思科DNA功能介绍

客户需求

- 了解思科DNA的界面
- 了解思科DNA如何实现基于用户的策略动态部署
- 了解思科DNA如何帮助加速网络问题定位和解决
- 了解思科DNA如何集成安全解决方案

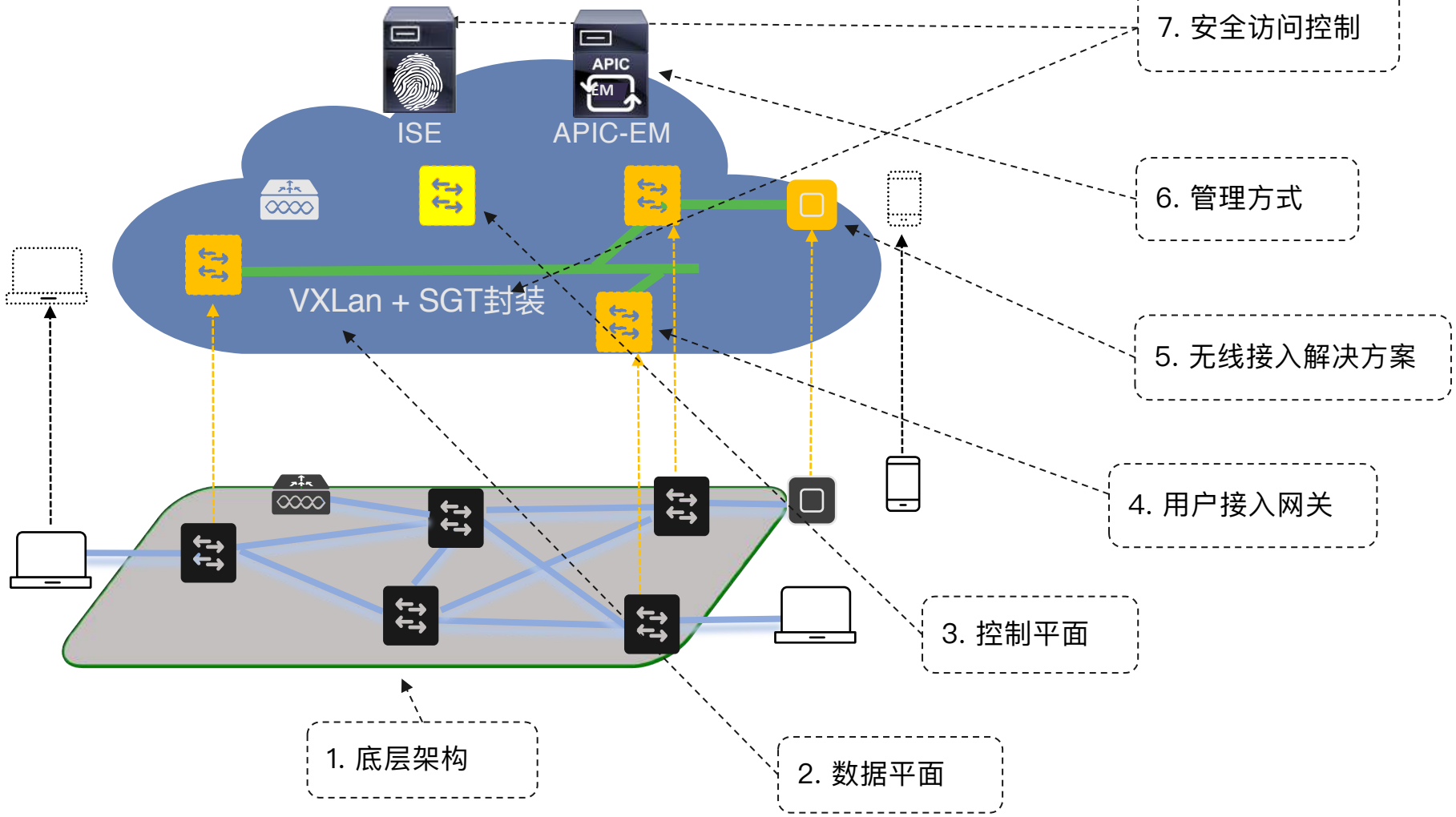
内容简介

- 创新和优势
- 思科DNA Center界面介绍
- 思科DNA Center的大数据平台
- 思科DNA安全方案的集成

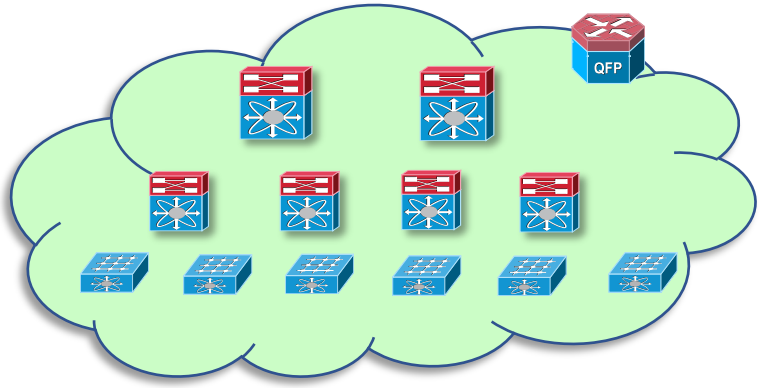
思科DNA和传统企业网对比

思科数字化网络架构的变革

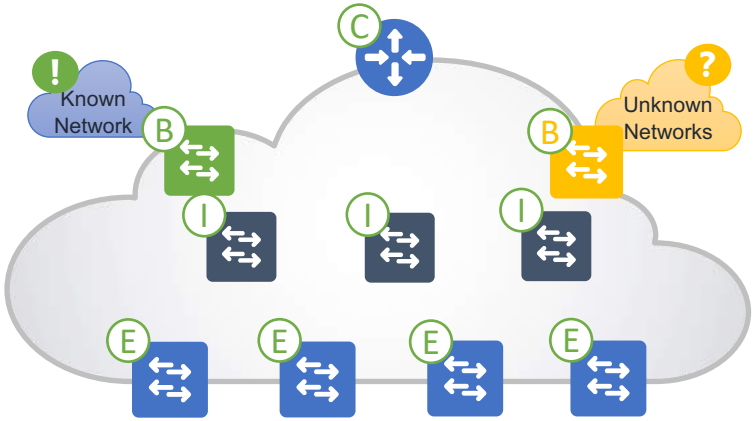
更加稳定，更加敏捷的园区网接入解决方案



底层架构的对比

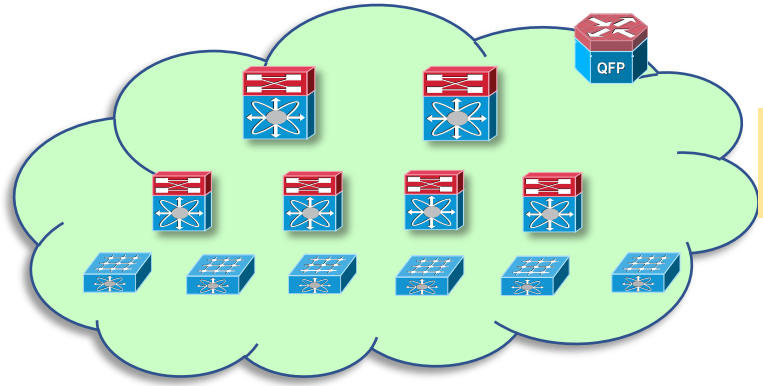


二层 vs 三层

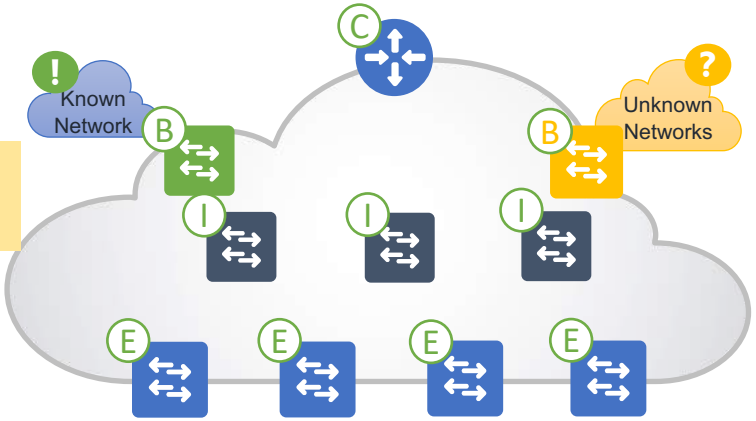


	传统企业网架构 二层	思科数字化网络架构 三层
网络的稳健性	依赖于生成树STP协议，收敛较慢 汇聚层有VSS/VPC/VWS等技术实现链路和单点备份	用户流量和底层架构独立 IP技术提供可达性，备份路由和快速重路由服务，保障用户流量几乎不受影响
广播流量	处于同一广播域的所有节点都需要处理广播流量，占用较多带宽	只有边缘节点处理广播流量 在底层架构内部由单播流量处理用户层广播流量，中间设备无需任何特殊处理
环路控制	环路是基于STP的二层架构最大的挑战之一，需要良好的设计预防环路的产生，和应对节点故障产生的可能的环路	基于IP的三层网络天然对环路免疫

数据平面的对比

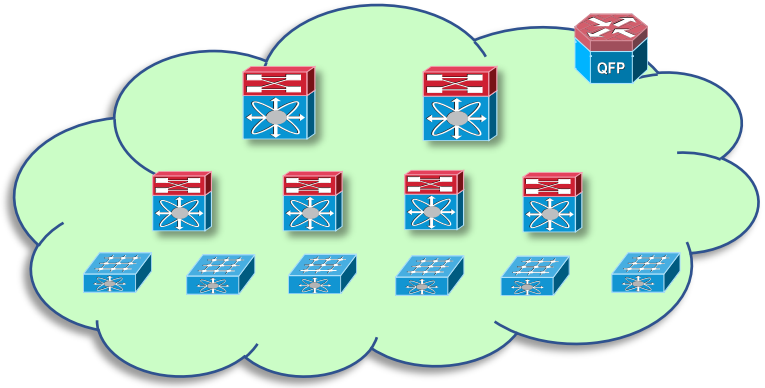


VLAN vs VxLAN

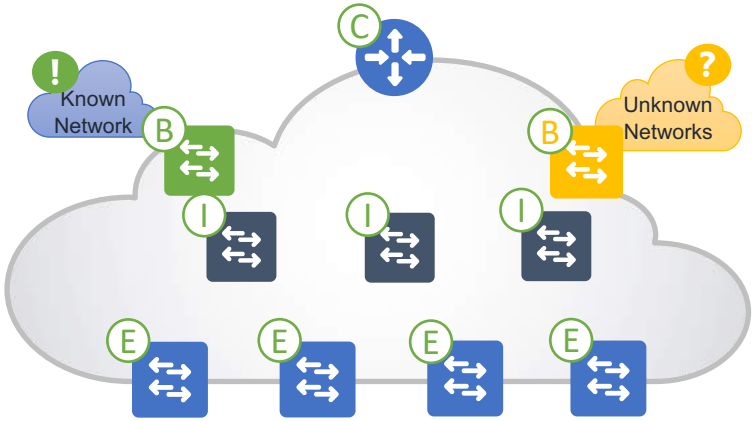


	传统企业网架构	思科数字化网络架构
广播域的支持	只支持本地二层网络，最多4000个vlan子网 扩展二层域需要其他技术且有诸多限制	基于IP/VxLAN的架构，支持远程多站点组建大二层，可支持远超过4000个子网
安全策略	人工配置静态的mac/IP地址控制访问列表	基于组的安全策略，用户的组信息存储于每一个数据包
负载均衡的优化	传统STP网络不支持二层流量的负载均衡，需要VSS/VPC/VWS等技术支持基于用户的负载均衡	基于UDP的VxLAN技术支持基于用户不同应用流量的负载均衡，更加优化链路使用状况。 中间转发设备不需要做深度数据包检测(DPI)，节省了计算资源，优化了全网的转发性能。

