拨开迷雾 - 我们需要怎样的SD-WAN

周剑

SD-WAN

Technical Solutions Architect

思科SD-WAN:
市场份额第一；获颁CRN年度产品奖

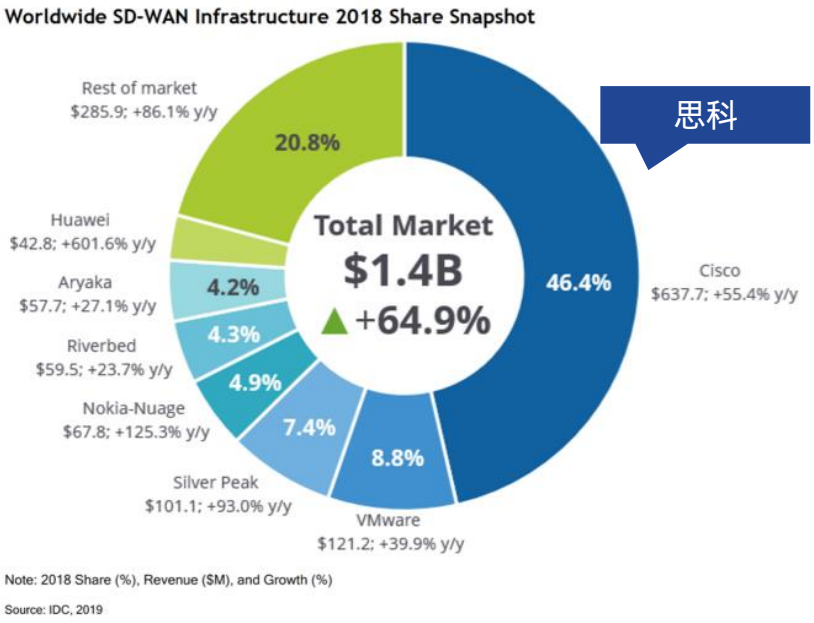
CRN 2019 年度产品奖

THE CHANNEL CO. CRN Products of the YEAR 2019

最佳软件定义
广域网产品

- 该奖项由合作伙伴投票评选，思科不仅赢得整体奖项，还横扫3个评选标准：
  - 技术
  - 收入和利润
  - 客户需求

市场份额第一，占46% @ IDC报告



WAN的变化

新应用：云、视频、IoT……

安全

架构：互信、准入、分段
互联网访问：防火墙、IPS、url过滤...

