

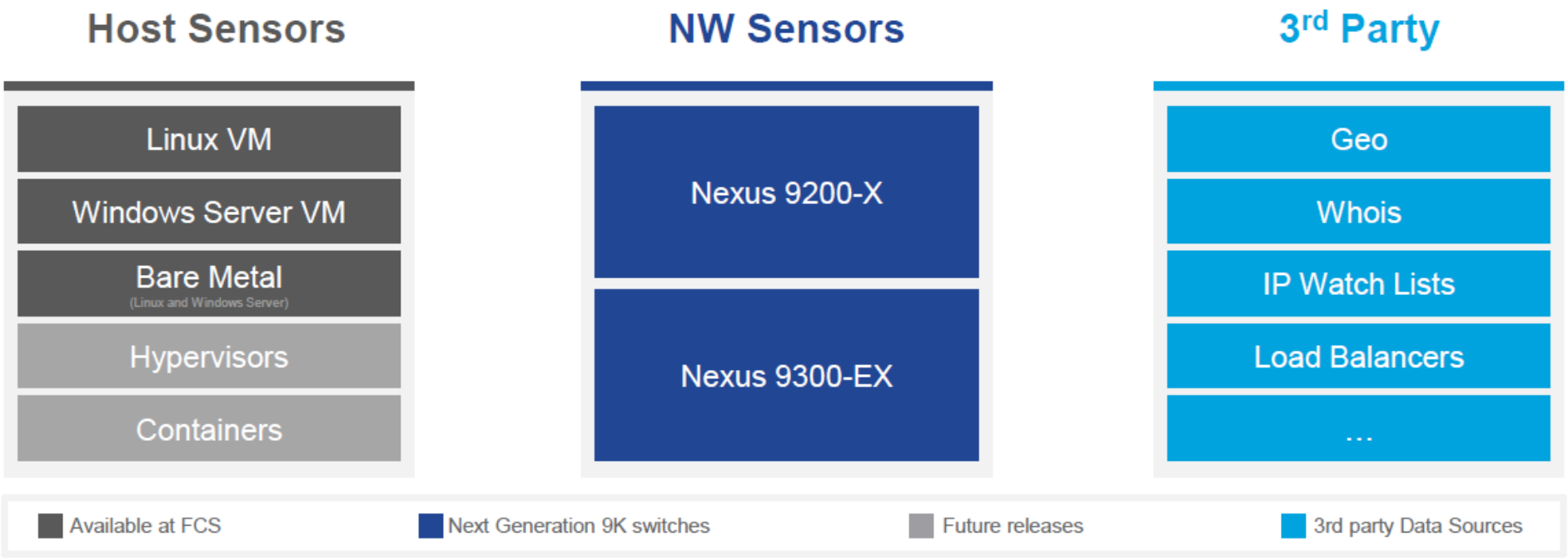
- Упрощение развёртывания FI & Blade
- Защита инвестиций расширяя ACI на существующие сети
- Миграция существующих сервисов на ACI
- Полное расширения фабрики в виртуальную инфраструктуру
- Микро-Сегментация Secure East – West Traffic, основанный на атрибутах виртуальных машин