控制平面的对比

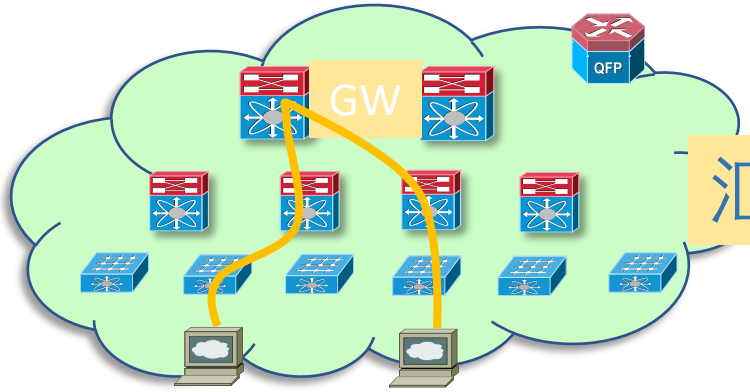


IGP vs LISP

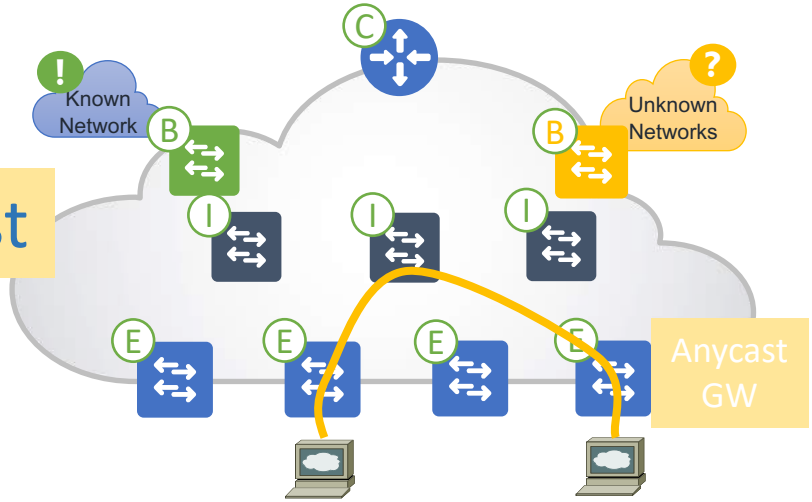


	传统企业网架构	思科数字化网络架构
路由协议弹性	二层mac信息靠flood-and-learn 三层IP信息靠路由协议	LISP支持二层mac信息和三层IP信息的管理
控制平面优化	基于分布式路由协议，每一台设备都需要存储大量路由信息	基于LISP的集中式控制平面，控制节点记录完整信息，其他设备只需要记录需要的路由信息即可

三层网关的对比



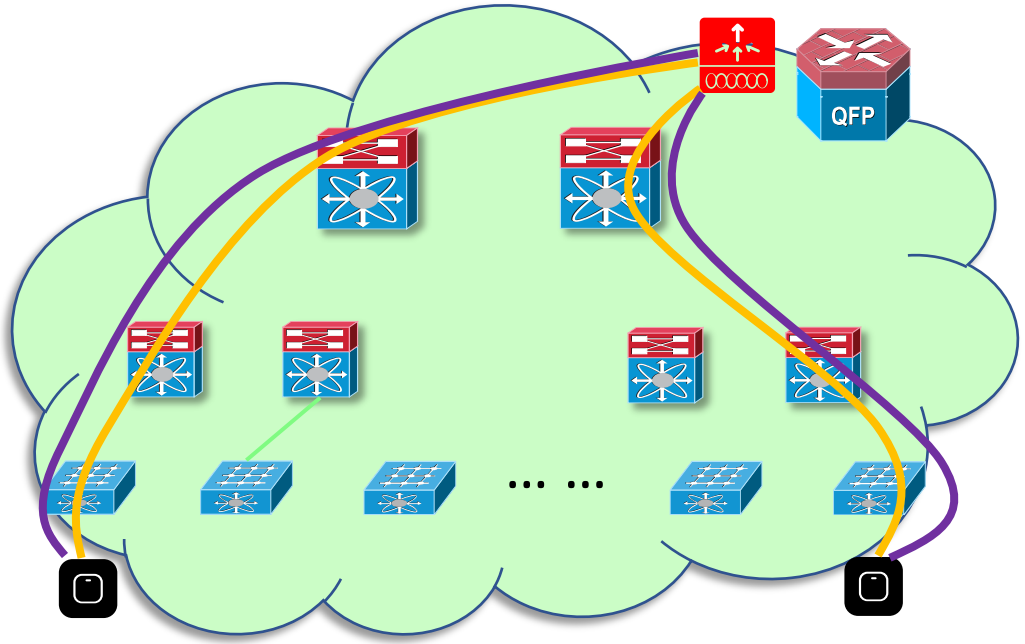
汇聚层 vs Anycast



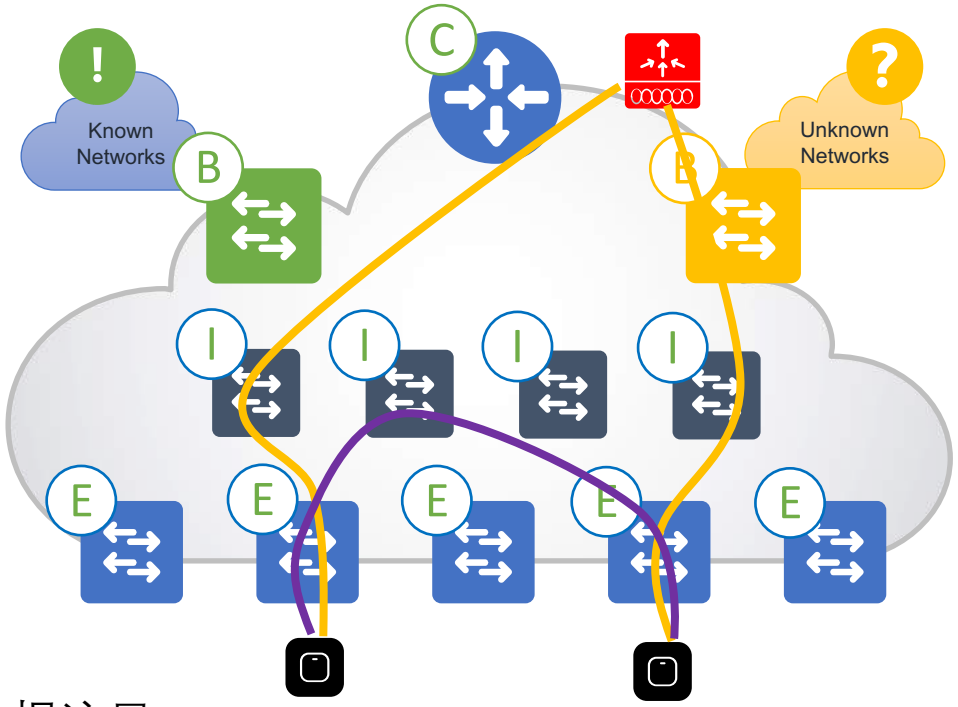
	传统企业网架构	思科数字化网络架构
服务器迁移	触发整个二层网络从新学习设备的新接入点并更新之前的记录，收敛前会产生广播流量	仅接入设备触发重新学习，无广播流量
流量模型和链路优化	跨IP网络的流量需要从接入交换机先发送到网关，再由网关下发到接入交换机，最终转发给终端设备	跨IP网络的流量可直接从直连流量源设备的交换机发送给直连流量目的设备的交换机

无线方案的对比

控制平面和数据平面都要依赖于无线控制器

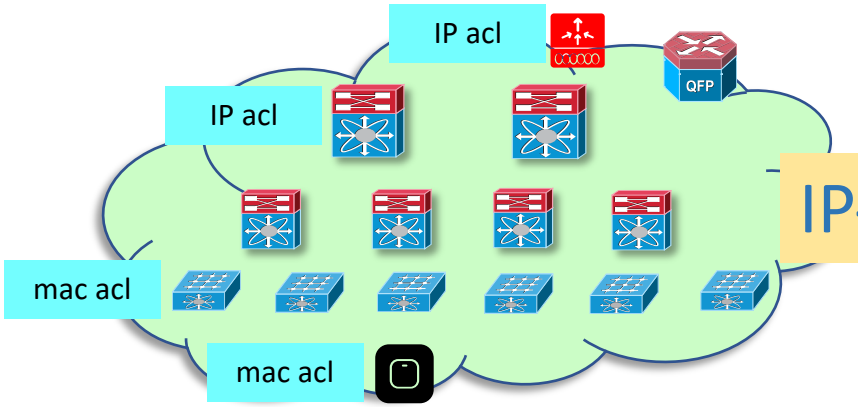


数据流量不需经过无线控制器

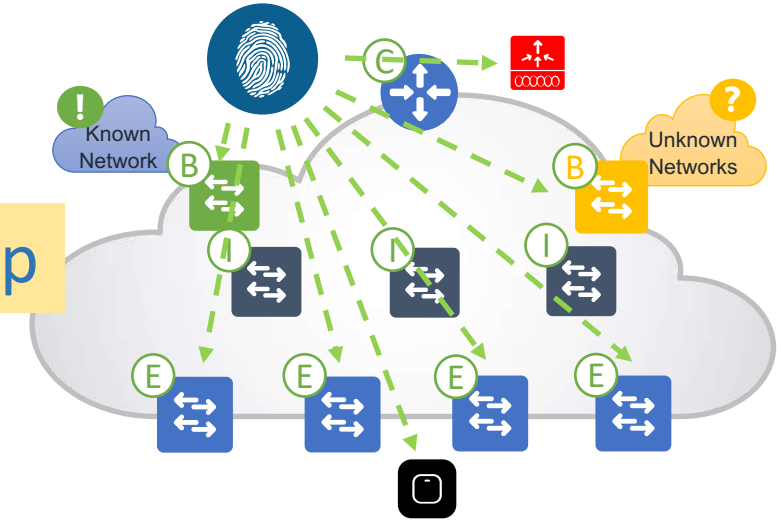


控制流量　　数据流量

安全策略的对比

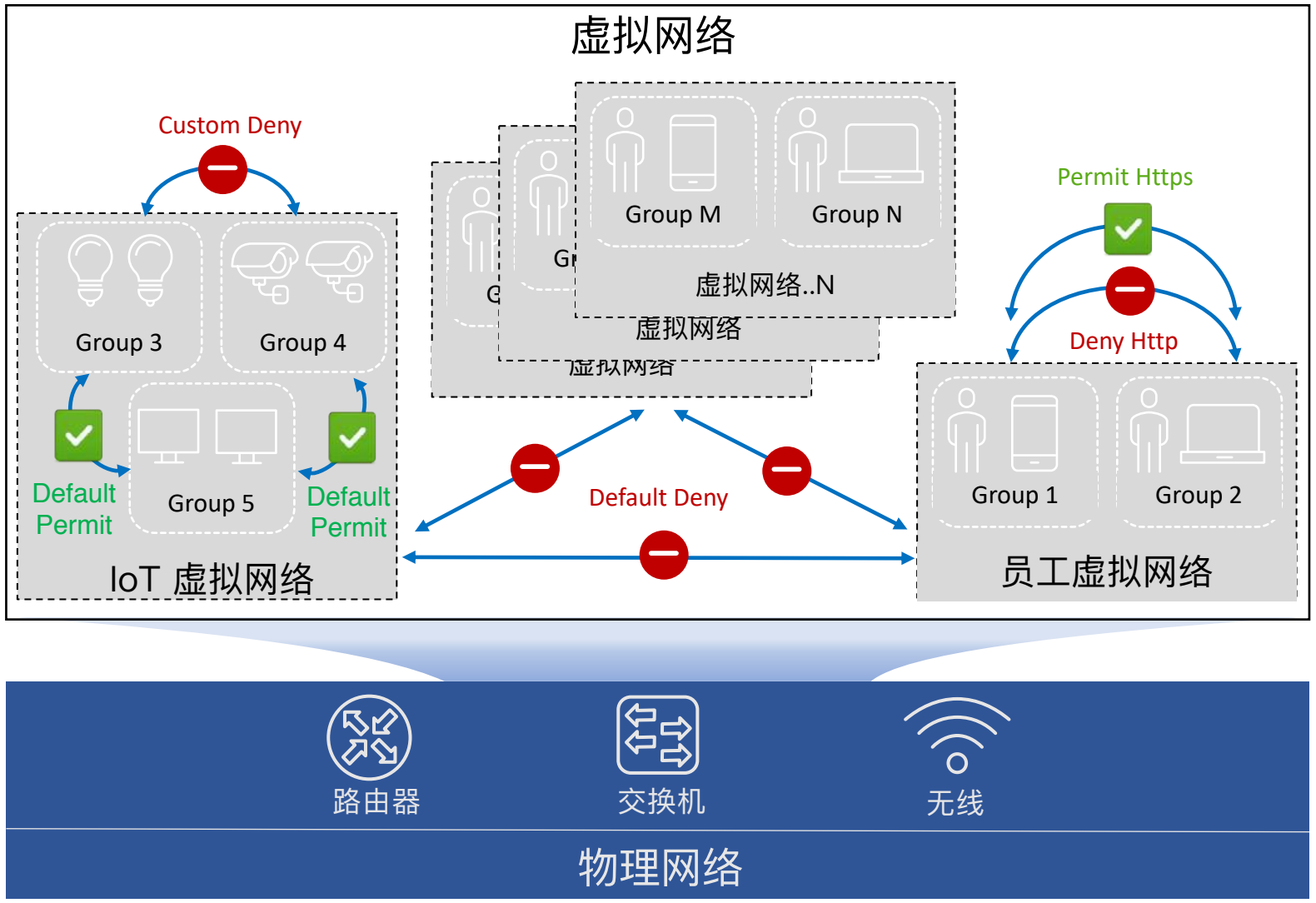


IP-based vs Group



	传统企业网架构	思科数字化网络架构
用户身份	Mac-based或者IP-based	Group-based/Role-based
网络隔离	通过VLAN, IP subnet和VRF隔离不同用户	通过虚拟网络(VN)和分段技术(Segment)隔离不同用户
NAT或地址伪造	基于IP，如果源或目的地址被更改则安全信息丢失	支持，身份信息存在于每一个数据包VxLAN头部，IP头部任何改变都不影响安全策略
策略动态部署（策略随行）	分布式的安全策略需要在所有设备上人工更新同步最新信息	身份服务引擎集中管理所有身份认证和安全策略 DNA Center确保所有设备实时同步最新安全信息，避免了分布式控制的风险（策略随行）