混合 WAN

组网

架构：扩展、容错
组网：路由、任意拓扑、策略、安全、流量工程、迁移
选路：多层复杂网络、多数据中心
体验：SLA、QoS

运维

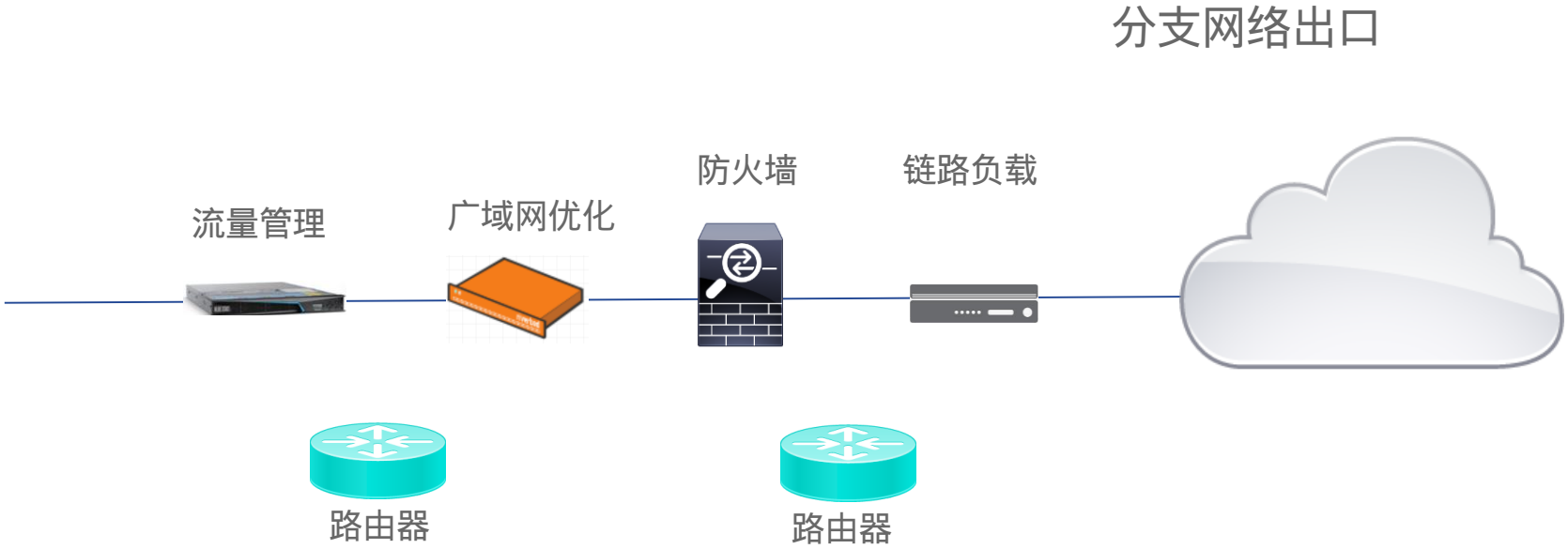
简易、可视、一致

SD-WAN：为什么大家都在做？

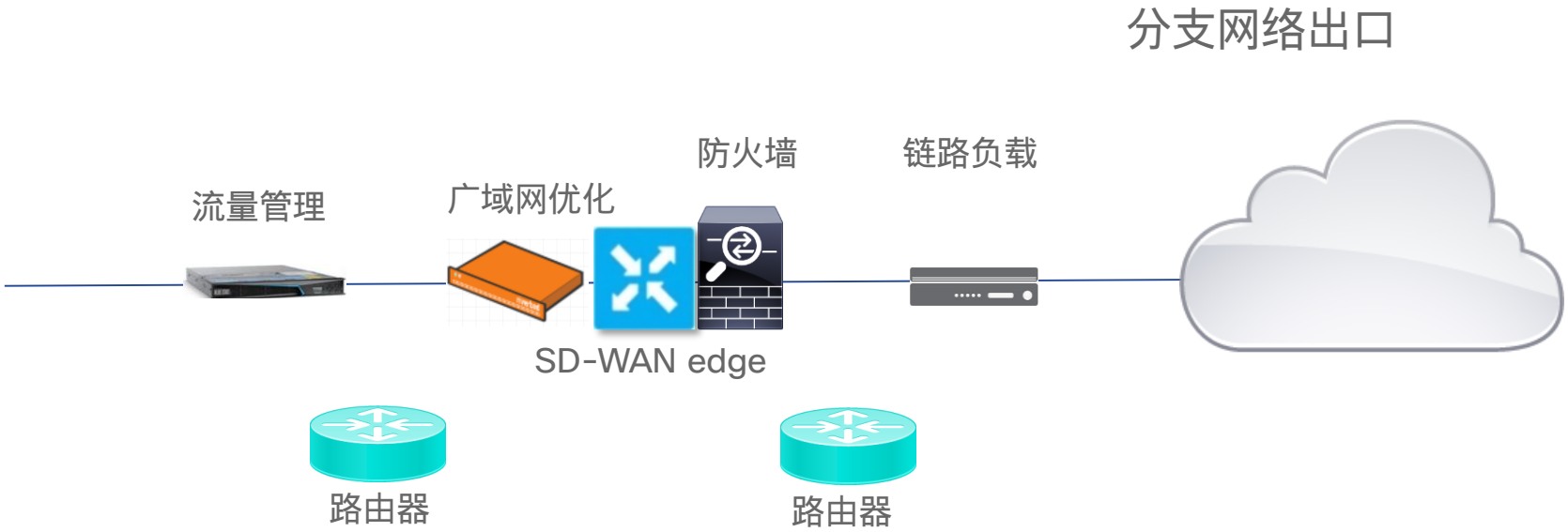
各种场景化需求

- 安全
- 应用识别与分类
- 流量可视化
- 链路负载
- QoS
- WAN优化
- 多云互联
- 等等

场景化需求的背后

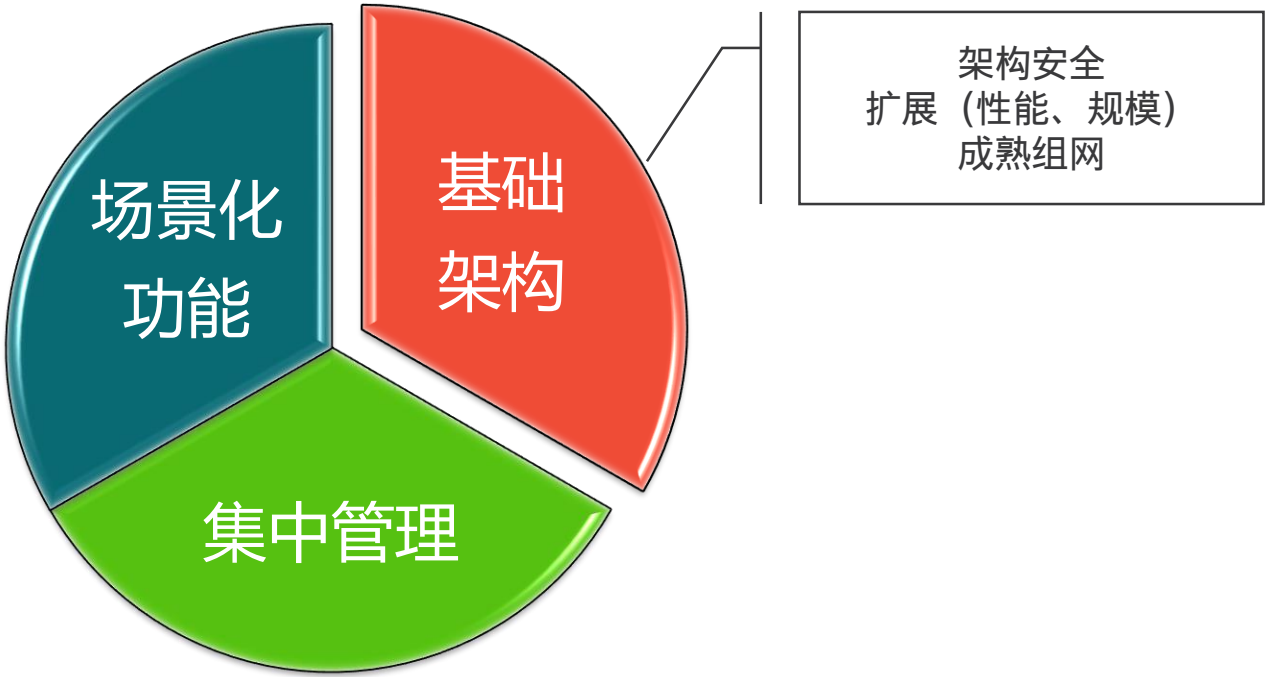


场景化需求的背后

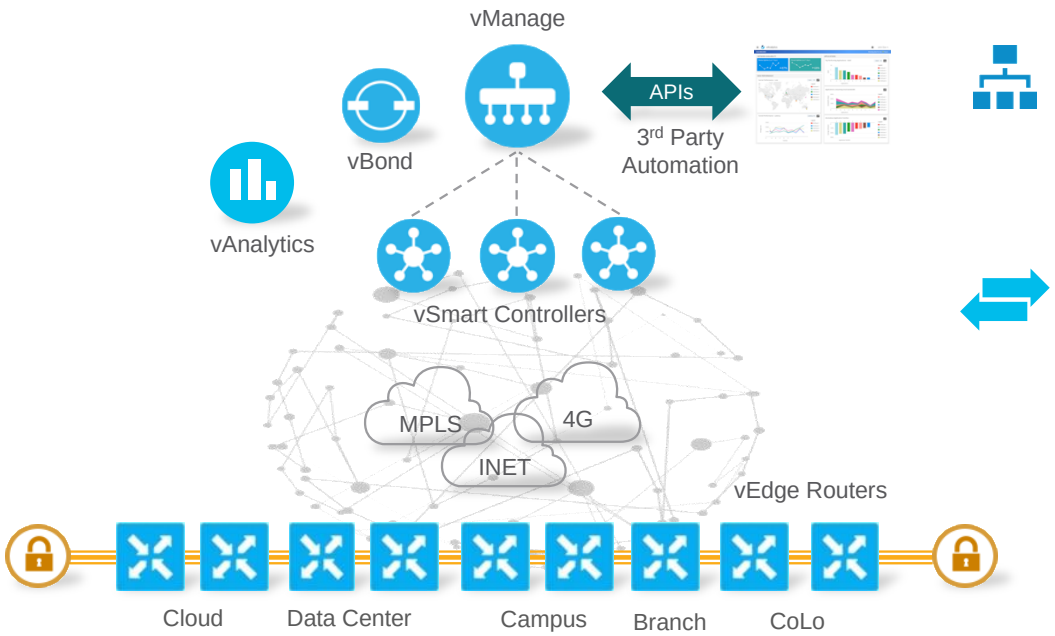


网络架构是场景化实现的基础

SD-WAN网络构建的要点



基础架构
解决方案核心组件



Orchestration = vBond

- 对控制和管理平面的统一编排
- 第一认证和注册点
- 将vSmart/vManage列表转发给所有vEdge

Management = vManage
(Multi-tenant or Dedicated)

- 对SD-WAN网络的配置和管理
- Policy template的集中管理
- GUI界面，简单易用
- API：Rest北向接口

Control Plane = vSmart
(Containers or VMs)

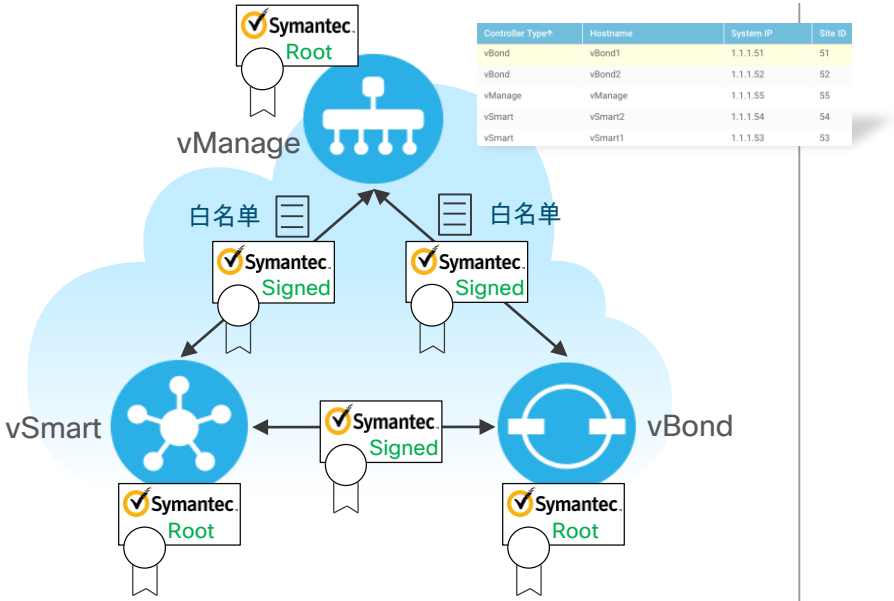
- 与vEdge共同形成控制平面
- 在vEdge之间分发数据平面和策略信息
- 实施控制平面策略

Data Plane = vEdge
(Physical or Virtual)

- SD-WAN路由器，形成数据平面。
- 执行数据转发和策略
- 与现有网络通过路由协议连接

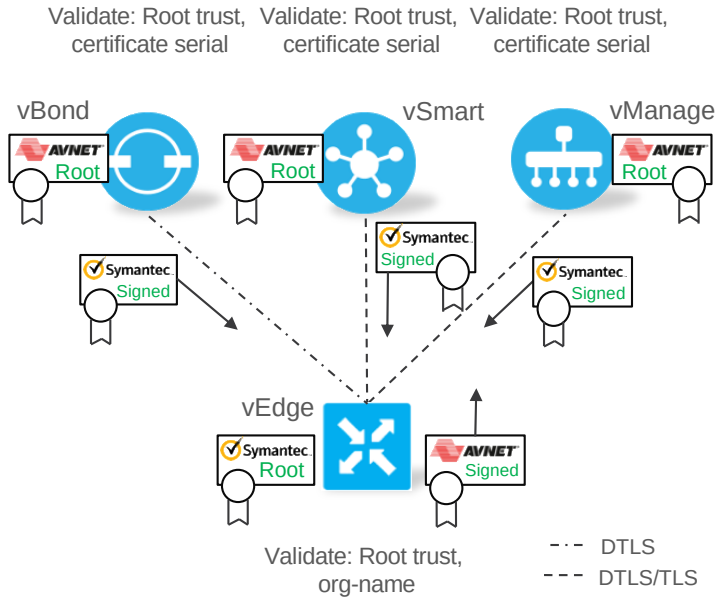
基础架构

安全：组件之间的证书认证 – Zero Trust



Controller Type	Hostname	System IP	Site ID
vBond	vBond1	1.1.1.51	51
vBond	vBond2	1.1.1.52	52
vManage	vManage	1.1.1.55	55
vSmart	vSmart2	1.1.1.54	54
vSmart	vSmart1	1.1.1.53	53

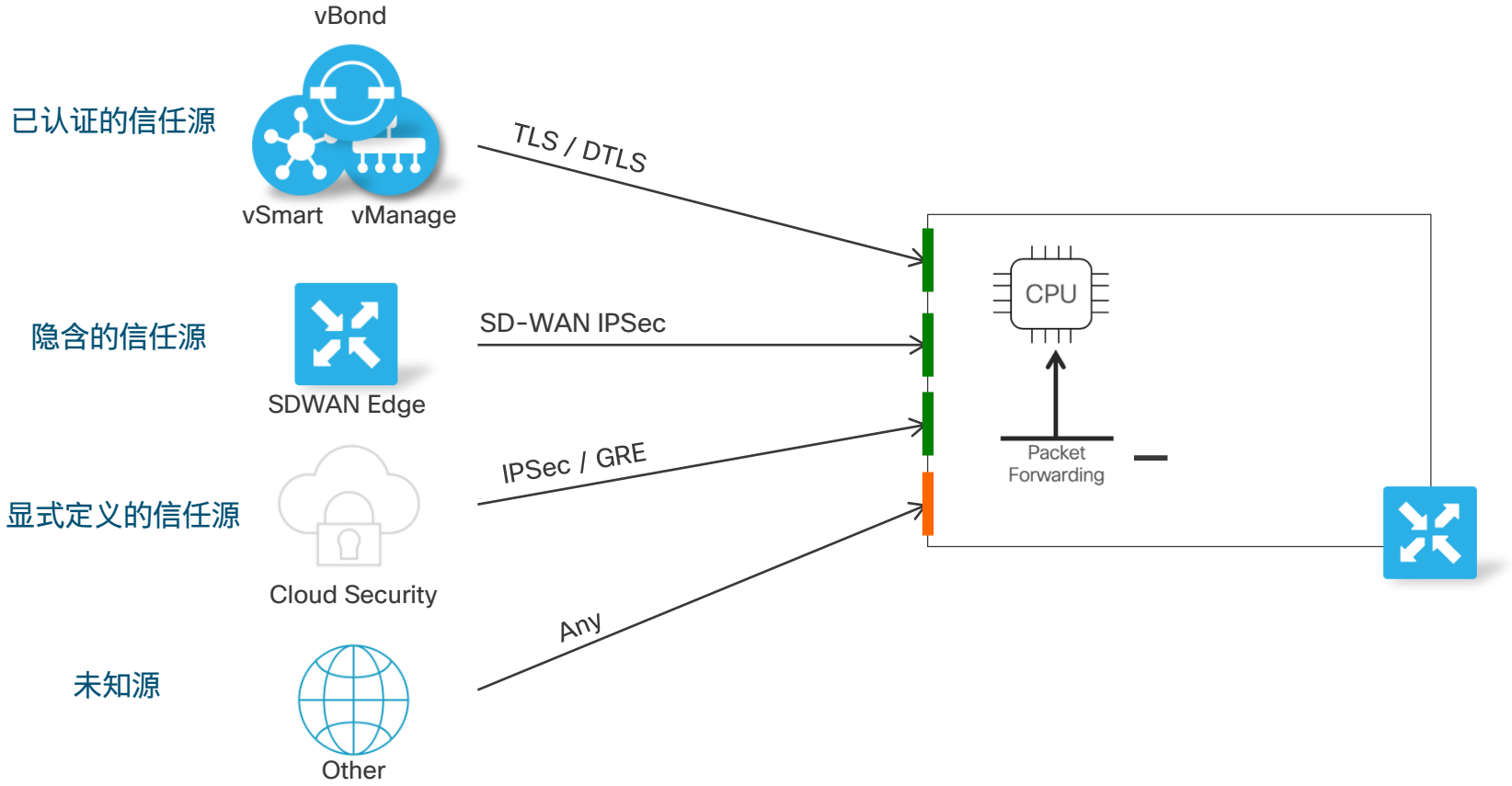
- 通过白名单定义允许入网的Edge设备
- 企业CA证书实现控制器间的相互认证



