IWAN：支持下一代分支机构

技术概述

Steve Wood，技术营销架构师
Scott Van de Houten，知名架构师

企业广域网 - 当前形势

- 广域网带宽需求日益增长！

  云、自带设备/万物互联和视频使广域网带宽需求加剧

- IT 预算持平或下降

  传输/带宽成本占广域网预算的一大部分

- 这些因素在不断推动实现广域网现代化

  低成本传输 - 互联网、LTE、运营商级以太网、 云应用性能监控和优化

  安全性 - 强加密和威胁防范

思科智能广域网可以解决这一市场需求！

云

50% 的首席信息官希望，到 2015 年能够利用云实现日常运营

移动

6 倍 到 2015 年，移动数据流量将增加

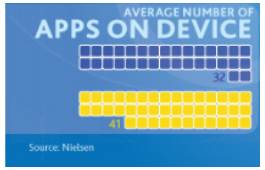
胖应用

2/3 的移动流量将为视频

移动设备网络流量

每个设备的平均应用数*

41



平均应用大小**

23MB iOS

6MB Android

25MB Windows

操作系统更新文件大小***

1.1GB 用于 iPhone6 的 iOS 8

388MB KitKat 4.4

400MB Windows 7

来源：

* http://www.nielsen.com/us/en/newswire/2012/state-of-the-appnation-%C3%A2%C2%80%C2%93-a-year-of-change-and-growth-in-u-s-smartphones.html

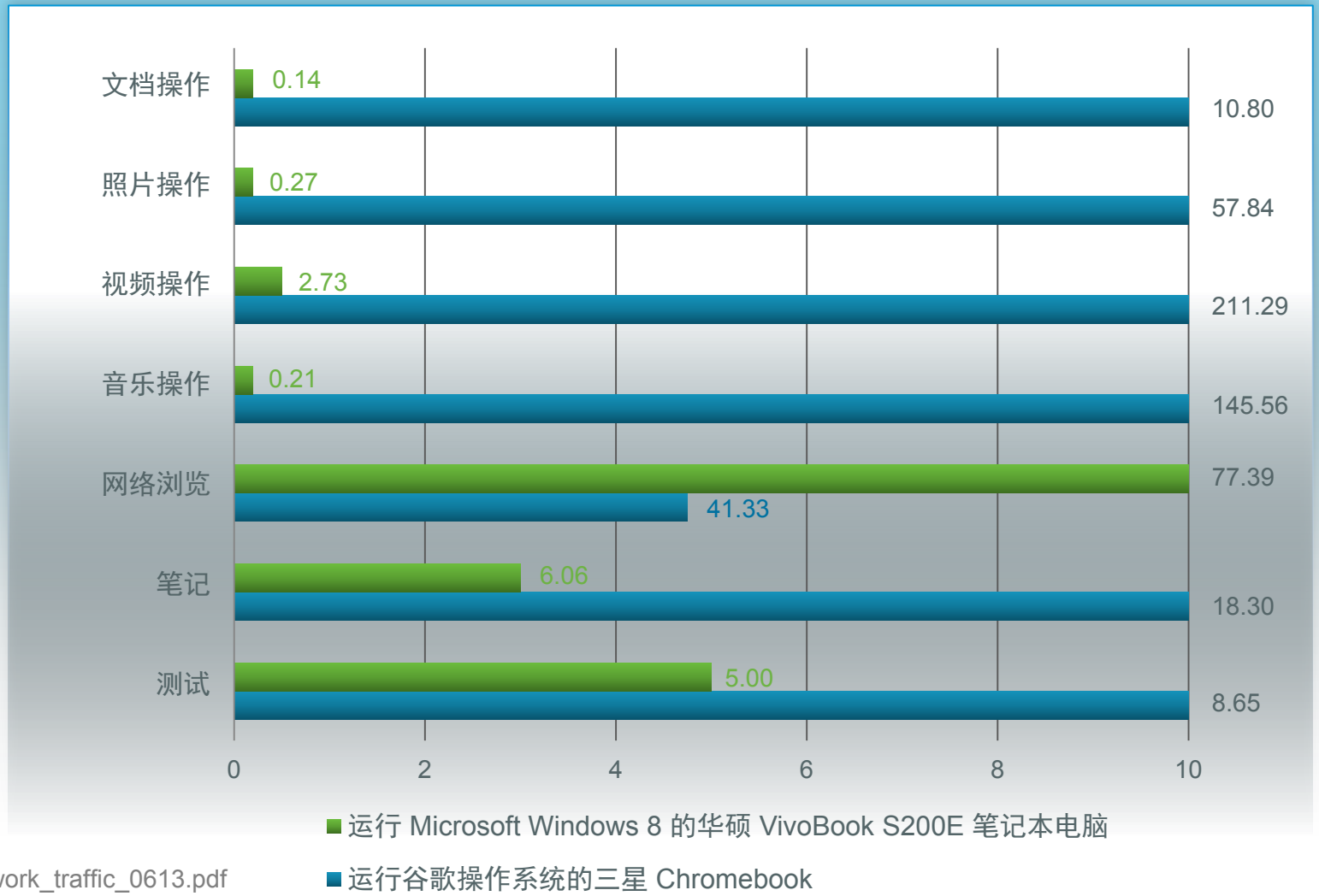
** https://www.abiresearch.com/press/average-size-of-mobile-games-for-ios-increased-by-