安全策略 之策略分级

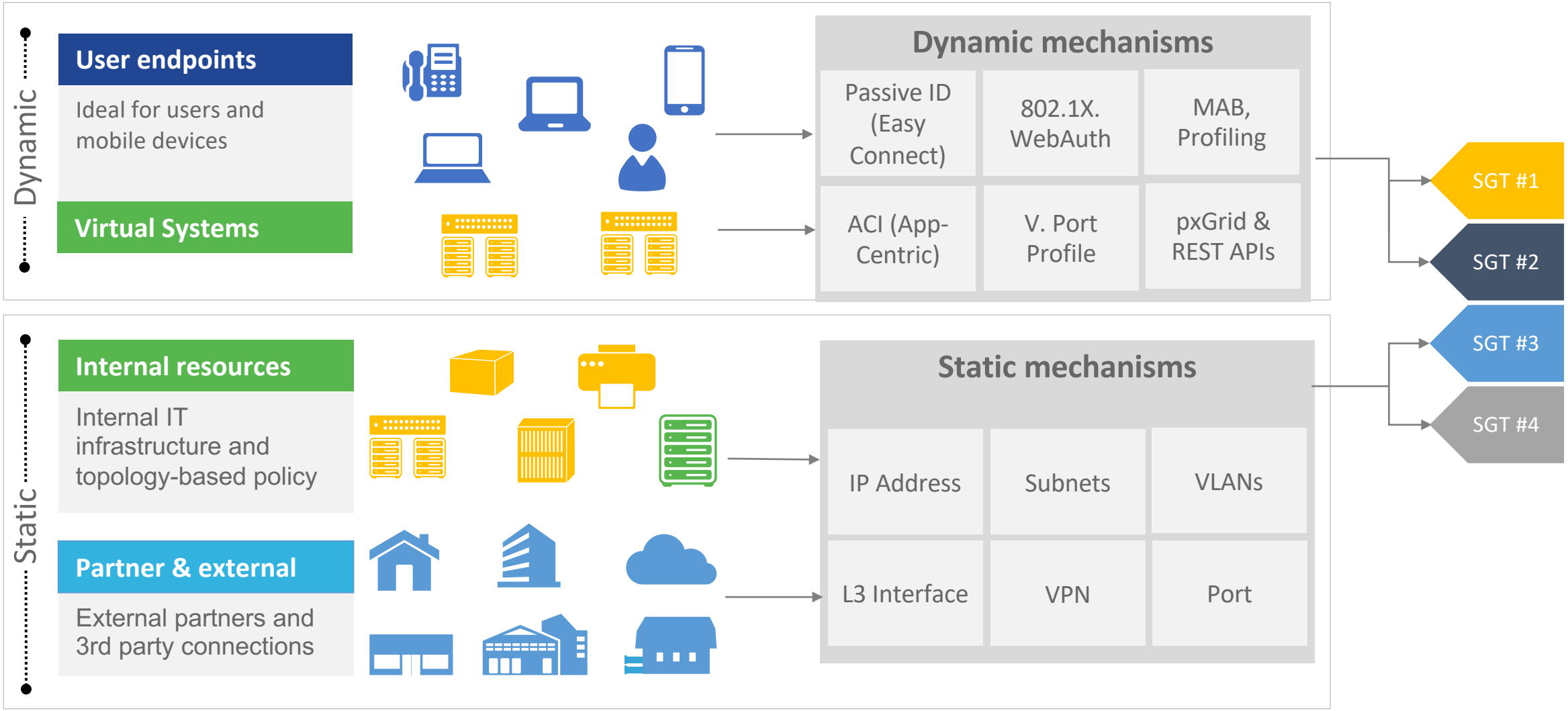


Virtual Networks-虚拟网络

“VN” ≈ “VRF”

Groups-用户组

安全策略 之分组方法

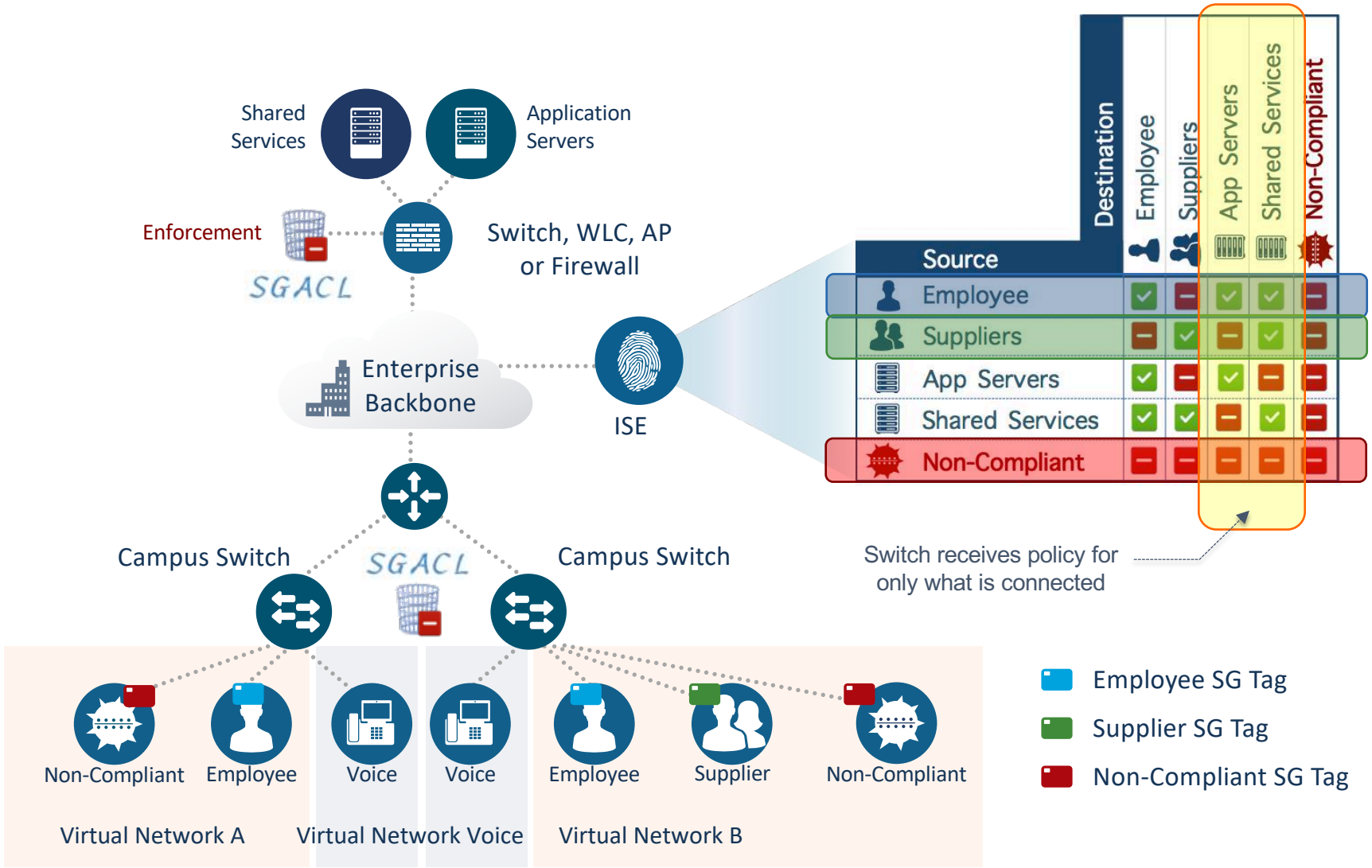

Dynamic
User endpoints
Ideal for users and mobile devices
Virtual Systems
Dynamic mechanisms
Passive ID (Easy Connect)
802.1X. WebAuth
MAB, Profiling
ACI (App-Centric)
V. Port Profile
pxGrid & REST APIs
Static
Internal resources
Internal IT infrastructure and topology-based policy
Partner & external
External partners and 3rd party connections
Static mechanisms
IP Address
Subnets
VLANs
L3 Interface
VPN
Port
SGT #1
SGT #2
SGT #3
SGT #4

安全策略 之访问规则

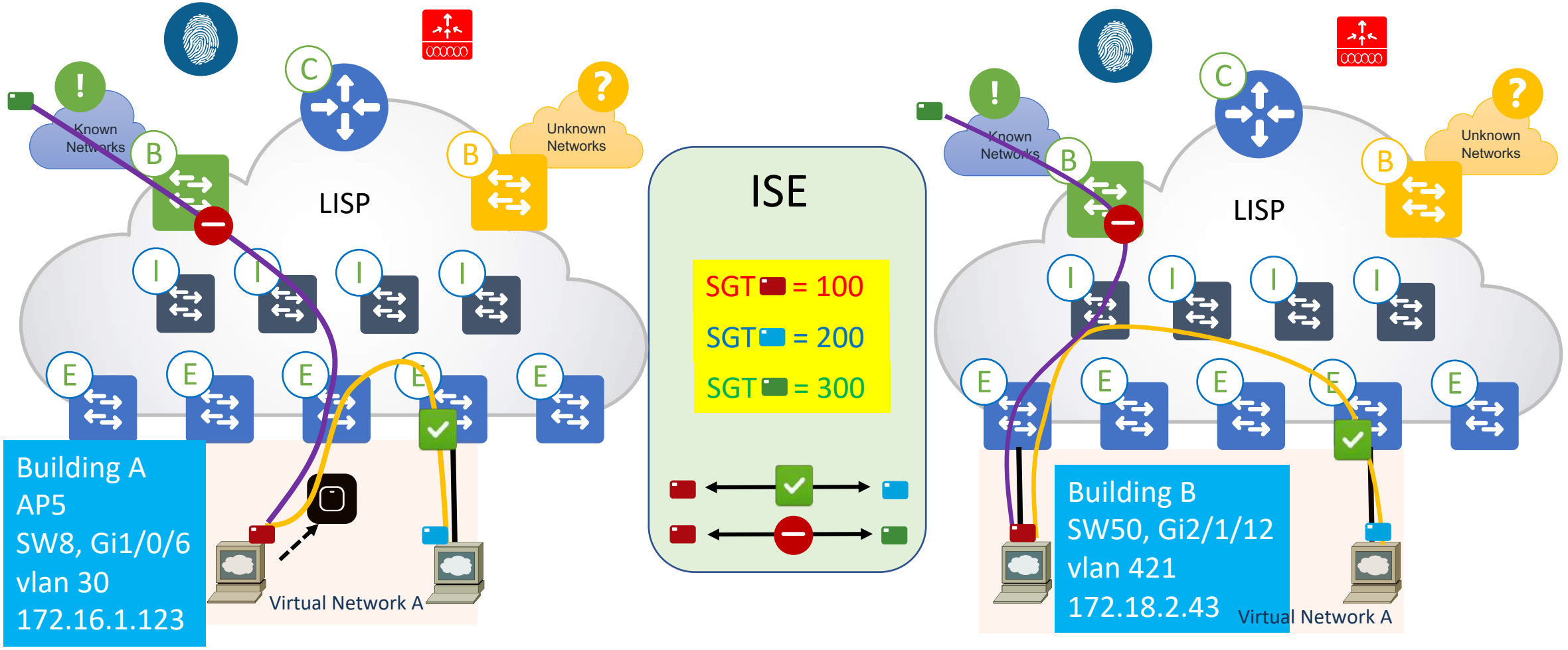
Enforcement
Group Based Policies
ACLs, Firewall Rules