- Controller验证Edge的证书，org-name，白名单等
- Edge验证controller的证书

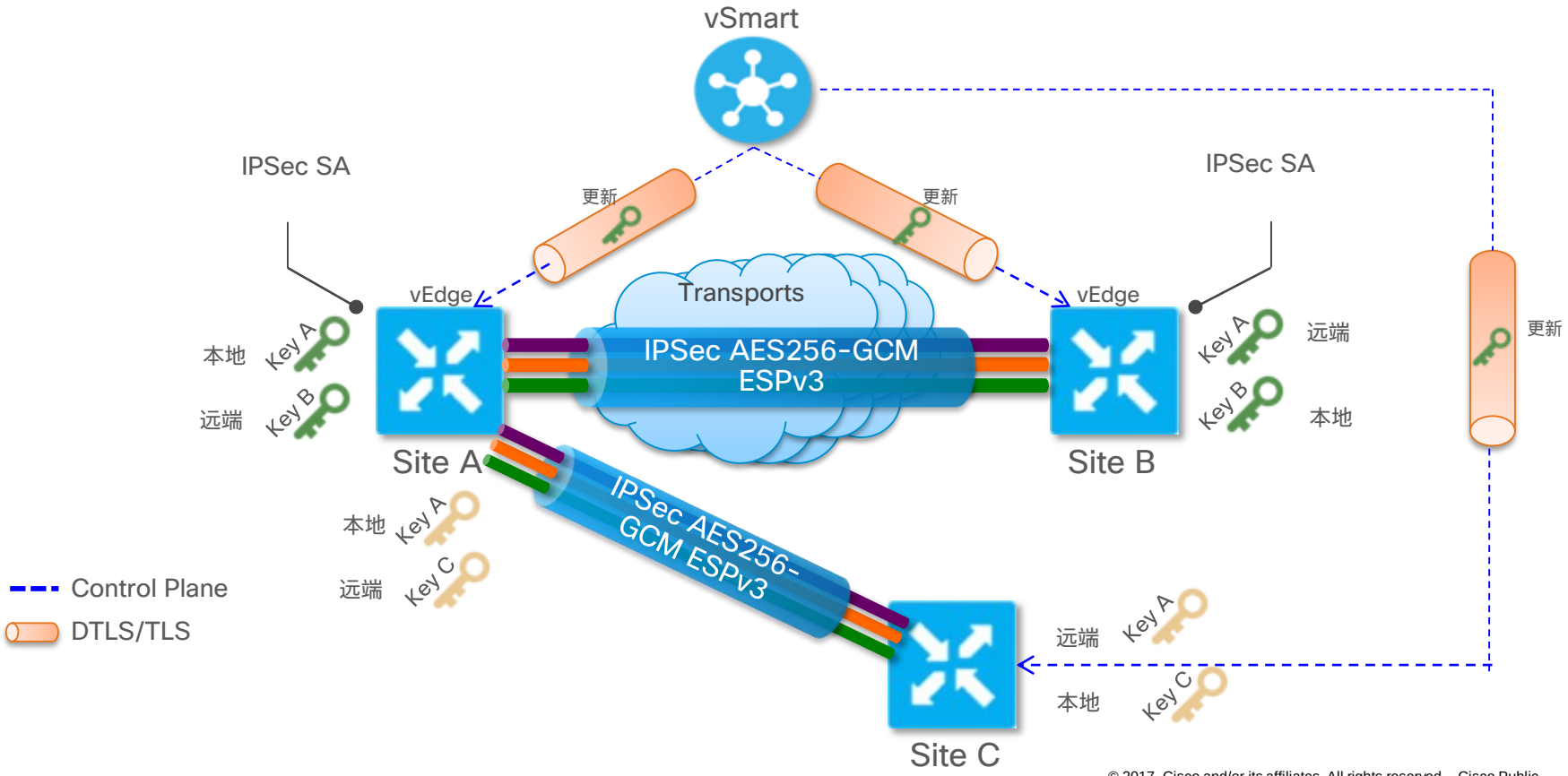
基础架构

安全：DDoS 保护



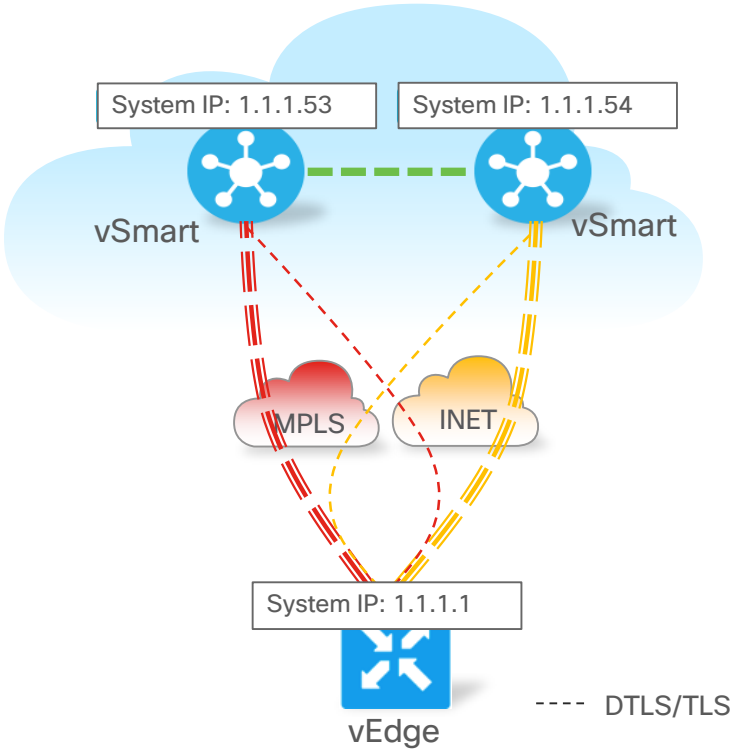
基础架构

安全：数据平面端到端安全

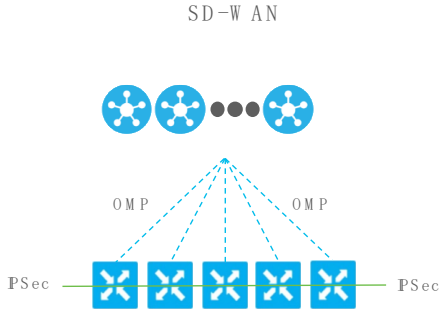


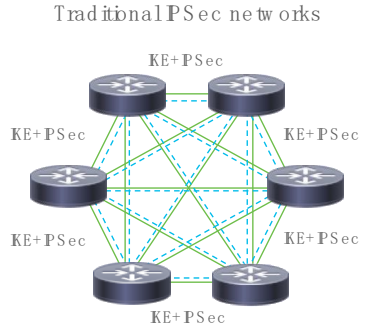
基础架构

扩展：控制层完全分离 – OMP协议



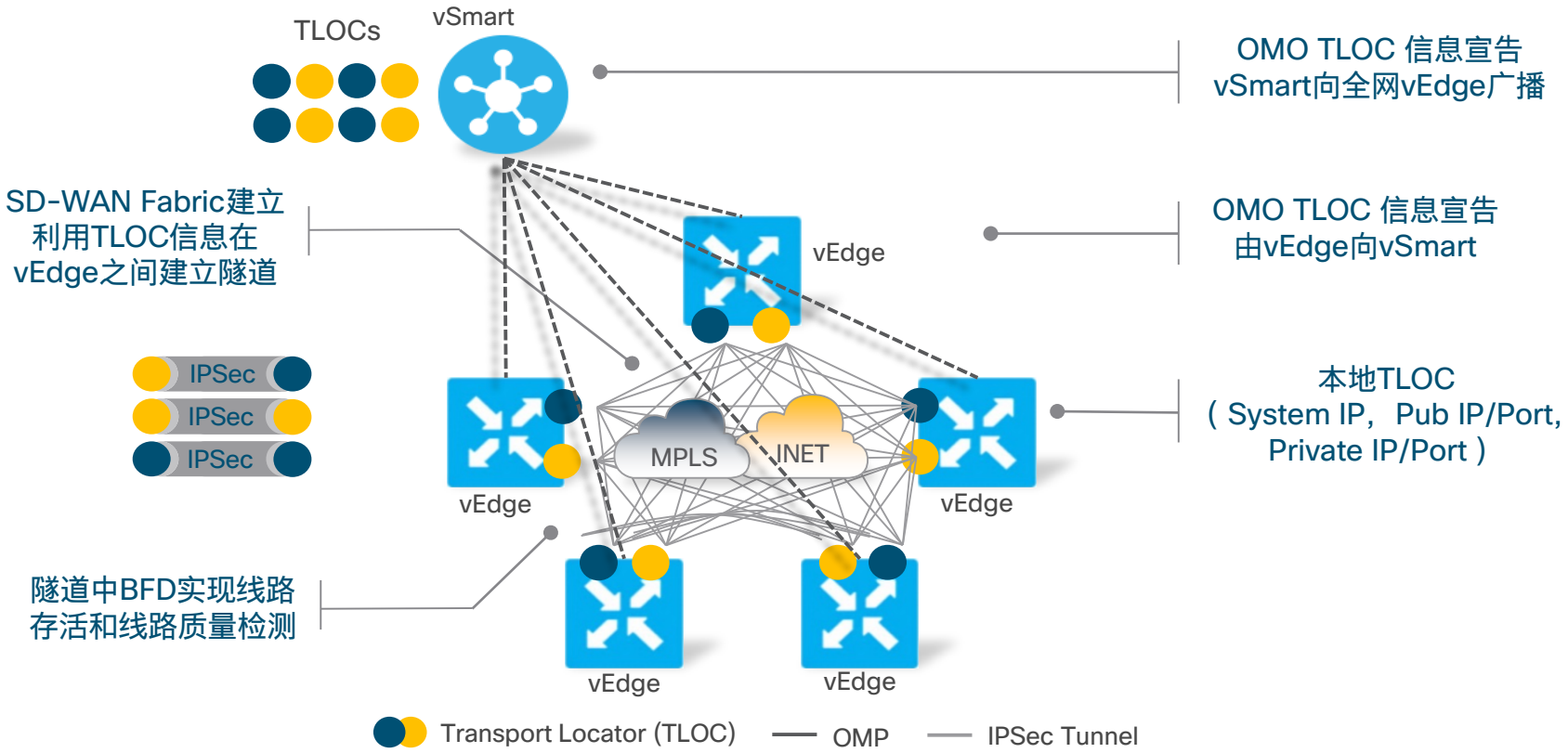
- 专用管理控制协议：OMP（Overlay Management Protocol）
- OMP在vEdge和vSmart之间建立，传递网络控制信息
  - 路由
  - IPSec密钥
- 极大的降低了控制平面的复杂度，网络扩展性大大增强
  - Edge性能
  - 网络规模
  - 管理运维能力