*** http://www.wirelessandmobilenews.com/2013/05/samsung-galaxy-s3-iii-update-android-4.2.1-jelly-bean.html
http://theiphonewiki.com/wiki/Firmware#iPad_4
http://answers.microsoft.com/en-us/windows/forum/windows_other-windows_update/what-is-average-monthly-size-of-update-downloads/dfe9bb34-c2dd-478e-a6cb-0a26228cf552

Chromebook 平均创建 152 倍的流量

第三方实验室测试：
Chromebook 与
Windows 8 笔记本电脑

- Chromebook 创建的网络流量高达 692.2 倍
- Chromebook 平均创建 152 倍的网络流量



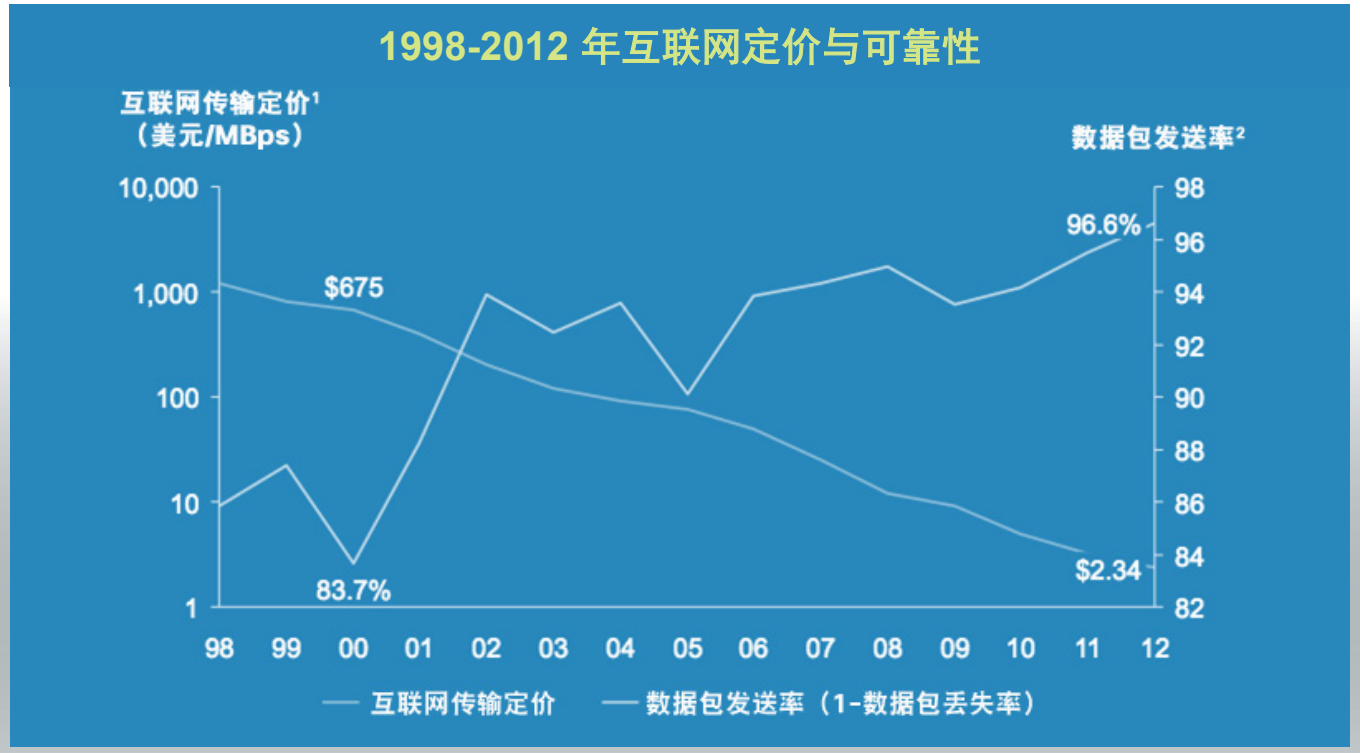
http://principledtechnologies.com/Microsoft/Chromebook_PC_network_traffic_0613.pdf