Cisco TetrationAnalytics Architecture Overview

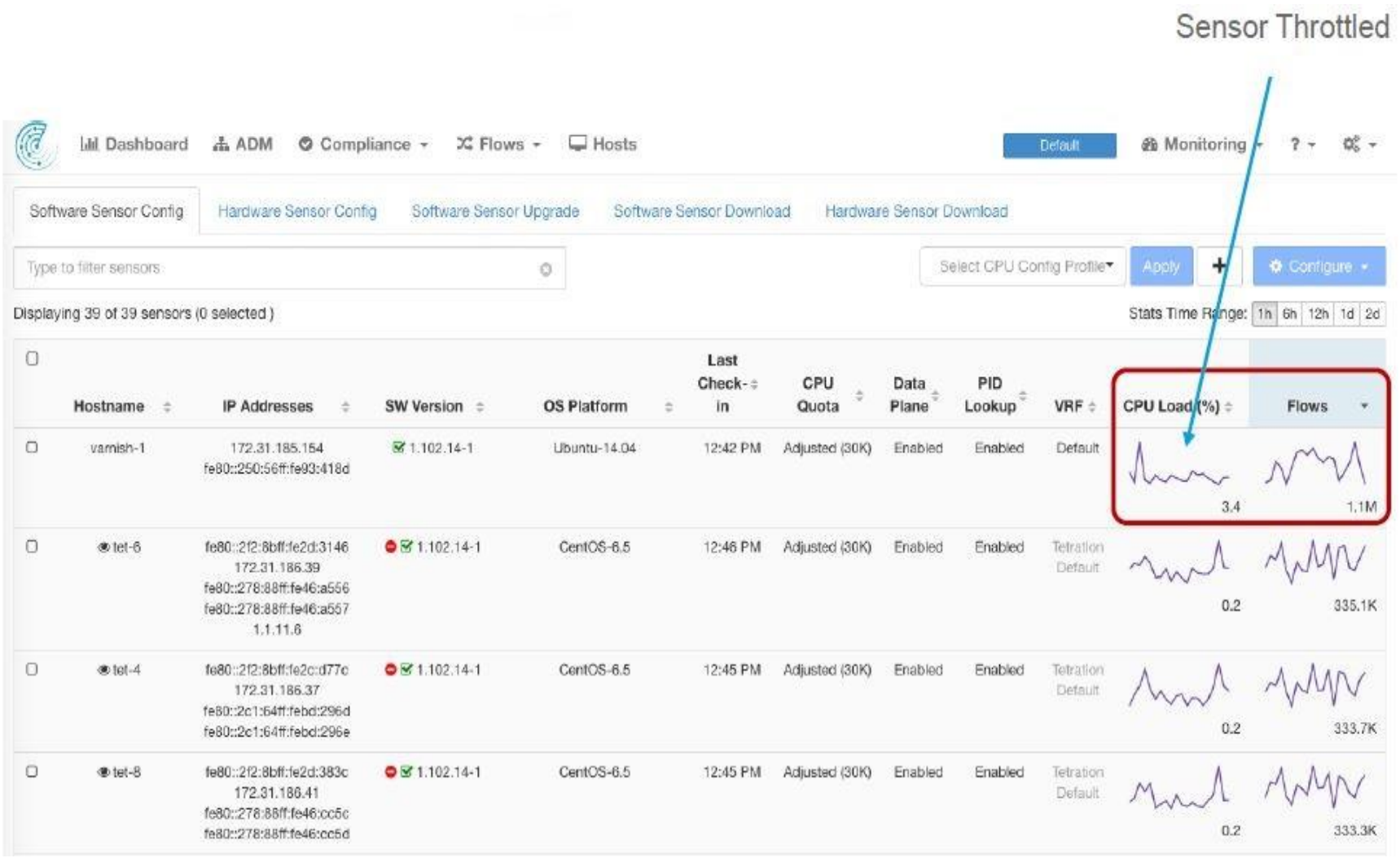


Sensors

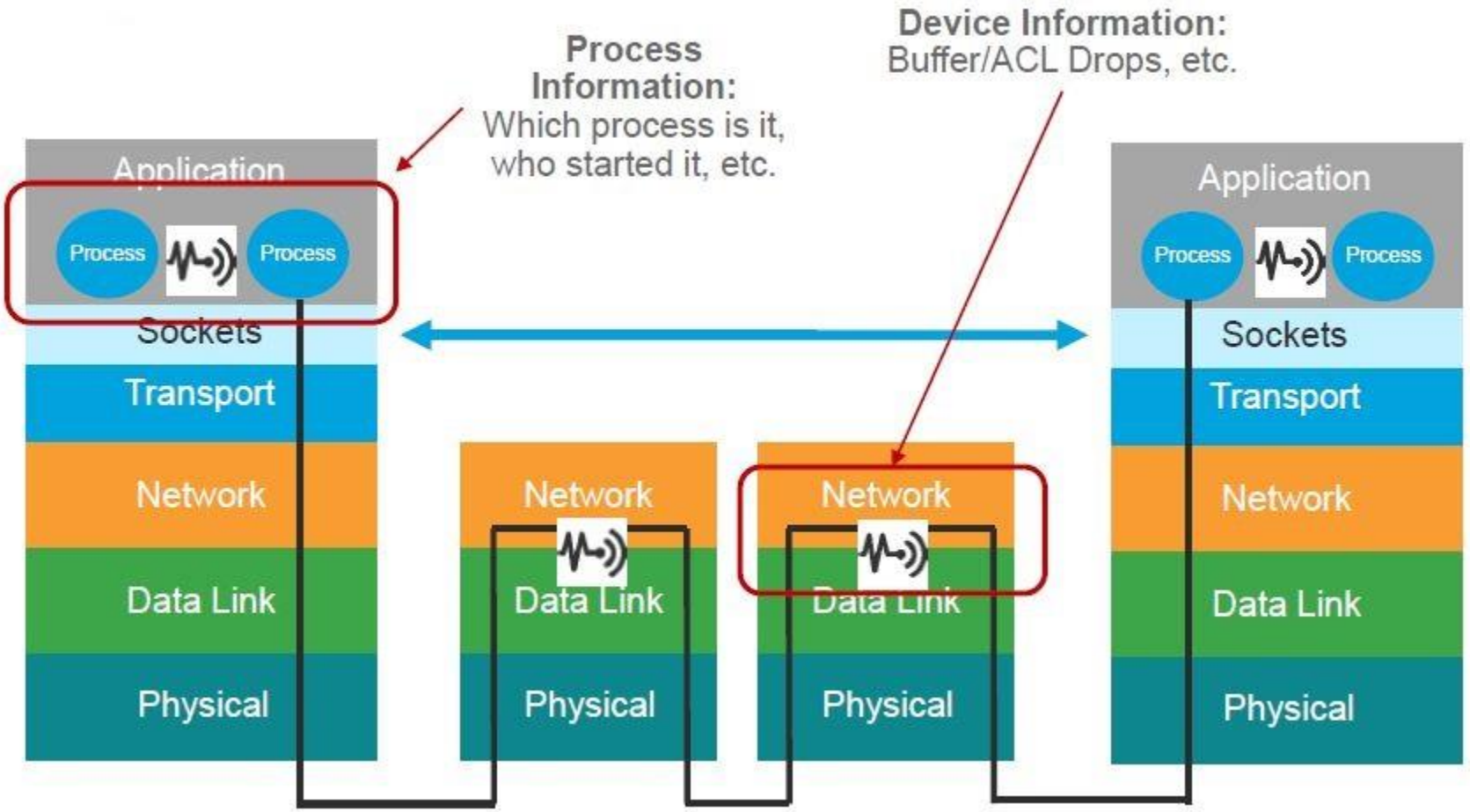


- ✓ **Low CPU Overhead (SLA enforced)**
- ✓ **Low Network Overhead (SLA enforced)**
- ✓ **Highly Secure (Code Signed, Authenticated)**
- ✓ **Every flow (No sampling), NO PAYLOAD**