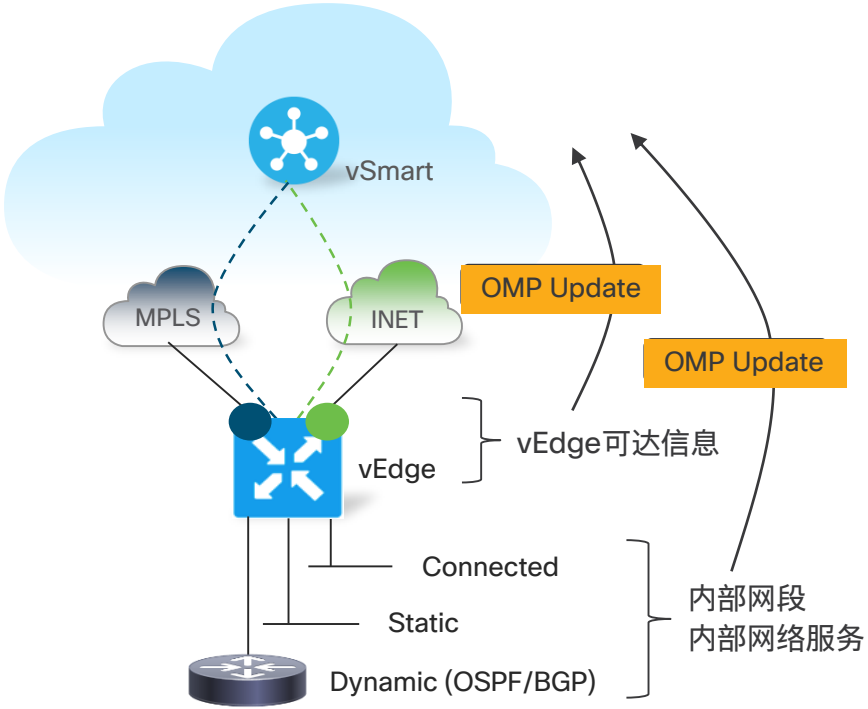
基础架构

组网：OMP协议自动VPN



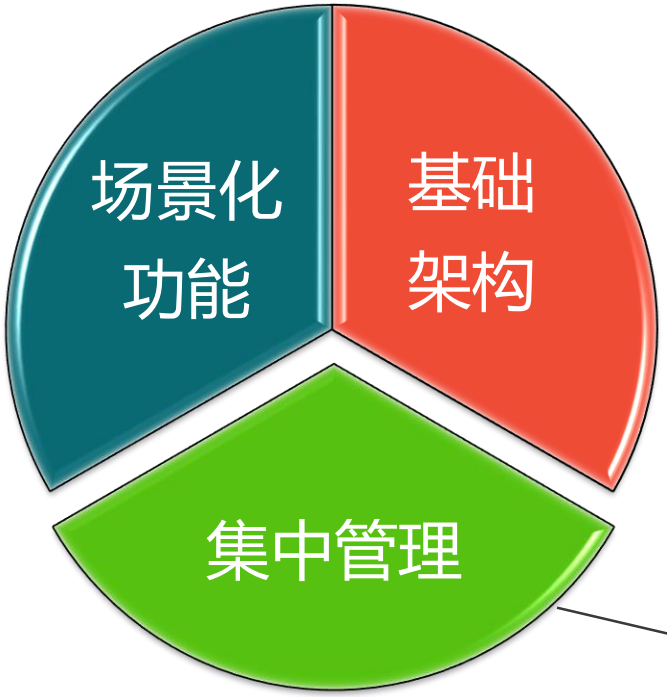
基础架构

组网：全网一致的路由视图



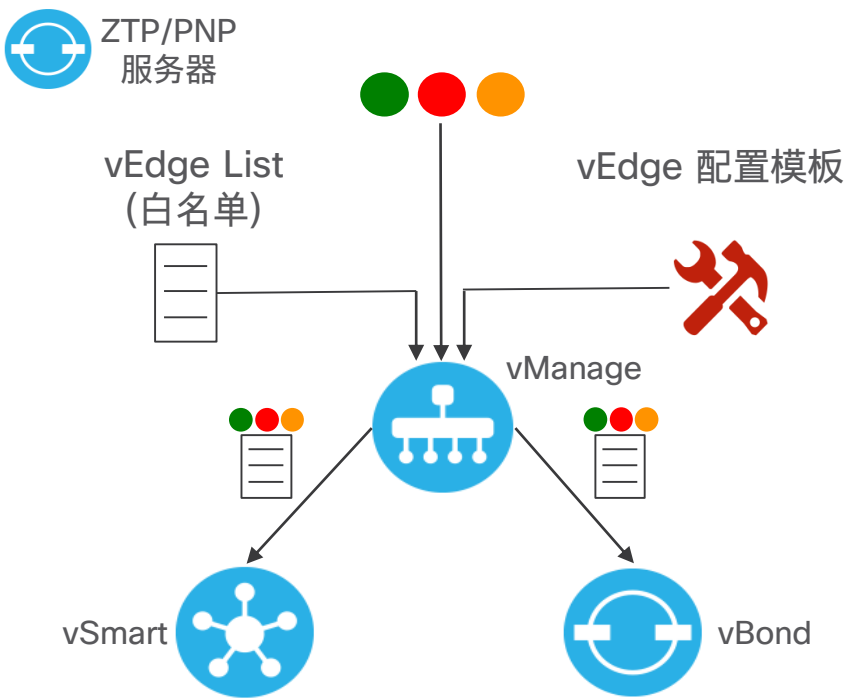
- vEdge向vSmart宣告如下信息：
  - vEdge自身的可达性信息（TLOC），用于建立vEdge间的IPSEC连接，支持动态IP和NAT后的IP
  - vEdge本地学到的内网网段信息，可包括直连路由、静态路由、OSPF/BGP路由
  - vEdge本地支持的网络服务，比如防火墙、IPS等
- 每台vEdge只向vSmart宣告，vSmart广播到全网
- 全网路由视图始终保持一致