Propagation
Carry “Group” context through the network using only SGT

Classification
Static or Dynamic SGT assignments



安全策略 之策略随行

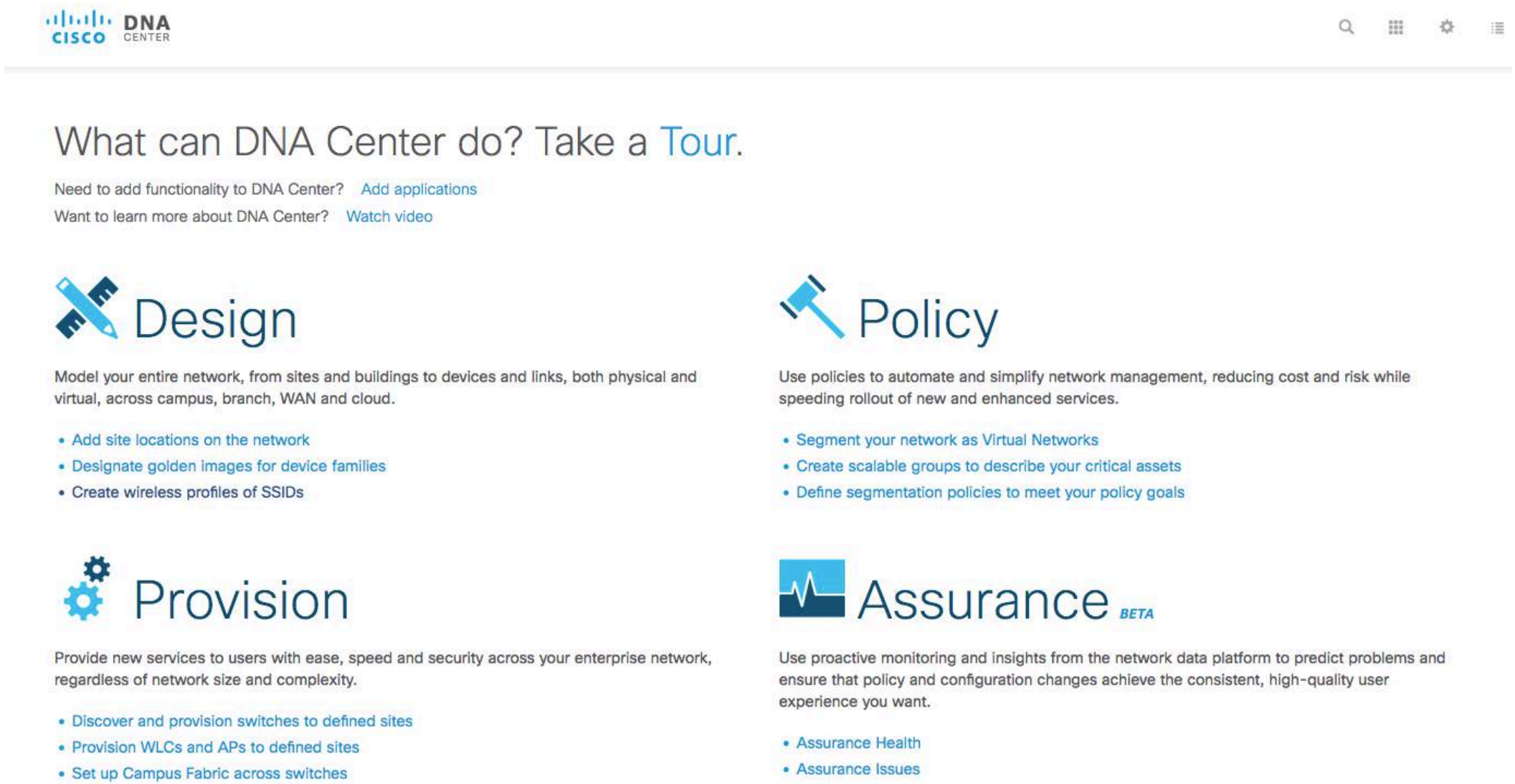

Known Networks
Unknown Networks
LISP
ISE
SGT = 100
SGT = 200
SGT = 300
Building A
AP5
SW8, Gi1/0/6
vlan 30
172.16.1.123
Virtual Network A
Known Networks
Unknown Networks
LISP
Building B
SW50, Gi2/1/12
vlan 421
172.18.2.43
Virtual Network A

思科数字化网络架构之集中式管理界面

	传统企业网架构	思科数字化网络架构
设备配置	需要逐一登录设备并配置 命令行模式	终端设备零配置 一切配置都在DNA Center用户界面完成
设备管理	需要逐一登录 不同设备不同的用户接口	不需要登录设备 所有设备都由DNA Center用户界面统一呈现
网络服务集成	无线，防火墙，路由器，交换机，DHCP，AAA等不同服务各自有一套配置管理界面	开源的接口，DNA Center统一的管理界面
网络维护	需要不同领域的技能以及应对复杂网络的排错能力	完整的网络状况监测 Telemetry **网络大数据平台** NDP 人性化的网络状况界面 快捷有效的排错建议