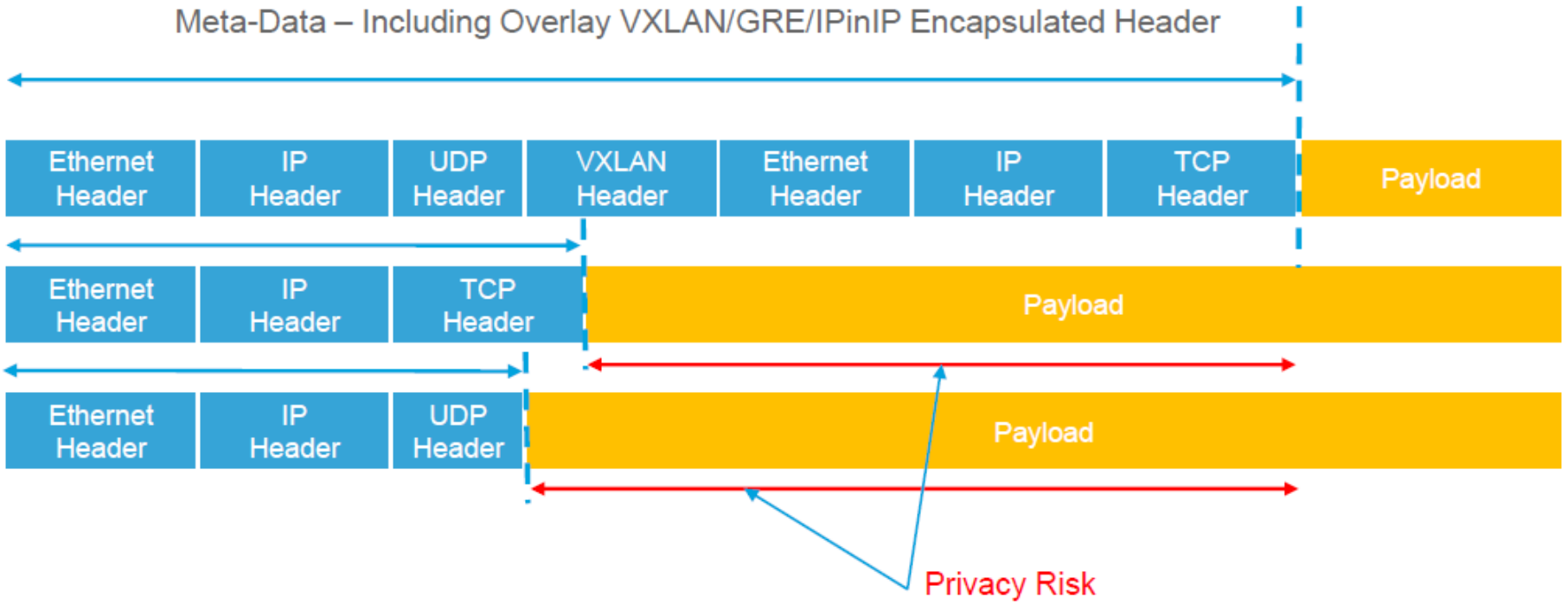
Sensor Monitoring and Maintenance



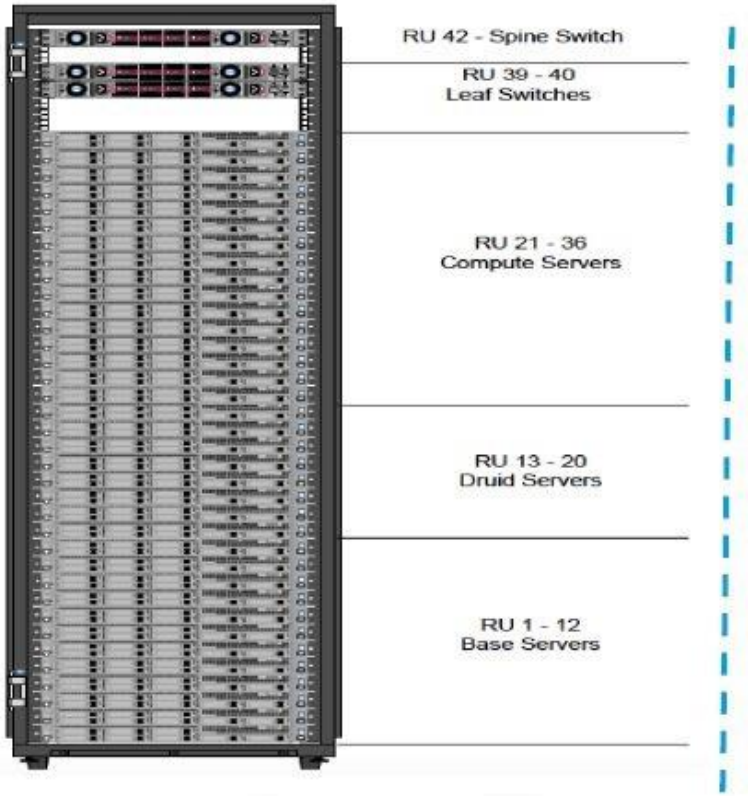
Что собирает сенсор?