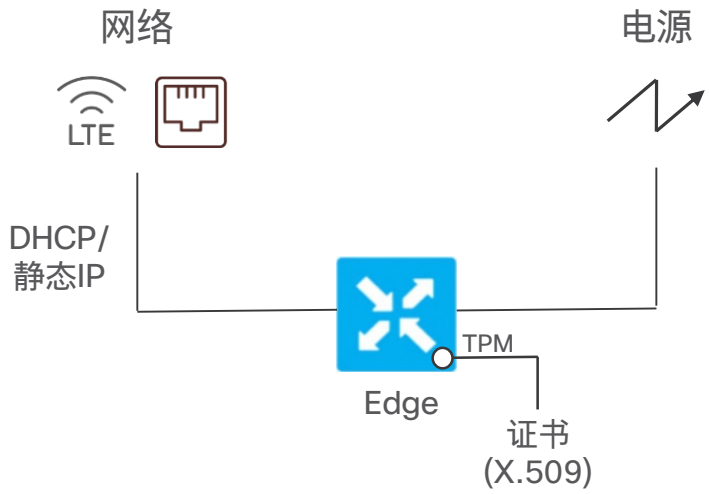
SD-WAN网络构建的要点



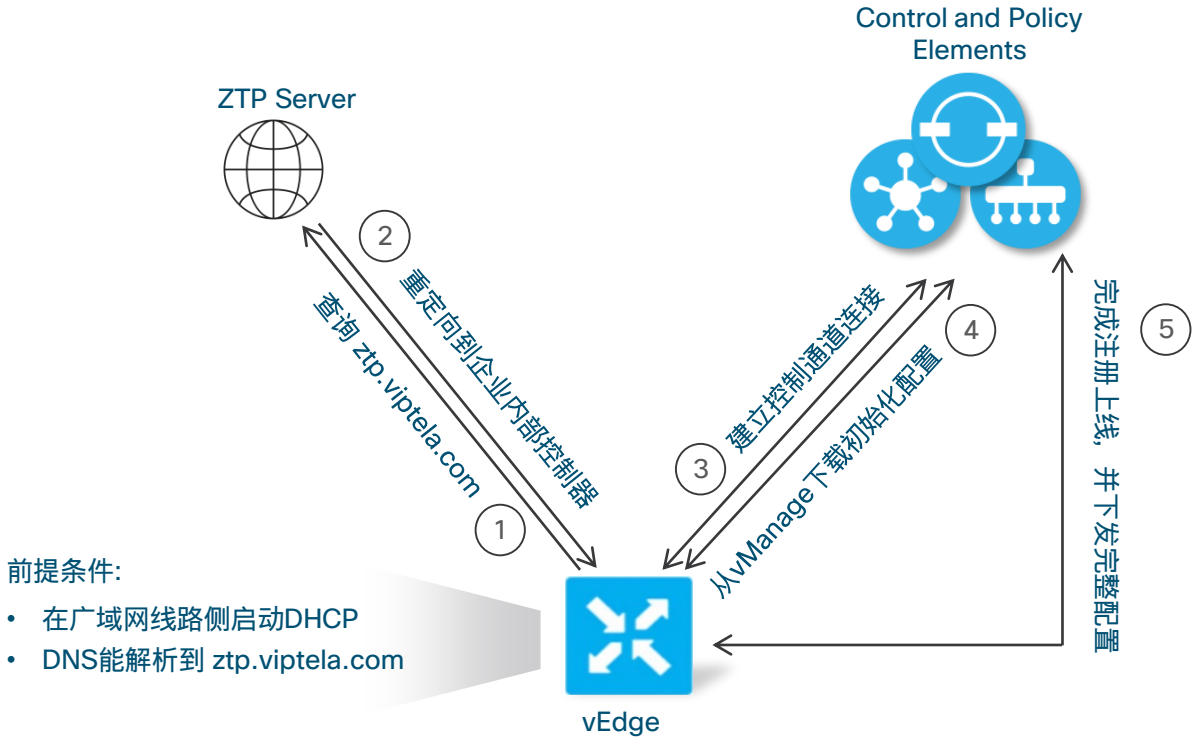
ZTP (零接触部署)
全网统一视图
集中策略配置与下发
完善的排障工具

集中管理
零接触部署





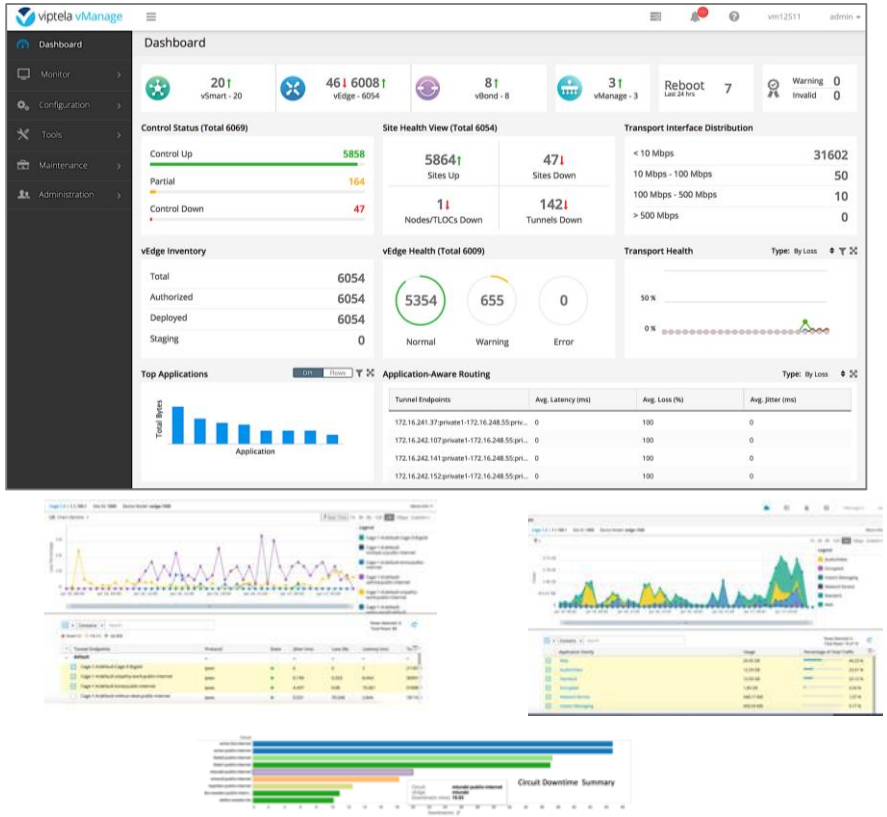
集中管理
零接触部署



前提条件:

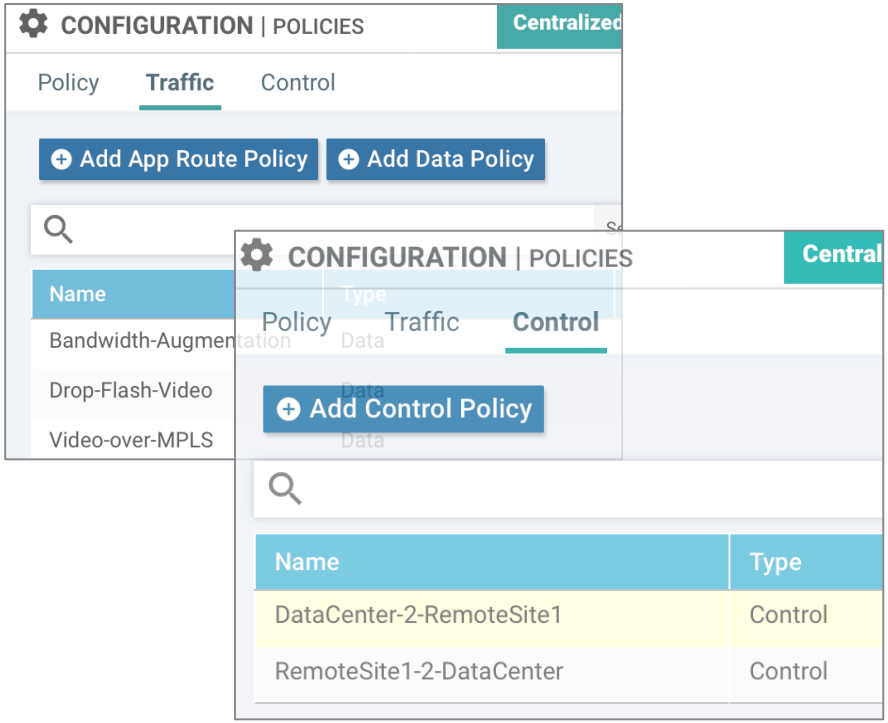
- 在广域网线路侧启动DHCP
- DNS能解析到 ztp.viptela.com

集中管理
全网统一视图



- 全GUI操作界面
  - 管理、监控、排错
- 云端或本地部署
- 单租户/多租户
- RBAC
- 可集群配置支持扩展与高可用
- REST APIs

集中管理
精细的策略控制



- 多样的策略类型 - 控制策略、数据策略以及应用感知的策略
- vManage中统一定义与下发，由vSmart（控制策略） 或 vedge（数据与应用感知策略）执行
- 应用于不同的站点集合

集中管理
故障排查

Connectivity

Device Bringup

Control Connections(Live View)