DNA Center界面介绍

DNA Center四步工作流程



DNA Center两大功能类

自动化部署和保障服务

Automation

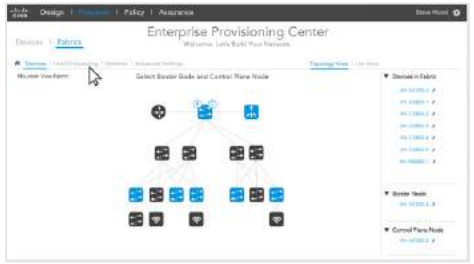
Design

- Global settings
- Site profiles
- DDI, SWIM, PNP
- User access

Policy

- Virtual networks
- ISE, AAA, Radius
- Access control
- Application control

Provision



- Fabric domains
- Device on-boarding
- Device inventory
- Host on-boarding

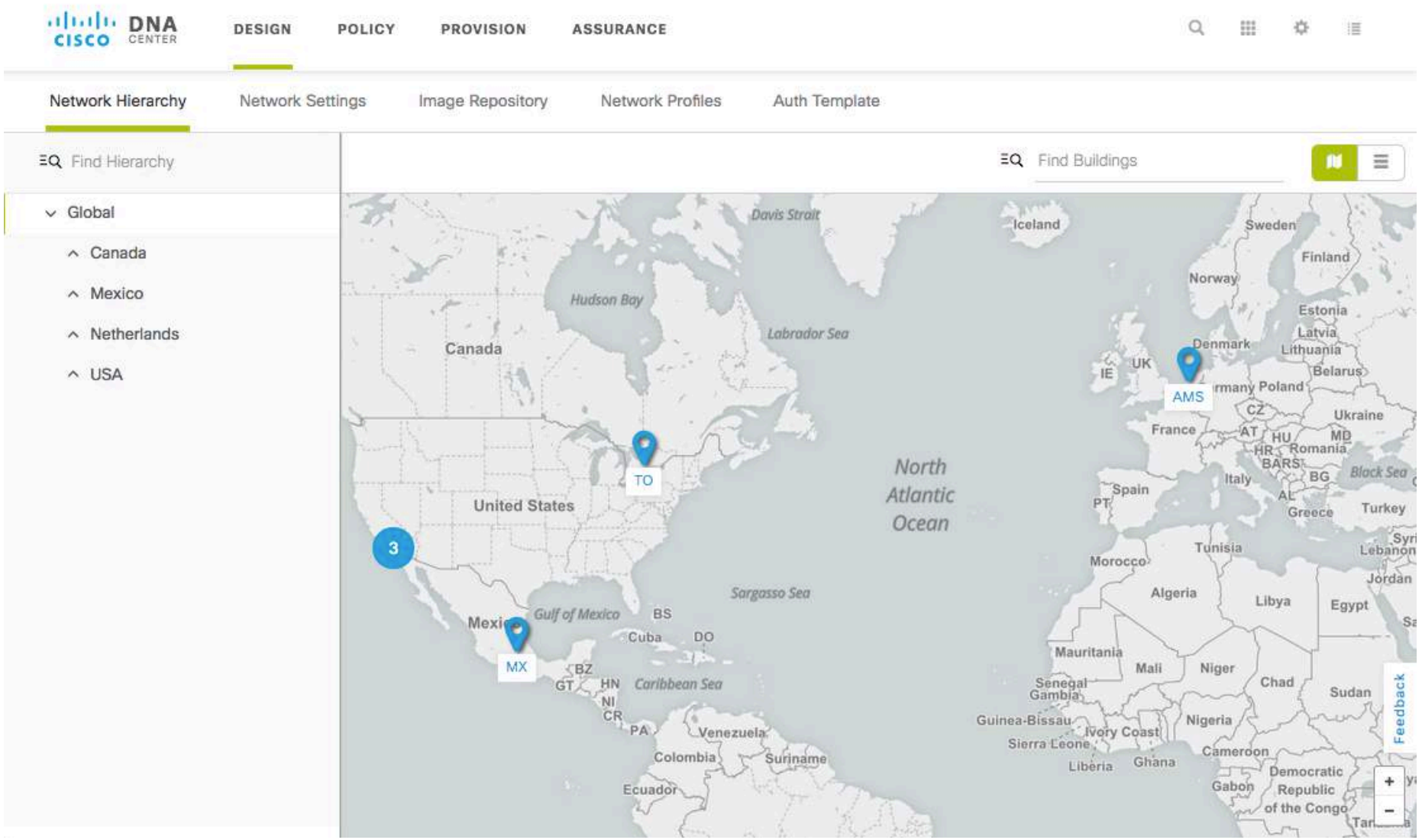
Assurance

- Issues and trends
- Performance
- Proactive troubleshooting

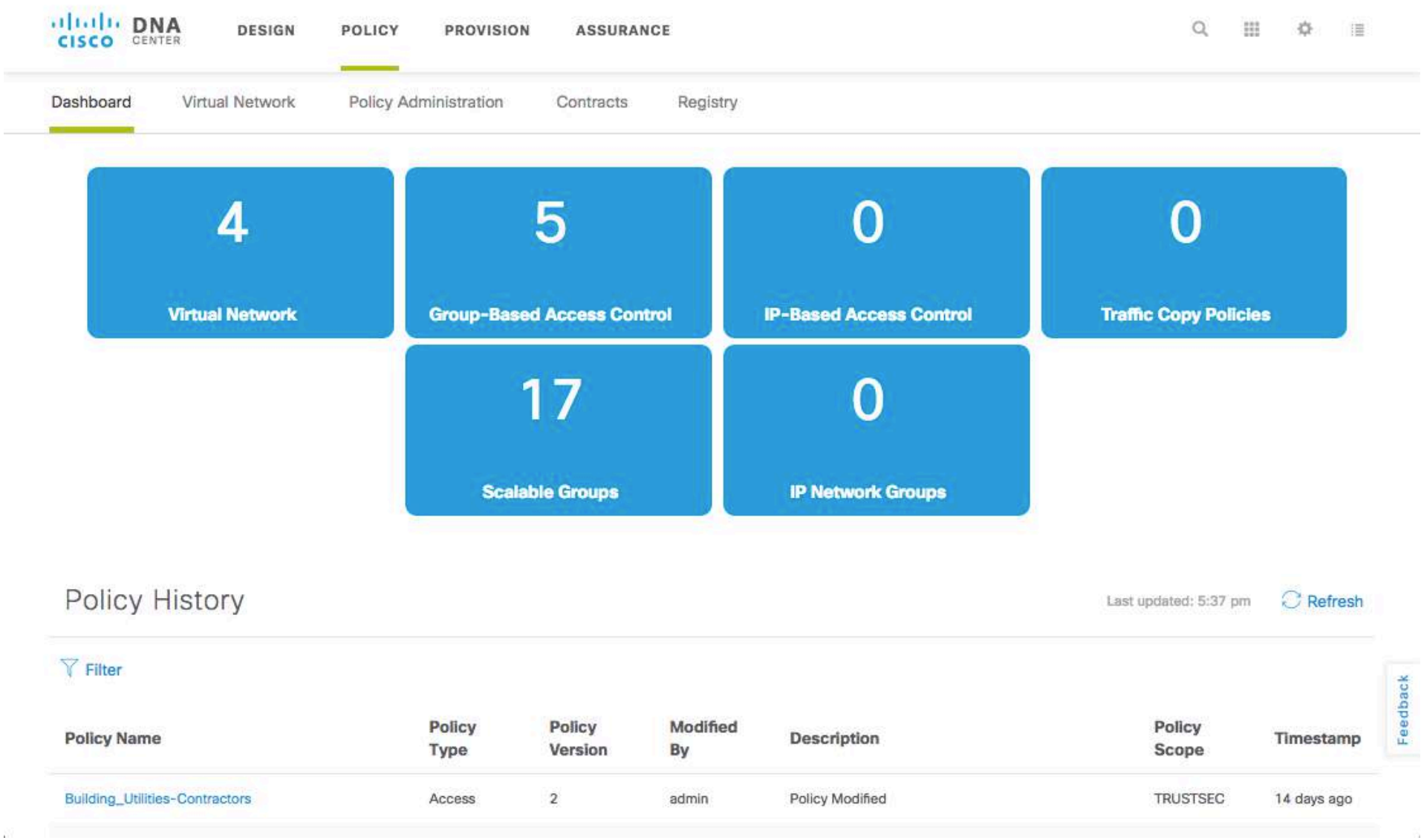
Planning, installation and migration

Proactive and predictive network, client and application assurance

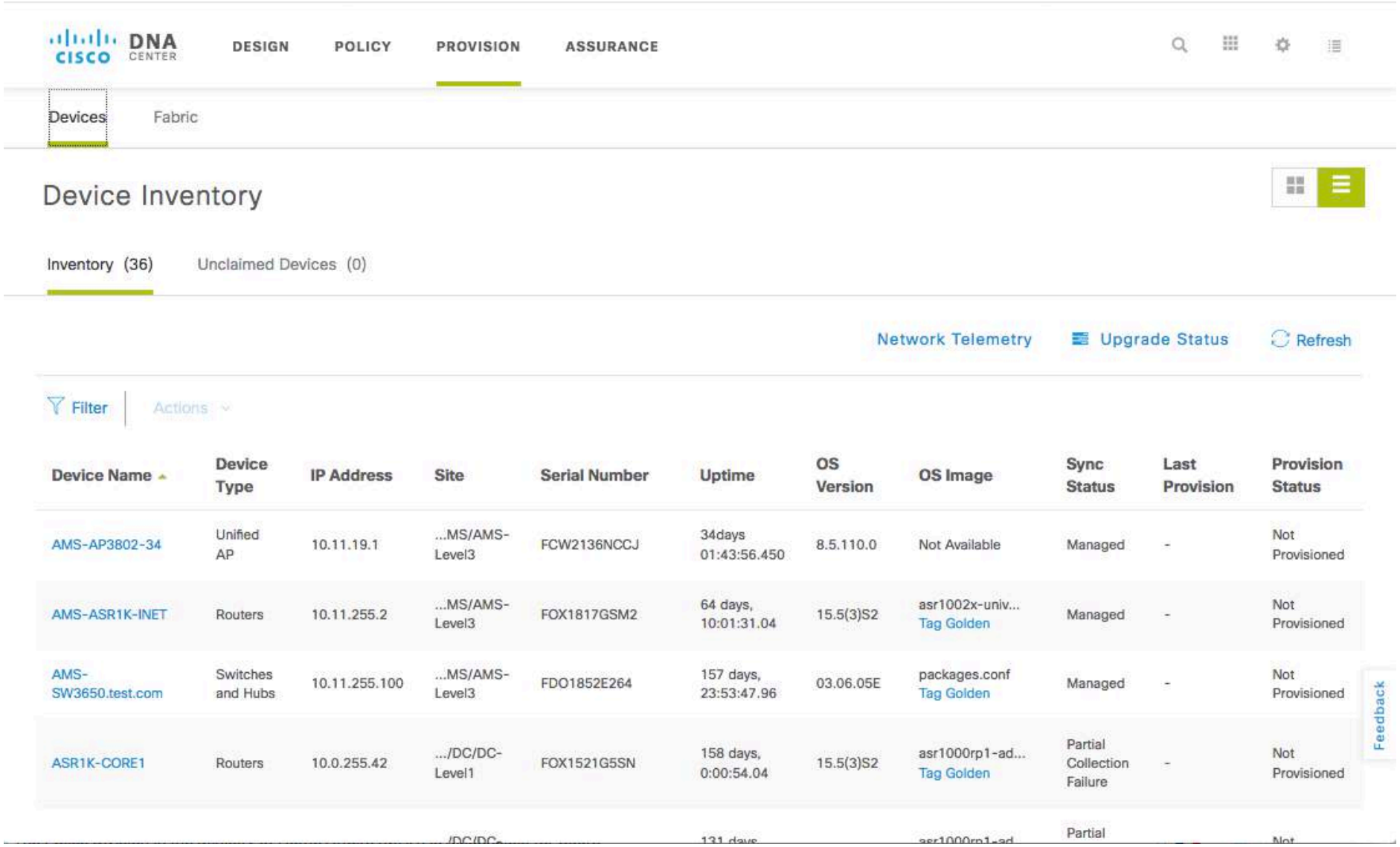
Design网络规划


DNA CENTER
DESIGN
POLICY
PROVISION
ASSURANCE
Network Hierarchy
Network Settings
Image Repository
Network Profiles
Auth Template
Find Hierarchy
Find Buildings
Global
Canada
Mexico
Netherlands
USA
AMS
TO
MX
3
Davis Strait
Iceland
Sweden
Finland
Norway
Hudson Bay
Labrador Sea
Canada
Estonia
Latvia
Lithuania
Denmark
IE
UK
Belarus
Poland
Ukraine
France
CZ
AT
HU
MD
HR
Romania
BARS
Black Sea
Italy
BG
Spain
PT
AL
Greece
Turkey
North Atlantic Ocean
United States
Tunisia
Morocco
Lebanon
Jordan
Sargasso Sea
Algeria
Libya
Egypt
Gulf of Mexico
BS
Cuba
DO
Mauritania
Mali
Niger
Chad
Sudan
BZ
GT
HN
NI
CR
PA
Caribbean Sea
Senegal
Gambia
Guinea-Bissau
Nigeria
Ivory Coast
Sierra Leone
Liberia
Ghana
Cameroon
Venezuela
Colombia
Suriname
Ecuador
Gabon
Democratic Republic of the Congo
Feedback

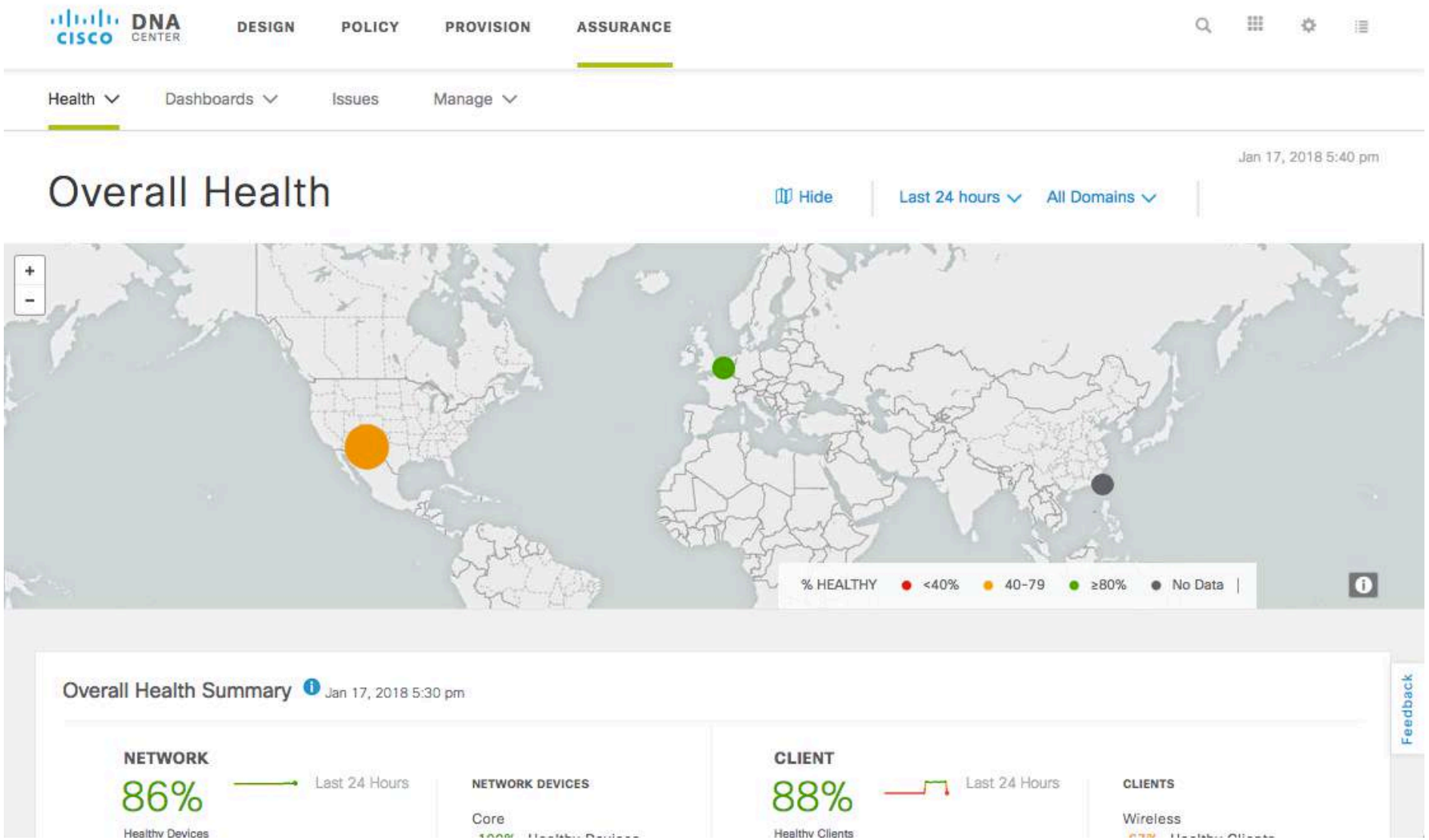
Policy策略


DNA CENTER
DESIGN
POLICY
PROVISION
ASSURANCE
Dashboard
Virtual Network
Policy Administration
Contracts
Registry
4
Virtual Network
5
Group-Based Access Control
0
IP-Based Access Control
0
Traffic Copy Policies
17
Scalable Groups
0
IP Network Groups
Policy History
Last updated: 5:37 pm
Refresh
Filter
Policy Name
Policy Type
Policy Version
Modified By
Description
Policy Scope
Timestamp
Building_Utilities-Contractors
Access
2
admin
Policy Modified
TRUSTSEC
14 days ago
Feedback