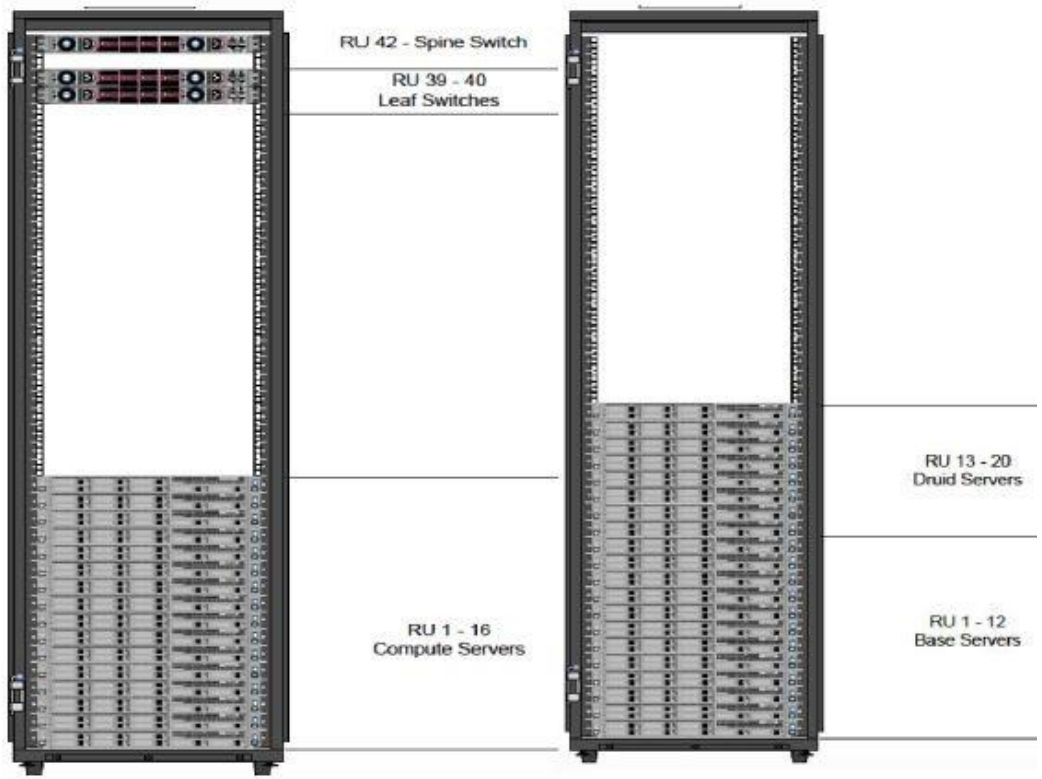
Collects the Meta-Data not the Packet



Cluster Configurations

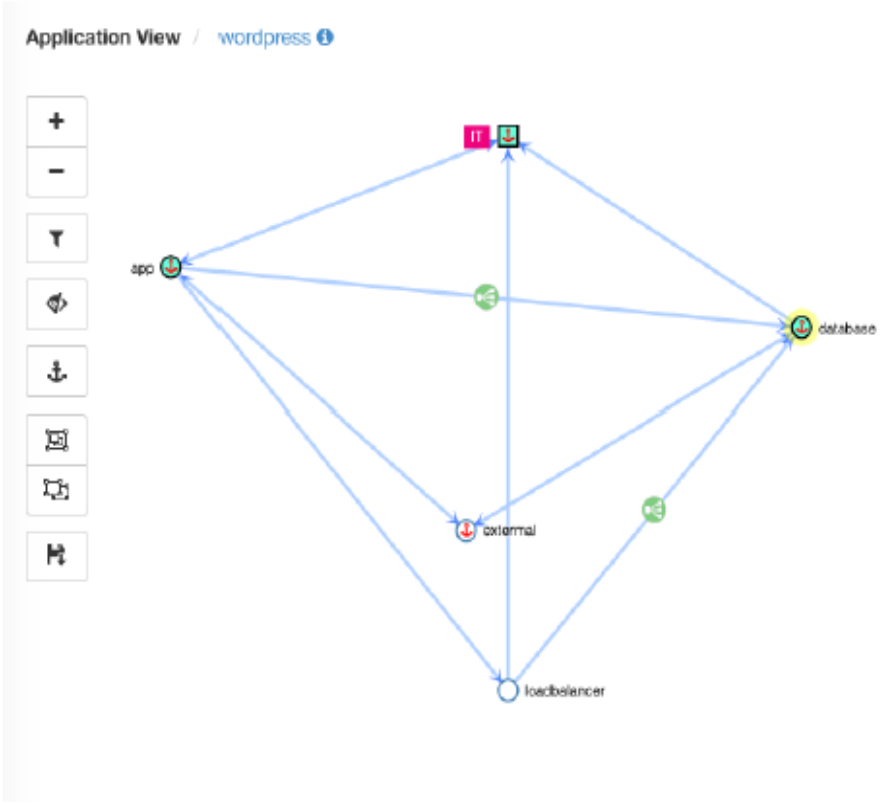


22.5 KW Peak Power



11.5 KW Peak Power

Results of the Clustering Machine Learning



Tetration Uses Cases

Tetration Application Insight: Преимущества решения

- App Insight derived based on actual communication