Ping

Trace Route

Speed Test

Traffic

Tunnel Health

App Route Visualization

Packet Capture

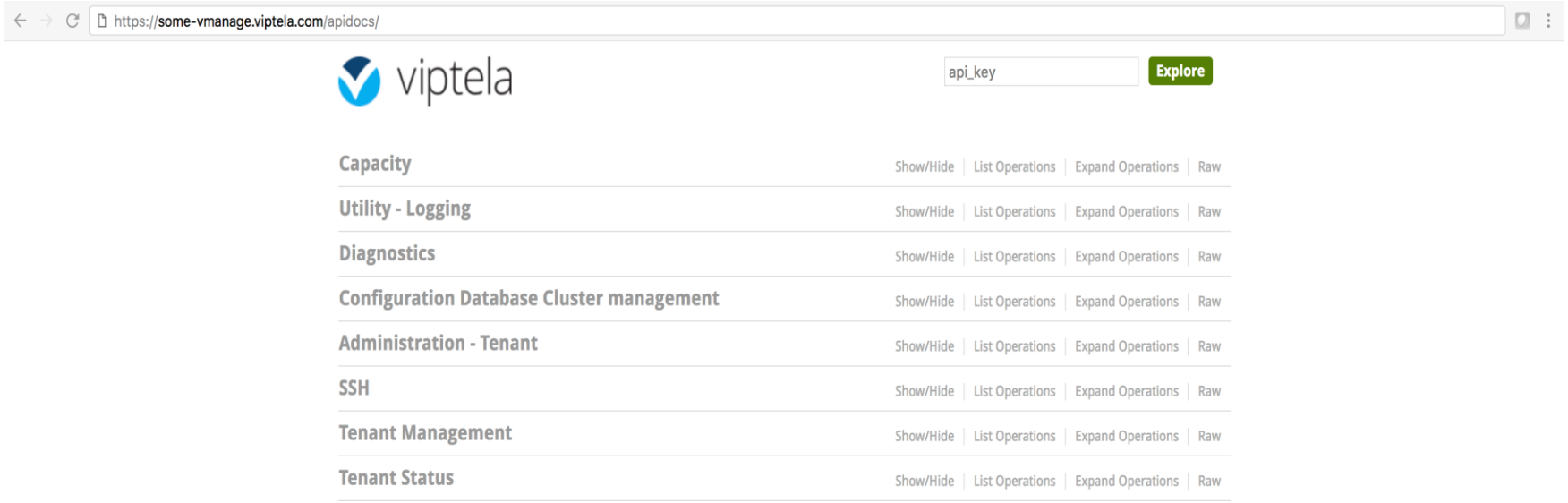
Simulate Flows

Logs

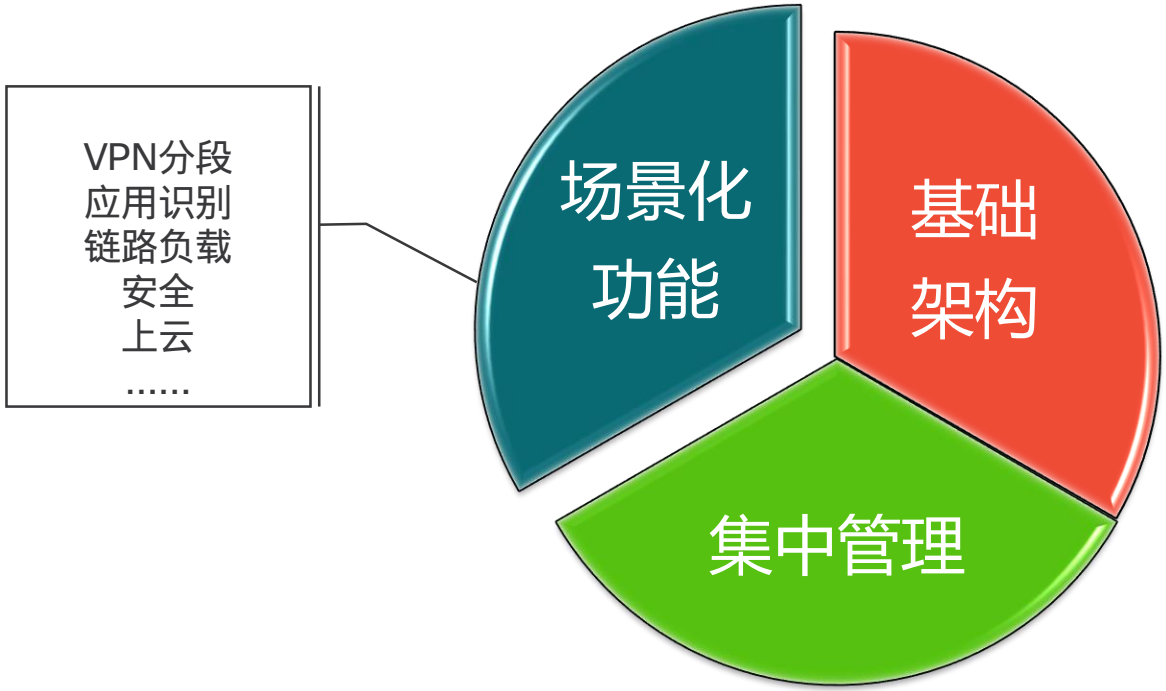
Debug Log

集中管理
vManage API编程接口

/apidocs

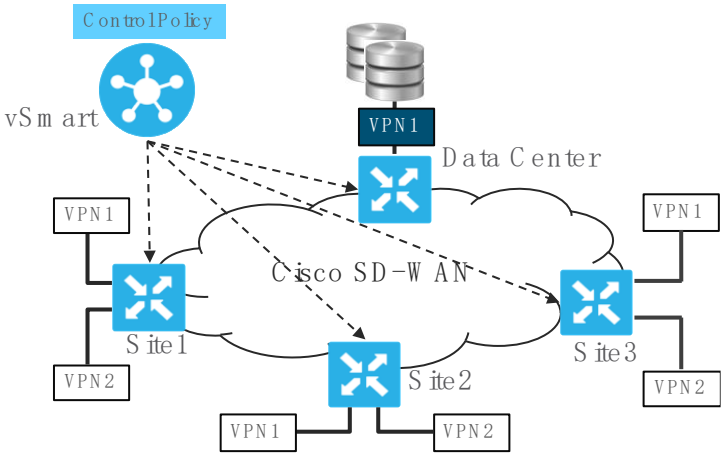


SD-WAN网络构建的要点

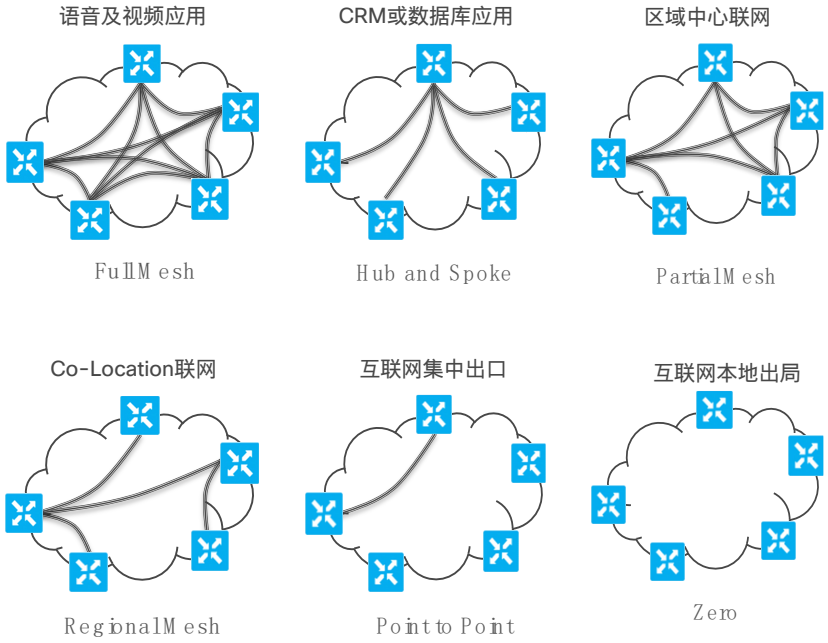


思科SD-WAN应用场景一

多租户与逻辑拓扑：基于应用或租户的逻辑拓扑



- 根据应用或租户定义VPN，不同的VPN可以单独定义逻辑拓扑。
- 如：CRM应用为Hub-Spoke拓扑，Voice应用为Fully Mesh拓扑。

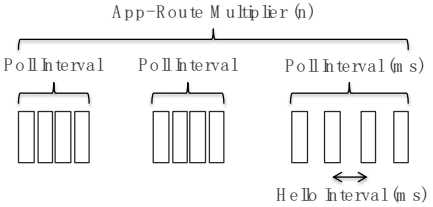


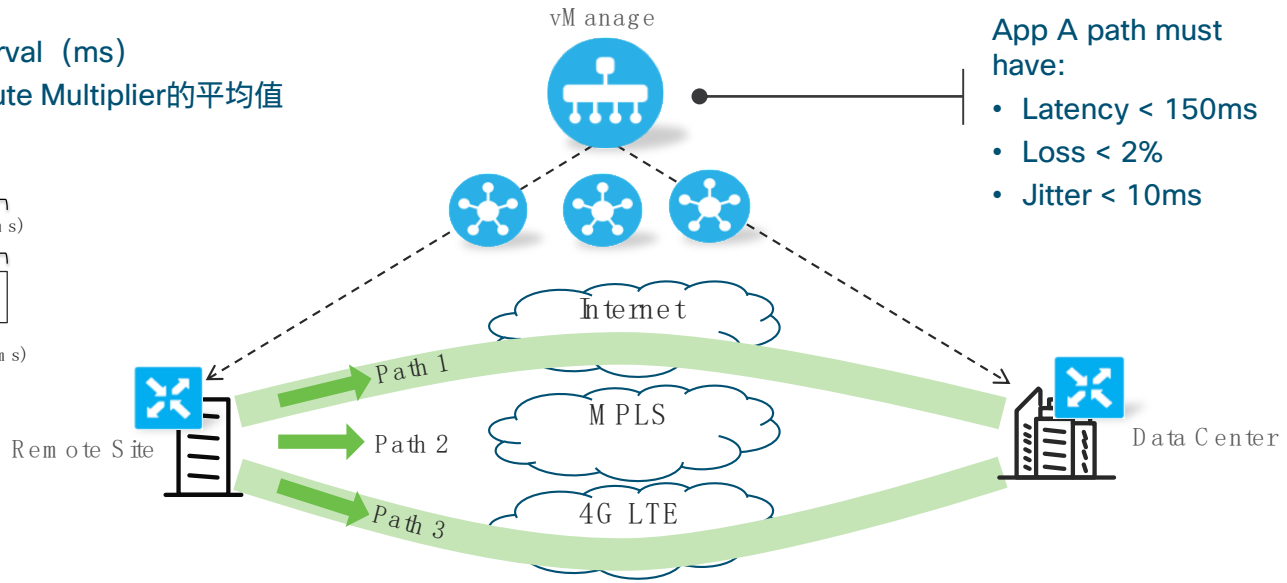
思科SD-WAN应用场景二

应用识别与智能调度：关键应用基于SLA智能选路

vEdge周期性执行线路可用性和质量检测

- 通过BFD进行检测
- 周期性：Hello/Polling Interval（ms）
- 线路质量计算的是App-Route Multiplier的平均值



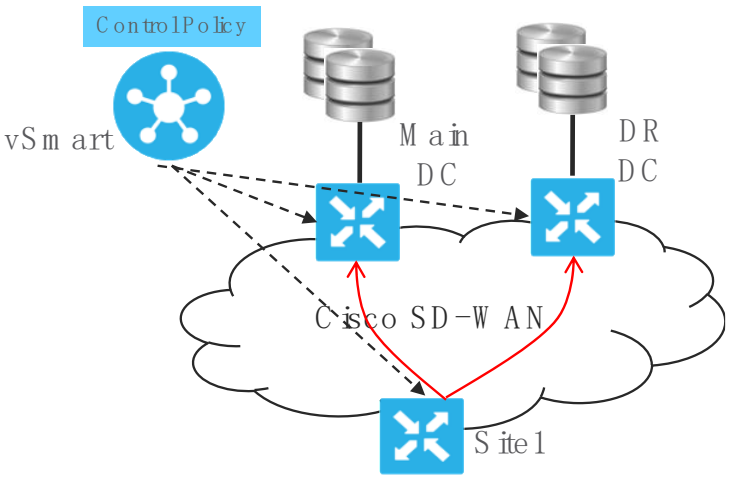


Path1：10ms，0% loss，5ms jitter
Path2：200ms，3% loss，10ms jitter
Path3：140ms，1% loss，10ms jitter