Provision网络部署



Assurance保障



DNA Center大数据平台介绍

园区网大数据分析系统架构

4：所有信息交由统一的分析系统关联，分析。使用大数据及机器自学习技术，实时、准确的提供分析结果，而无需专业人员介入

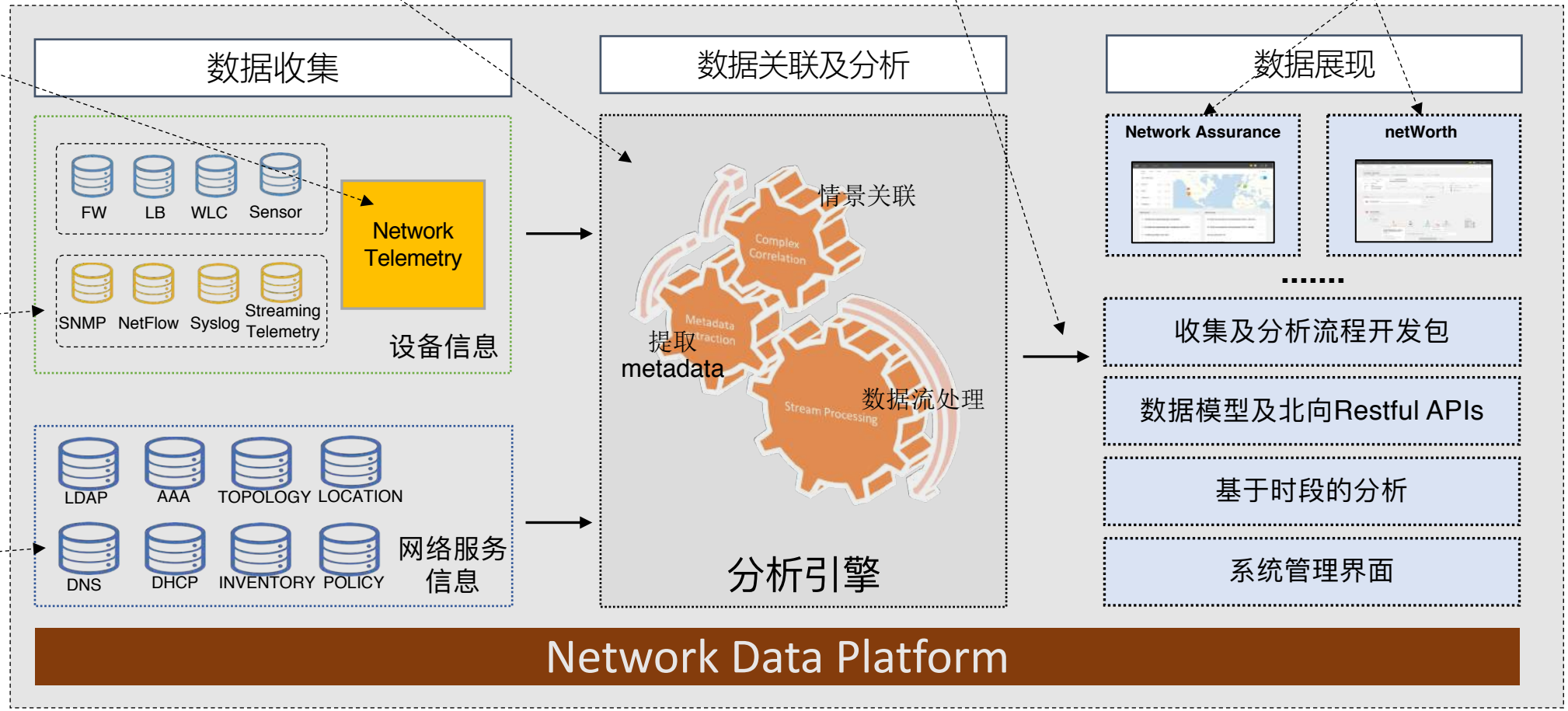
5：分析结果可由北向接口输出，采用Restful+Json通用接口规范以及SDK，易于用户二次开发

6：思科同时提供前段展示图形化界面

3：设备状态信息可由设备主动发出，频率可达10秒一次，可避免SNMP Polling间隔时间过长问题

1：收集所有网络设备的状态信息，包含NetFlow，Syslog等

2：统一收集网络服务系统的信息，包含DHCP，AAA等

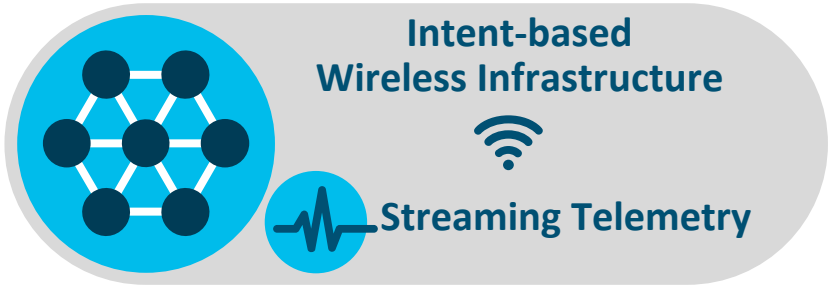


传统数据收集方式 vs 思科Telemetry

传统方式

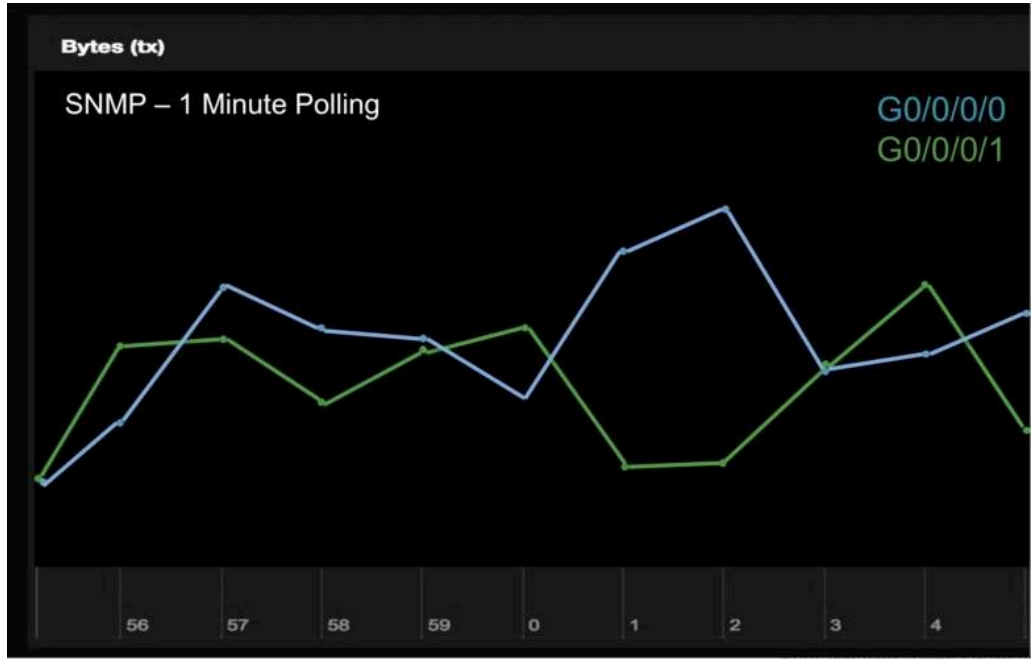
SNMP / Legacy data pull methods

Telemetry

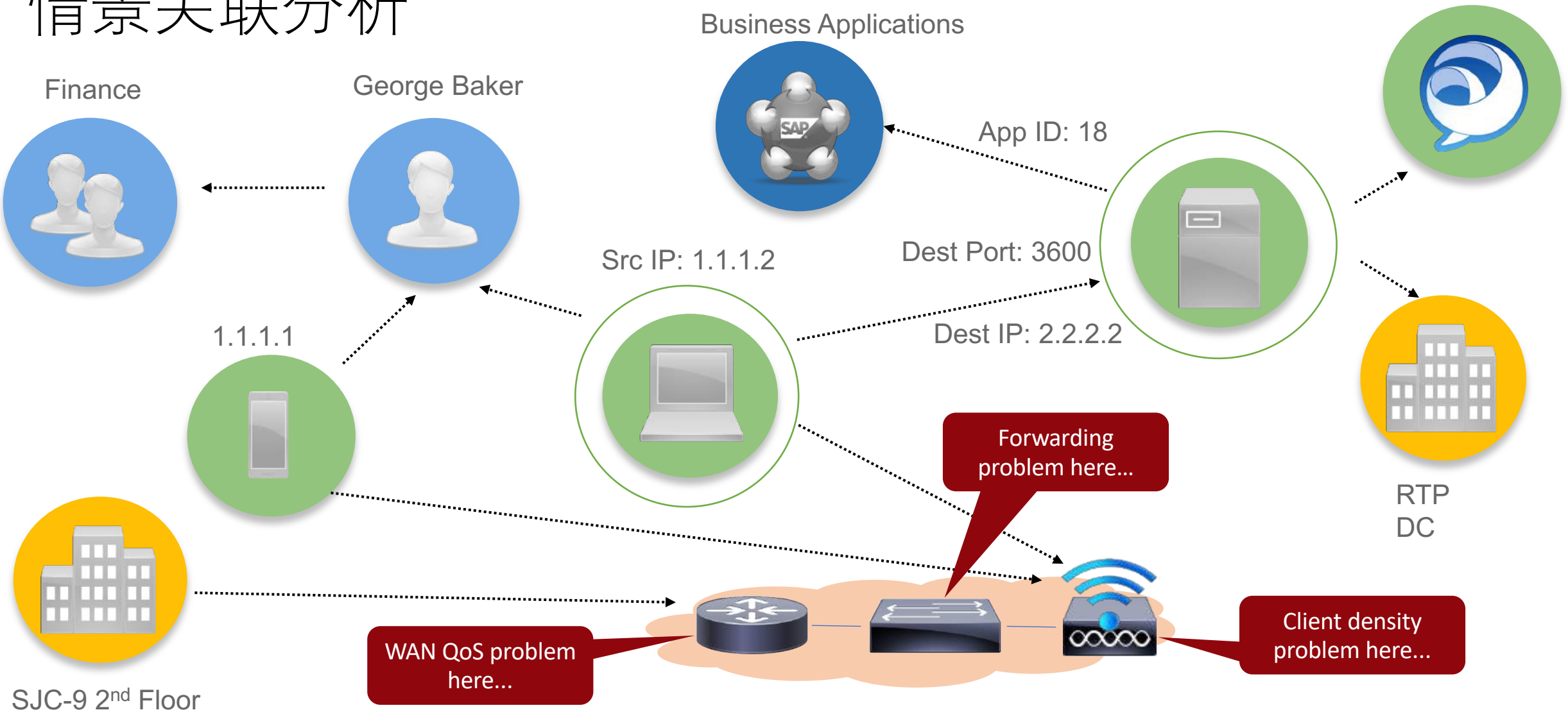


Pull方式数据导入	→	Push方式设备导出
CPU消耗严重	→	低CPU消耗
密集数据直接导出	→	优化后YANG Model导出数据，更低带宽消耗
不支持实时通告和事故报警	→	发生任何变更立即发送通告
最轻量级轮询丢失重要信息	→	管理数据低延时保证

Telemetry和SNMP的对比



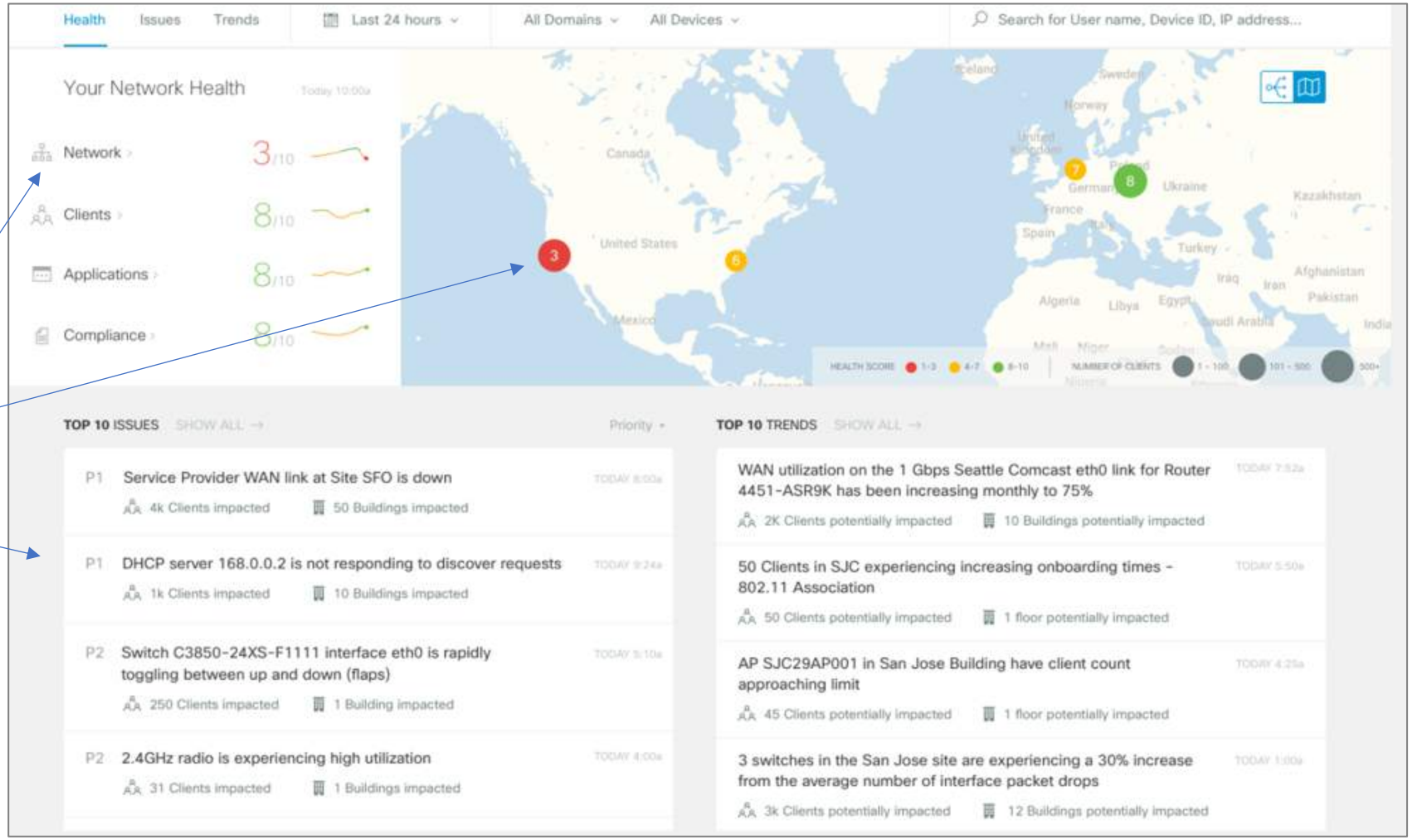
情景关联分析


Business Applications
Finance
George Baker
App ID: 18
Src IP: 1.1.1.2
Dest Port: 3600
Dest IP: 2.2.2.2
1.1.1.1
Forwarding problem here...
RTP DC
WAN QoS problem here...
Client density problem here...
SJC-9 2nd Floor
Netflow
AVC
DDI
ISE/Radius
Topology
CMX, DNAC
Device