- Automated grouping of similar endpoints in a cluster
- Keep your App Insight up-to-date based on application evolution
- Flexibility of using hardware or software sensors

Зачем нужно понимать зависимости внутри многоуровневого приложения?

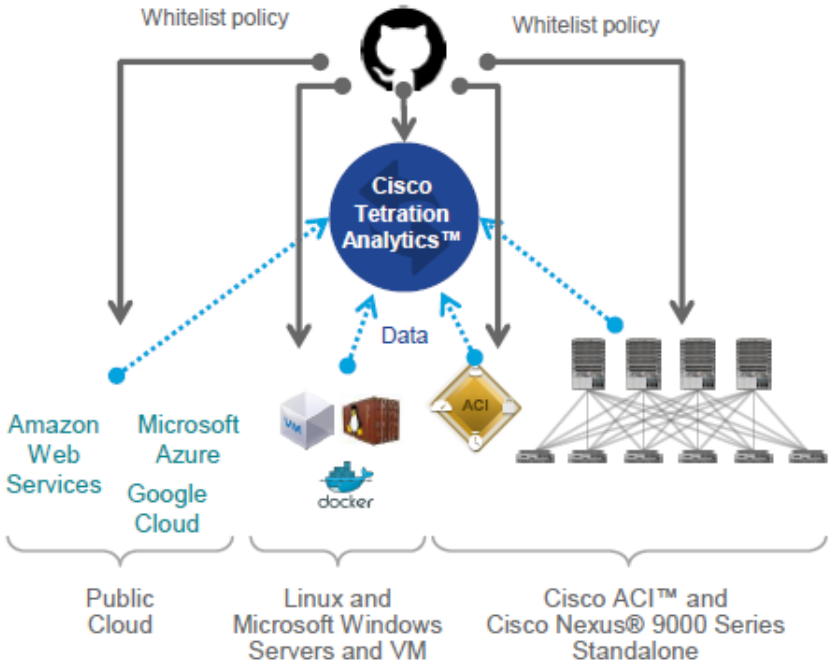
Identify a single point of failure that should be replicated