思科SD-WAN应用场景三

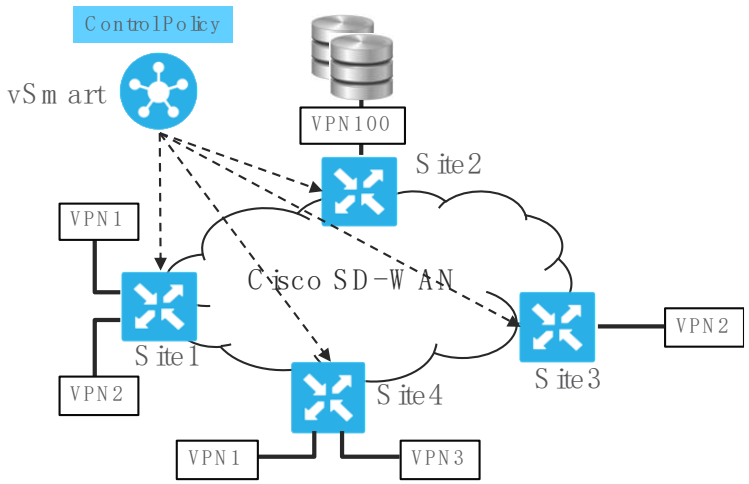
流量工程：多中心选路及公共服务区域

双中心优先选路



- 主备份中心优先级定义和冗余备份。
- 可以为不同的接入站点分别定义不同的主备份中心。

公共服务区域

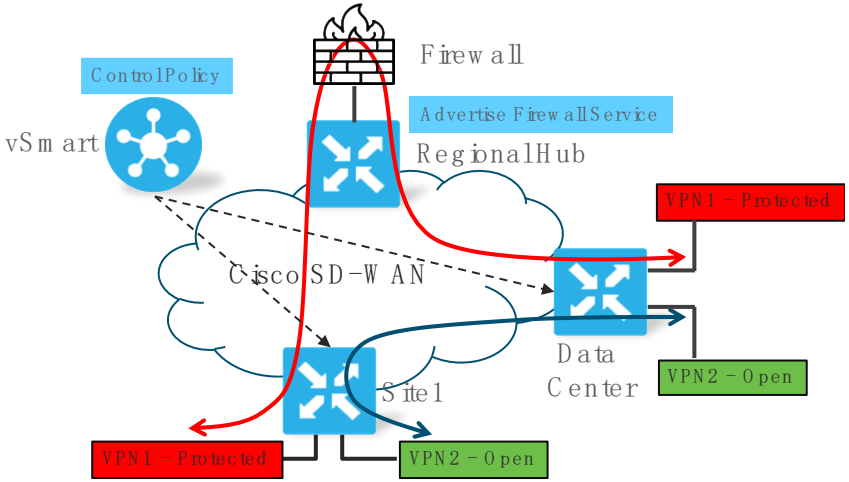


- 网络中多种应用或租户通过VPN隔离。
- 网络中存在公共服务区域（DHCP、DNS等），为多个VPN提供服务。

思科SD-WAN应用场景三

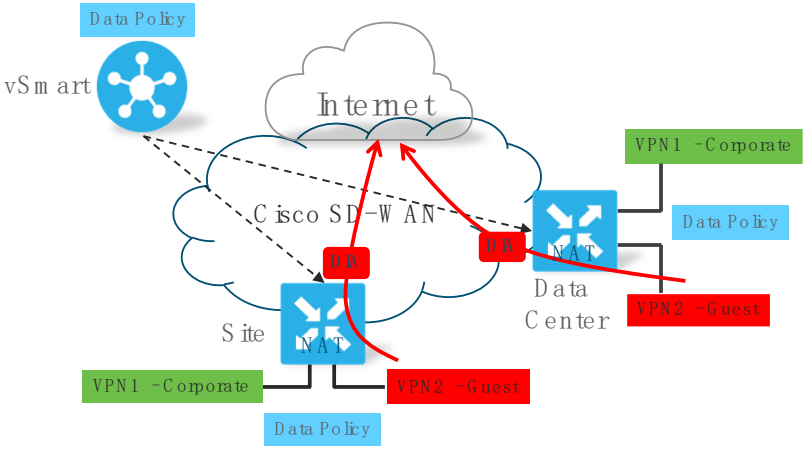
流量工程：基于流量工程的安全调度

区域安全中心流量调度



- Region Hub为区域性安全中心，提供安全性功能。
- 某些应用在进入到数据中心之前，需要先经过区域安全中心的防火墙保护，其他的应用不需要经过防火墙，直接进入到数据中心。

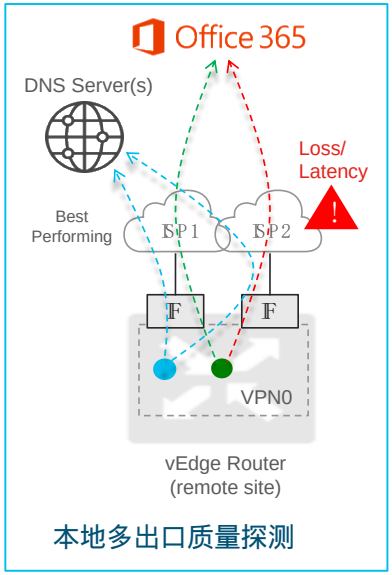
访客访问互联网本地出局



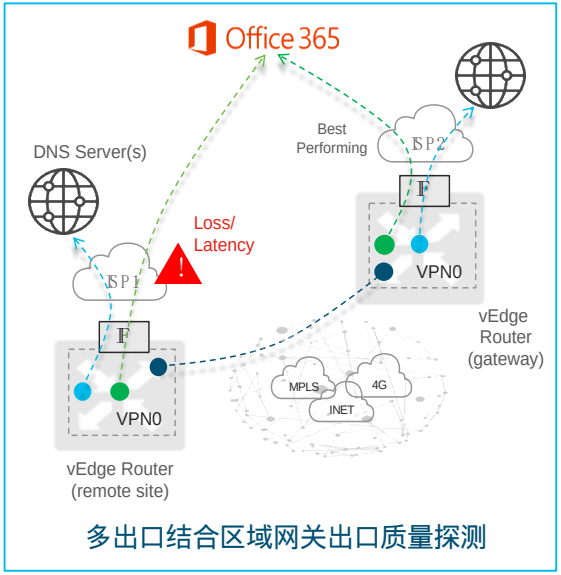
- 访客访问互联网流量从本地互联网出口出局。
- 企业员工访问互联网流量从总部互联网出口出局。
- 专线线路作为互联网线路出口备份。

思科SD-WAN应用场景四

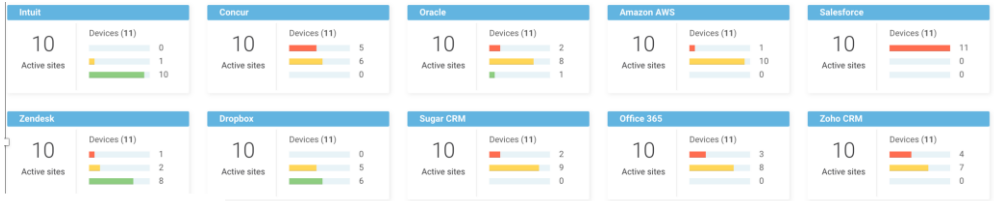
SaaS 优化



本地多出口质量探测



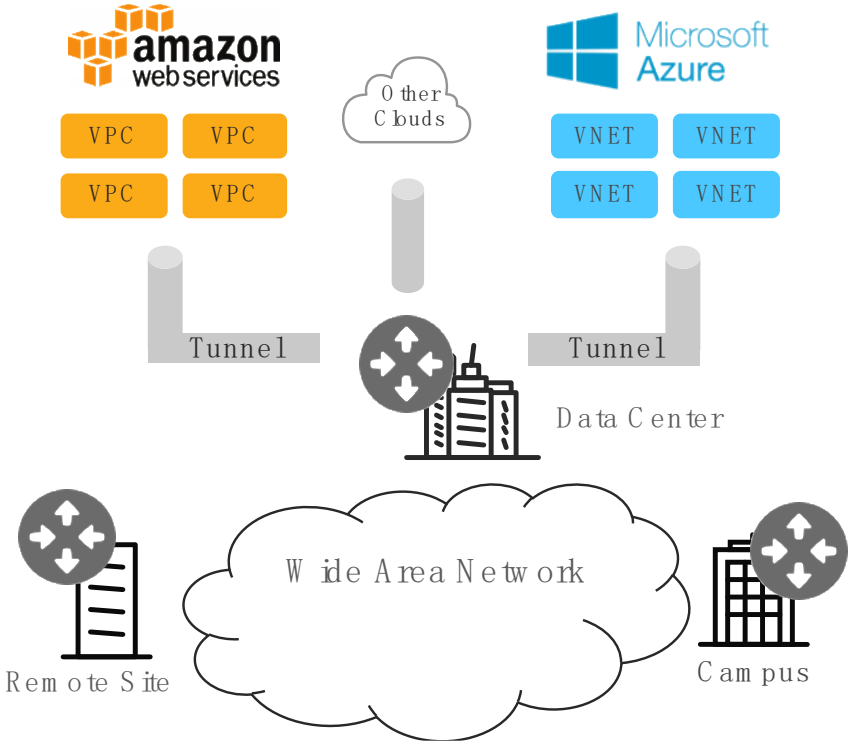
多出口结合区域网关出口质量探测



- DNS解析需要质量探测的云服务域名
- 周期性发探针进行质量探测
- 根据反馈的丢包和时延计算每调线路的vQoE分值
- vEdge根据vQoE自动选择质量最好的线路出口
- vEdge DPI引擎自动识别访问云服务流量
- 根据选择的线路调度流量到相应的出口
- 出口质量探测可以涵盖区域网关综合计算vQoE

思科SD-WAN应用场景五

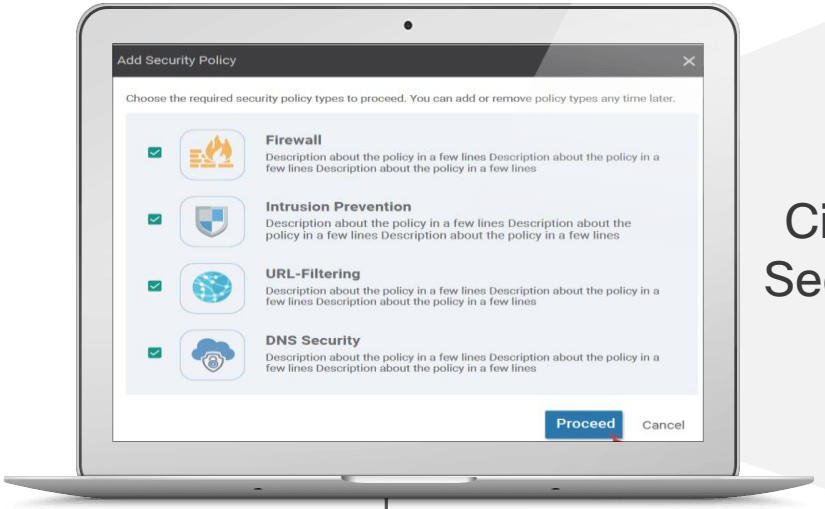
IaaS 多云互联



- 企业逐渐把应用迁移到公有云。
- 存在公有云（多家公有云混用）、私有云混合的情况。
- 企业希望有一个多云交互网络，将各公有云VPC打通。
- 多种线路上云如何整合带宽资源，包括Internet、专线。
- 安全性如何保证
- 能否实现自动化部署