大数据分析的威力–场景一

登录页显示:

1. 网络，用户和应用的健康状况小结
2. 各个站点的情况，哪里问题最严重
3. 当前网络中排名前十的问题



大数据分析的威力–场景二

大数据情景关联分析:

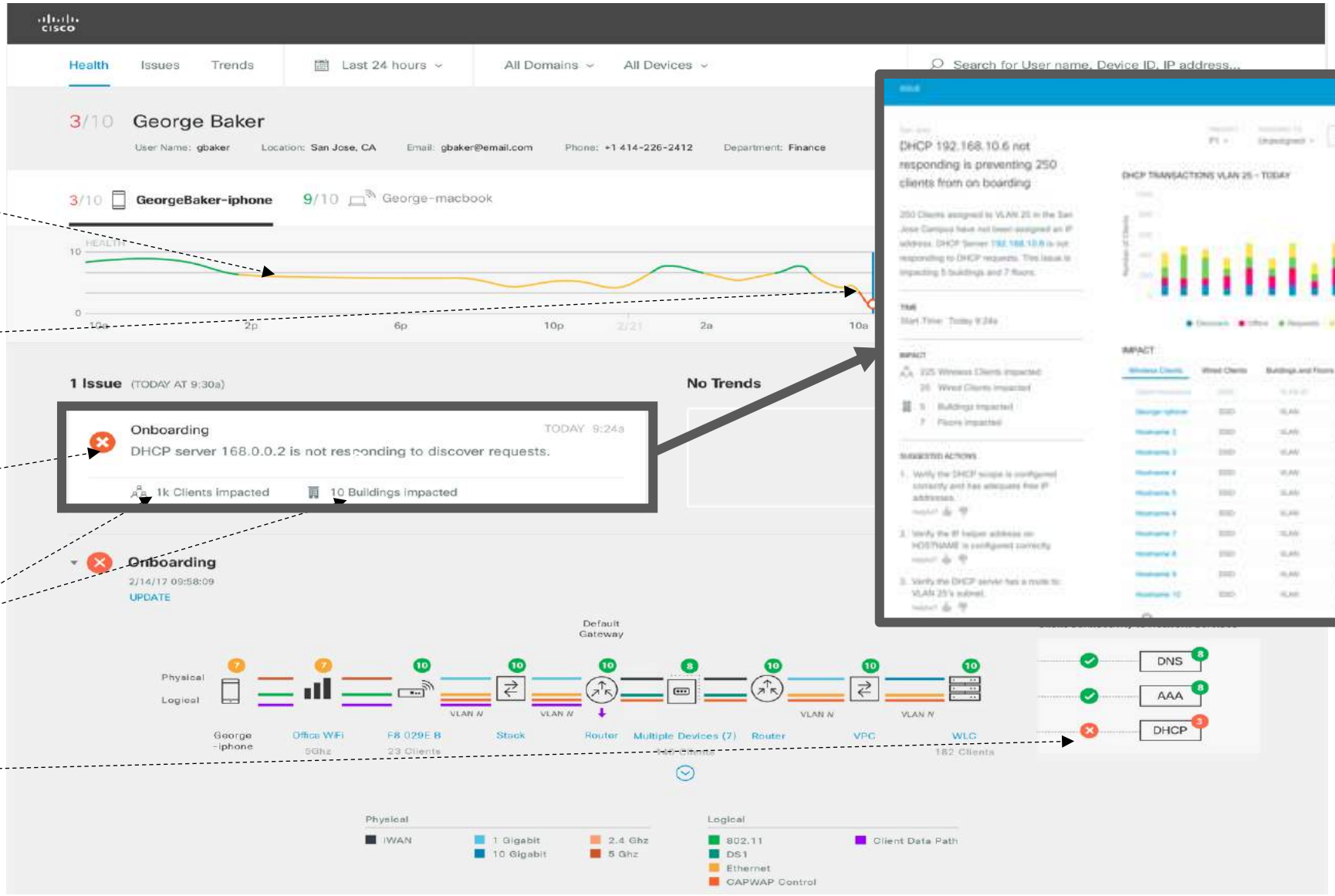
1：GeorheBaker的iphone在黄线所显示的时间段，使用体验出现不良状况

2：GeorheBaker的iphone在红线所显示的时间点无法接入网络，时间大概是在上午9:30左右

3：GeorheBaker的iphone无法接入的原因是没有收到DHCP Server 分配的IP地址

4：同样的故障影响到1K个客户端，分布在10个建筑中

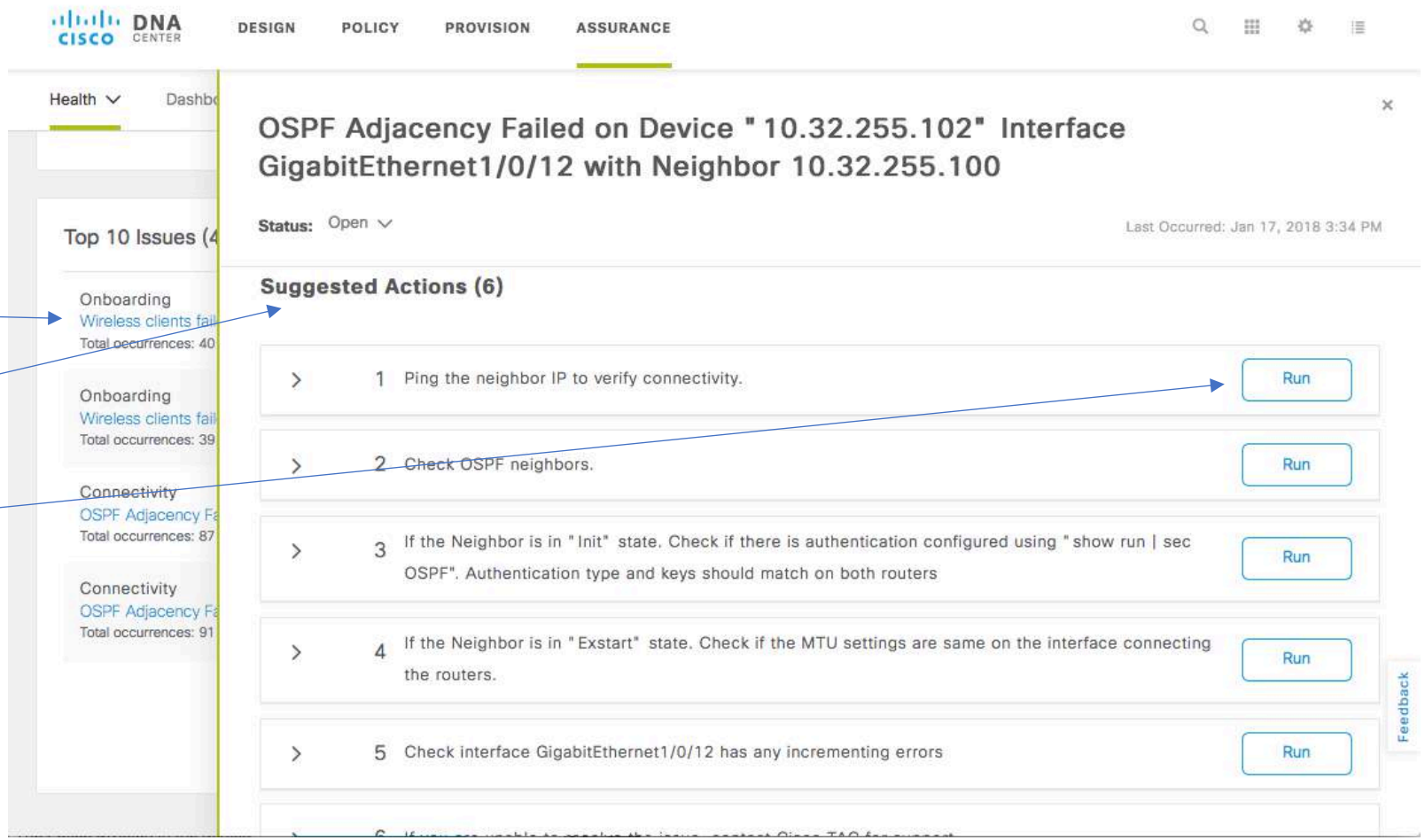
5：通过路径示意图，可以发现网络联通性没有问题，故障原因是DHCP Server出现故障



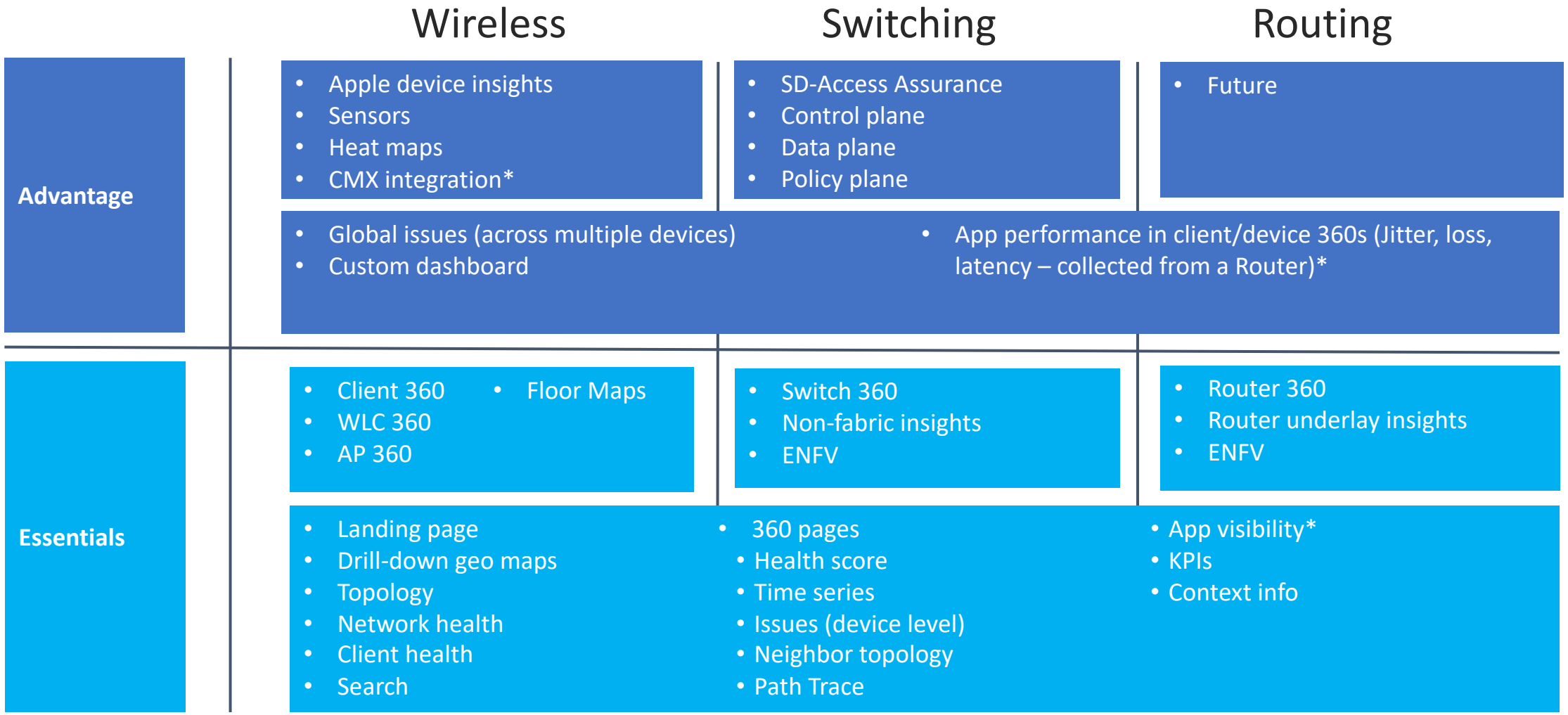
大数据分析的威力–场景三

解决方案:

1. 选择网络问题
2. 大数据平台分析问题，给出解决方案
3. 点击Run运行检测功能



思科DNA Assurance软件License(1.1版本)



* Jan'18 - @ Launch

DNA Center安全解决方案集成

防火墙选项

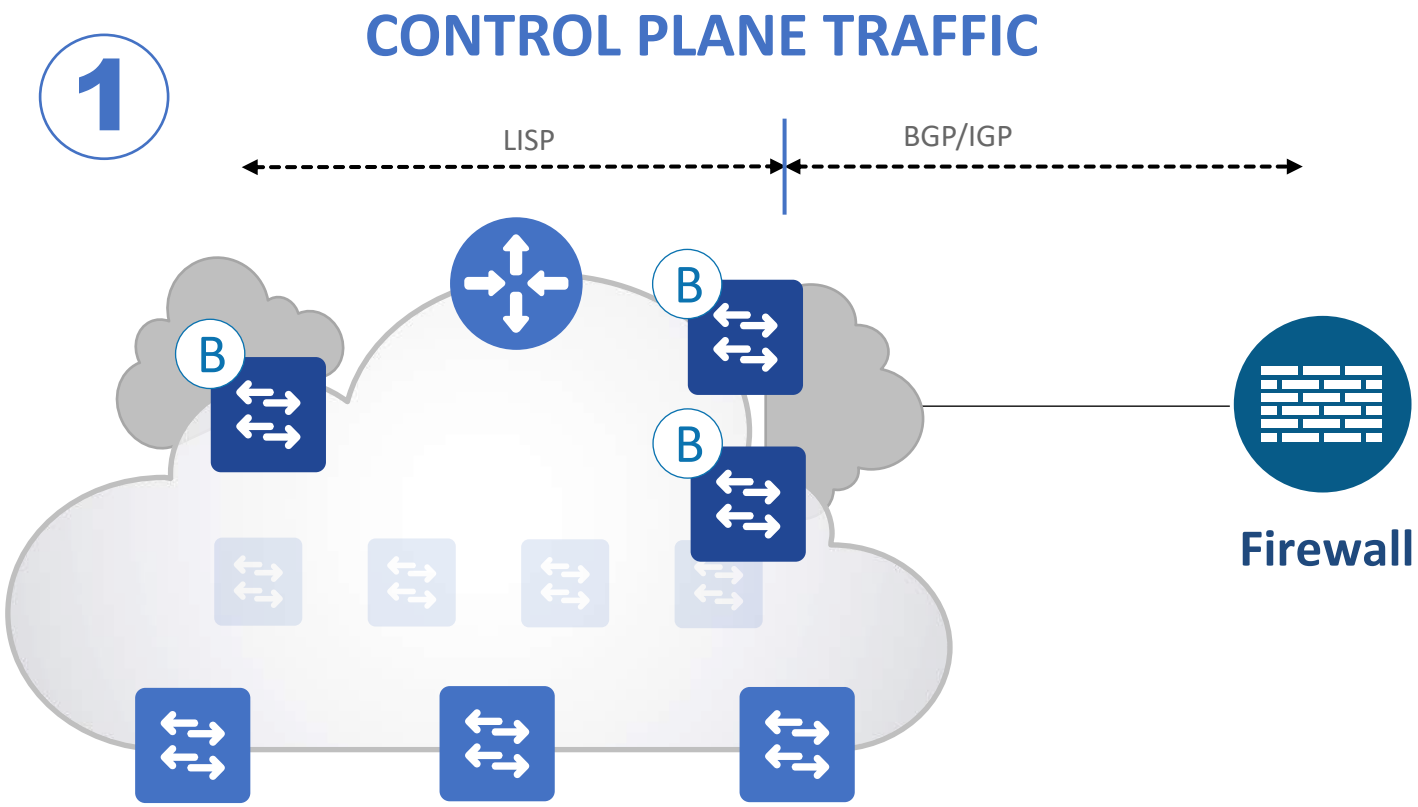
Non-Cisco Firewall:

- 从外部连接到Fabric
- 园区网内部Ip地址通过路由协议发送给防火墙
- **防火墙策略基于接口、子网IP、掩码和IP ACL**

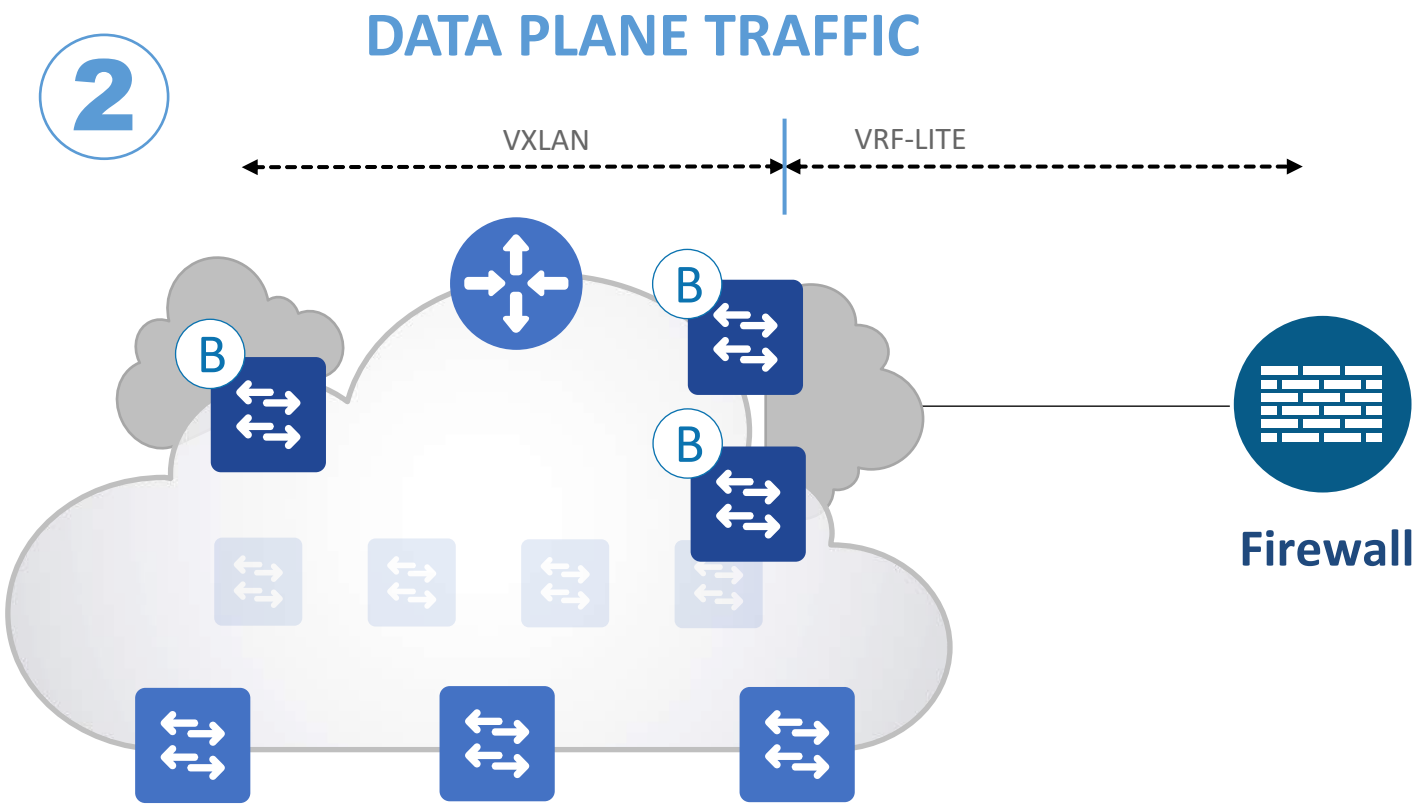
Cisco Firewall :

- 从外部连接到Fabric
- 园区网内部Ip地址通过路由协议发送给防火墙
- **基于思科TrustSec框架，在ISE和防火墙之间建立SXP连接，给防火墙传递SGTs**
- **防火墙策略基于SGT和SGTACL**
- 防火墙也支持基于接口和IP子网的策略来兼容brownfield

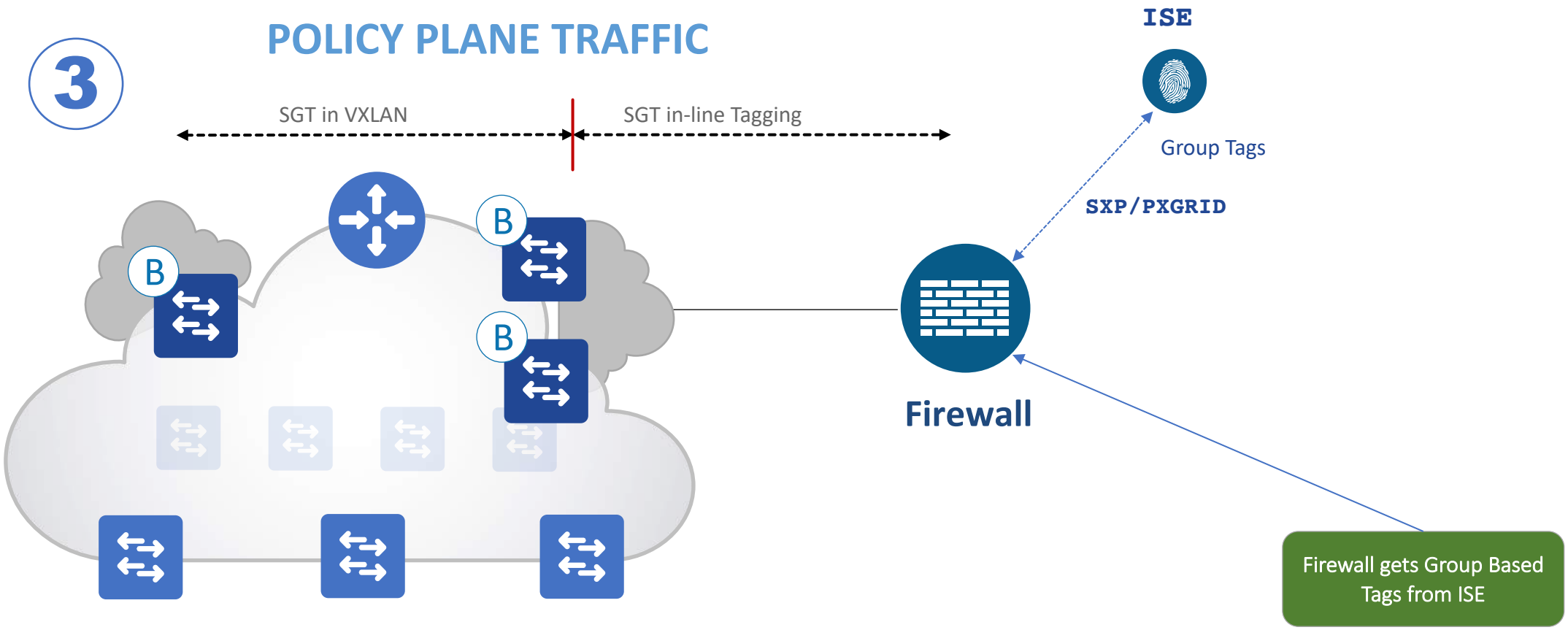
防火墙部署 – 控制平面



防火墙部署 – 数据平面



防火墙部署 – 策略平面


POLICY PLANE TRAFFIC
3
SGT in VXLAN
SGT in-line Tagging
B
B
B
ISE
Group Tags
SXP/PXGRID
Firewall
Firewall gets Group Based Tags from ISE

Q & A