Find all the parts of a service that should be migrated together to the cloud

Replace infrastructure components of an undocumented application

ACI application profiles, end point groups, and contracts based on applications

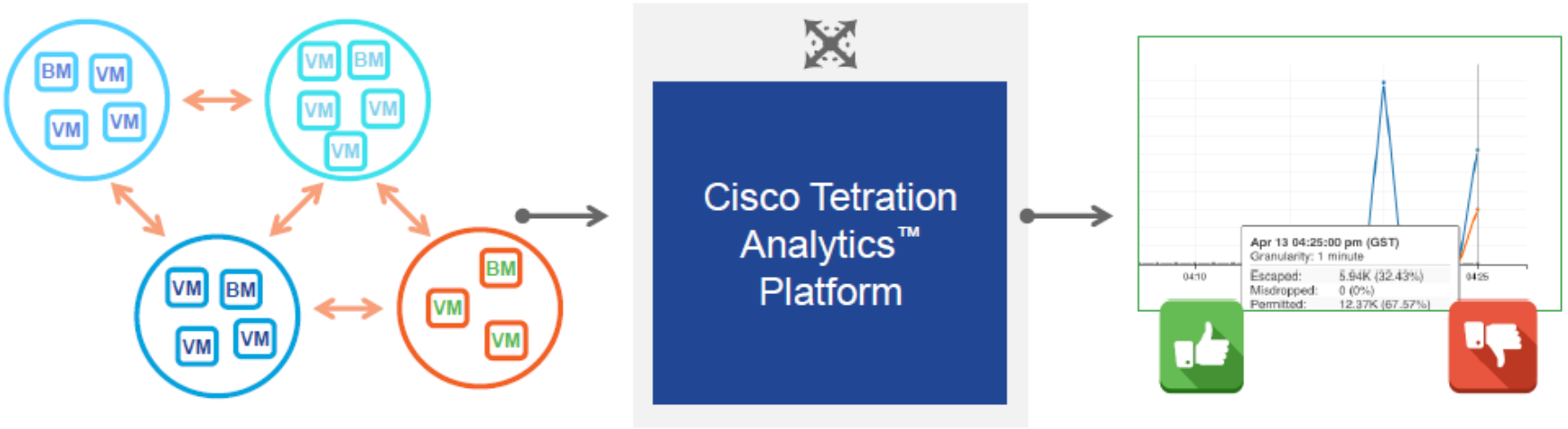
Enforcement Anywhere




```
{
"src_name": "App",
"dst_name": "Web",
"whitelist": [
  {"port": [ 0, 0 ],"proto": 1,"action": "ALLOW"},
  {"port": [ 80, 80 ],"proto": 6,"action": "ALLOW"},
  {"port": [ 443, 443 ],"proto": 6,"action":
"ALLOW"}
 ]
}
```

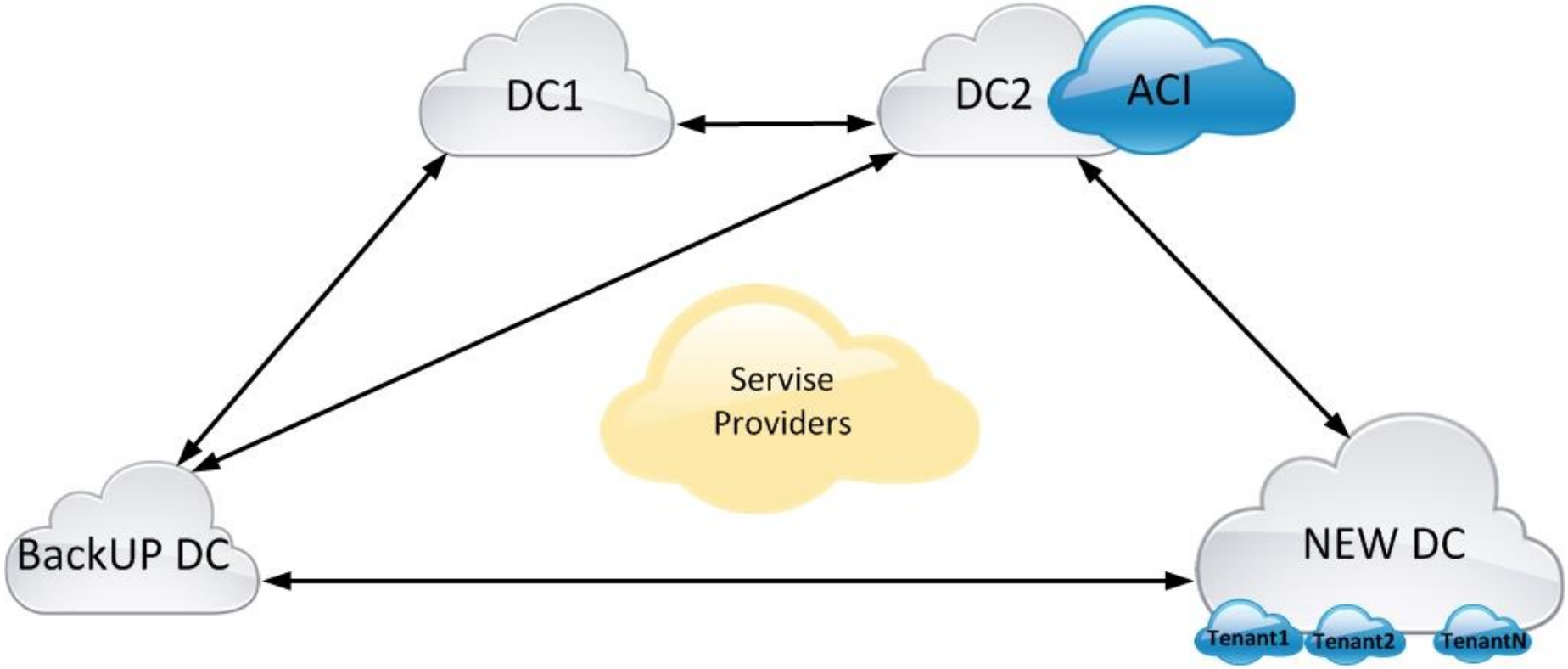
- Cisco ACI EGP/Contract Integration via Cisco ACI Toolkit
- Traditional Network ACL
- Firewall Rules
- Host Firewall Rules