思科SD-WAN应用场景六

互联网访问安全



Cisco SD-WAN

Cisco Security

企业级防火墙
支持超过1400种七层应用

IPS
业界广泛部署的IPS引擎

URL过滤
基于网站信誉度分值，超过82种网站分类和自动更新

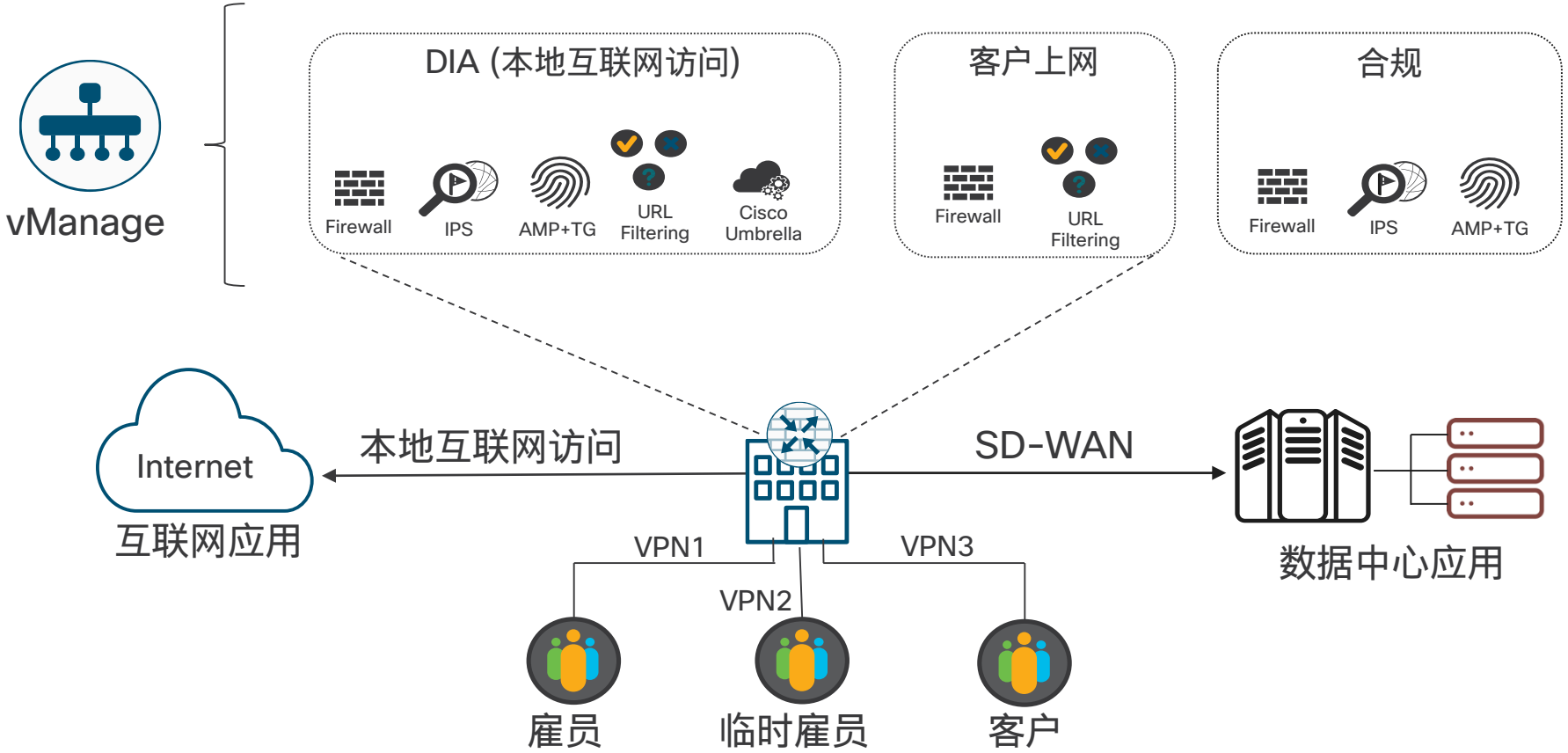
恶意代码防护
文件信誉度和沙箱

简化云安全
Umbrella易于部署

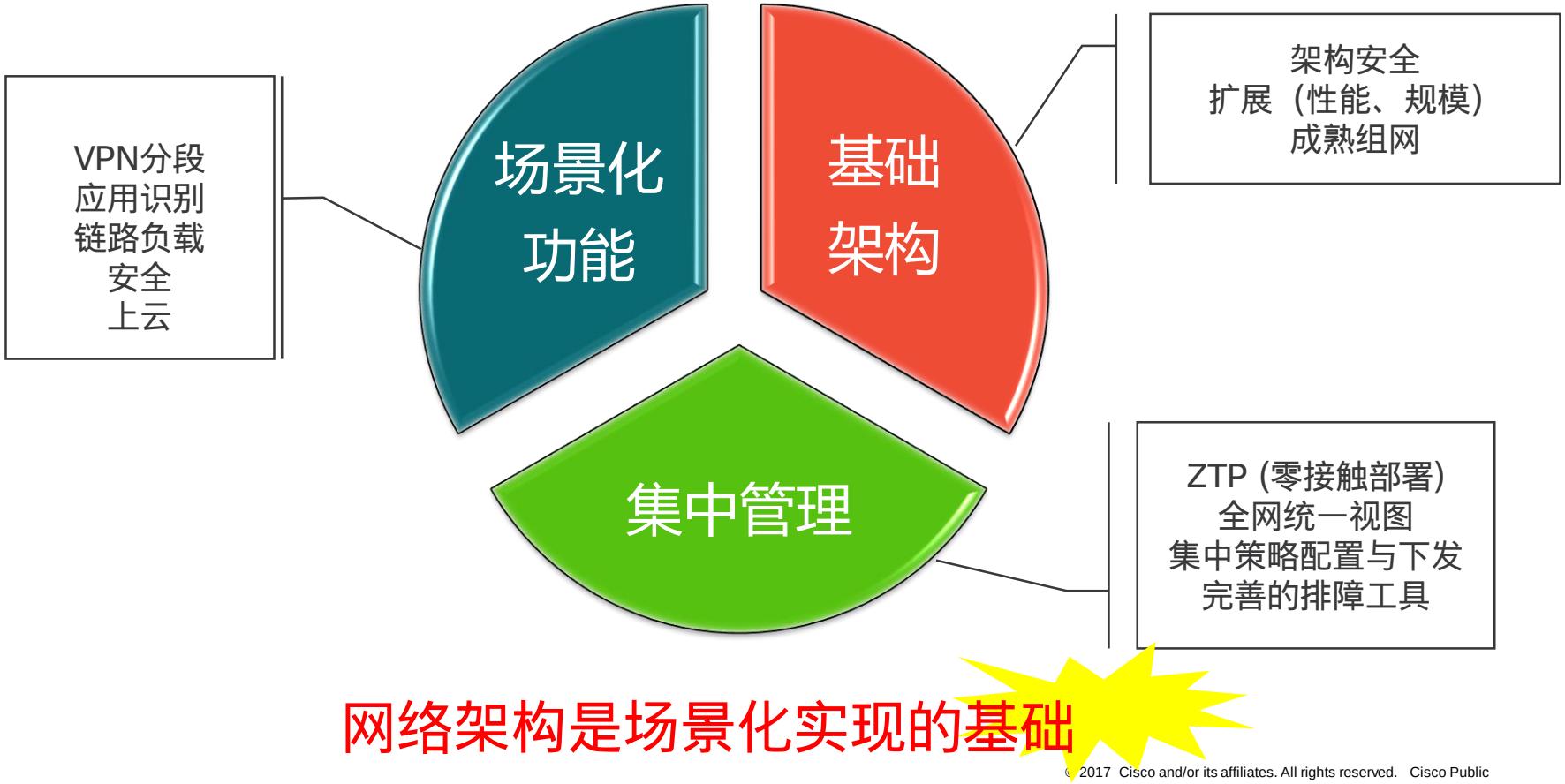
统一安全策略，加快部署时间

思科SD-WAN应用场景六

互联网访问安全



SD-WAN网络构建的要点



零售业案例分享

猩便利

客户面临挑战

- 无人便利店，当前互联网线路资源无法满足关键与时延敏感应用要求
- 后台应用在公有云，公网访问有安全隐患且不易管理；将应用从公有云迁回传统数据中心存在诸多技术困难
- 新店开张的设备与线路部署很耗时，以及线路故障难以迅速排除

思科解决方案

- Viptela SD-WAN 解决方案
- vEdge连接所有分支与公有云，提供路由、安全、加密一体化
- 流量工程与QoS
- 混合线路：Internet + 4G

客户获益

- 更经济与方便的网络连接
- 更可靠的关键业务保障
- 端到端的业务分段保证应用安全
- 远端设备自动上线，集中图形化运维实时监控，及时故障排除

金融业客户案例

客户面临挑战

- 海外专线费用高昂
- 海外机构现场无IT支持人员，出差费用高
- 分支机构部署时效性要求高
- 缺乏自动化、可视化运维工具

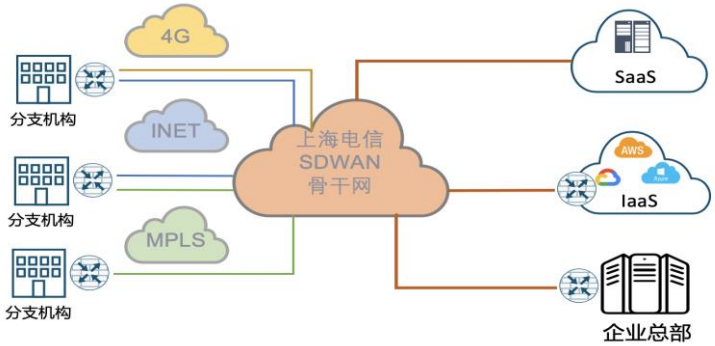
思科解决方案

- 在香港九龙湾和葵涌双数据中心部署4台ASR1K作为双HUB节点，多个海外机构选择ISR4300 作为分支路由
- HUB节点多条Internet线路整合，每台路由器采用HGC、PCCW 2个营运商线路出口

客户获益

- 互联网线路达到专线功能，费用节省显著
- 零配置上线帮助机构网络快速部署，满足业务要求
- 全面监控广域网业务流量，运维清晰
- 有效的利用带宽资源，流量负载均衡

运营商案例分享一



客户面临挑战

传统专线业务开通时间长，成本高

组网拓扑单一并且固定

最终用户无法自主管理和监控链路质量

无法根据应用类型进行灵活调度

很难和云业务进行紧密结合

依靠电信人工维护，维护费用高

思科解决方案

Cisco SDWAN解决方案和上海电信宽带及专线业务捆绑销售

基于多租户架构，最终用户IT人员拥有专属管理平面，自主管理和监控。

利用vEdge Cloud构建虚拟POP节点进一步优化流量

建立POP点和多个公有云互通，提供最终用户入云服务

每用户支持独立的安全策略，提供全栈式安全防护

开发自服务使用门户与电信既有OSS、BSS系统对接

客户获益

快速开通专线业务，从1个月提速到1周内

先进的转发和控制解耦架构，消除Hub故障点

有能力提供各种云增值服务

SDWAN结合最终用户IT应用，增加用户粘性

实现全网自动化运维

高扩展性，一期平台5000节点+支持能力


CISCO