Policy Simulation and Compliance



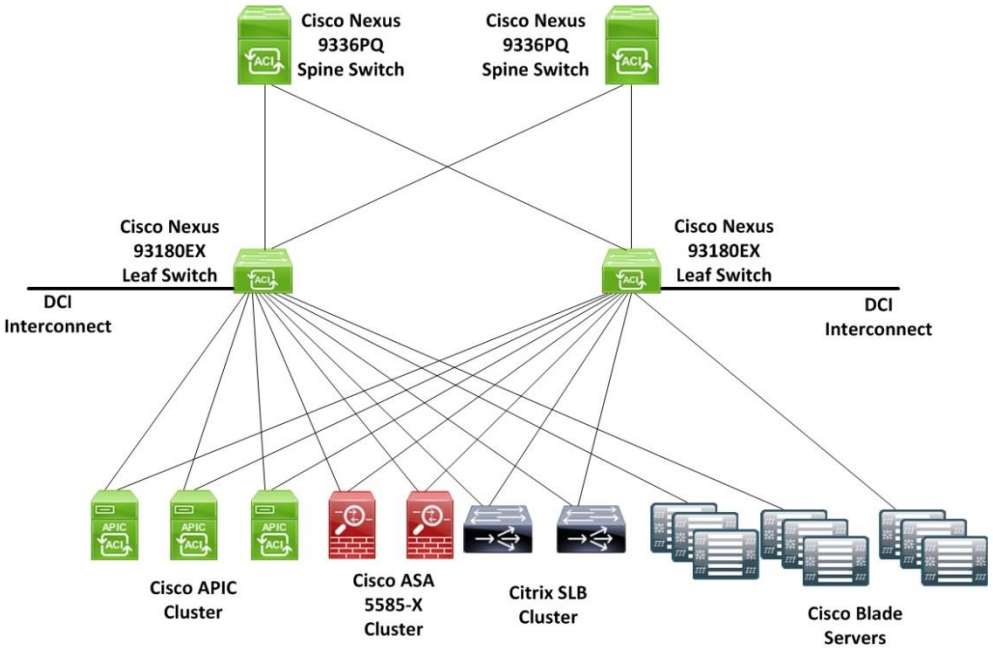
- Identify policy deviations in real-time
- Review and update whitelist policy with one click
- Policy lifecycle management

Кейс. Проект модернизации инфраструктуры банка



Кейс. Бизнес требования заказчика

- Нативная поддержка Multitenancy (для сдачи в аренду части мощностей сторонним организациям)
- Поддержка существующих сервисов (Citrix NetScaler, F5, FW ASA5585-X, FirePower 4110)
- Плотная интеграция с VMWare vSphere
- Поддержка микро-сегментации для ускорения ввода в продакшн и обслуживания внутренних сервисов



Кейс. Бизнес требования заказчика

- Поддержка Service Chain и возможность использования L4-L7 сервисов различными тенантами
- Гибкость и простота администрирования (из-за ограниченности ресурсов на обслуживание инфраструктуры)
- Поддержка внутренних средств самодиагностики и выявления ошибок в работе (Healthcheck, Device Tracking)