为什么转向广域网型互联网？

低成本替代方案

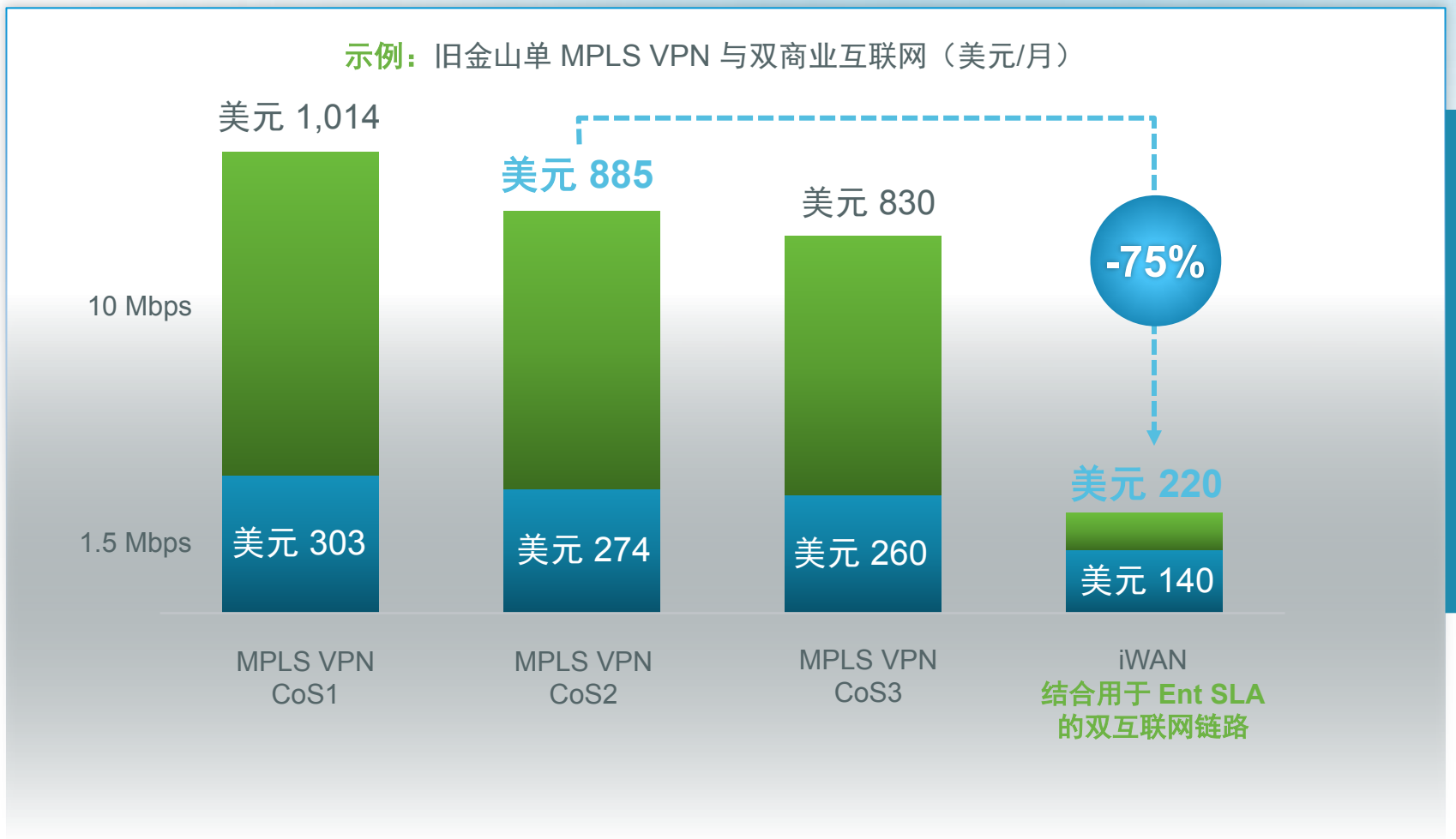
46%

的组织正在计划向互联网连接过渡



[1]互联网传输定价基于主要从互联网运营论坛（市场定价预测）收集的调查和非正式数据
[2]数据包发送基于位于加利福尼亚的 EDU.STANFORD.SLAC 的全球 PingER（全球服务器样本）长达 15 年的 ping 数据
资料来源：William Norton (DrPeering.net)；Stanford ping end-to-end reporting (PingER)（斯坦福发起的端到端性能监控项目 (PingER)）

并且互联网转型回报快



节省 665 美元/月 x
12 个月 x 1,000 个站点
= 每年
节约 800 万美元

资料来源：截止到 2013 年 3 月 Telegeography 对旧金山 MPLS VPN 的定价；Comcast 网站；Verizon 网站

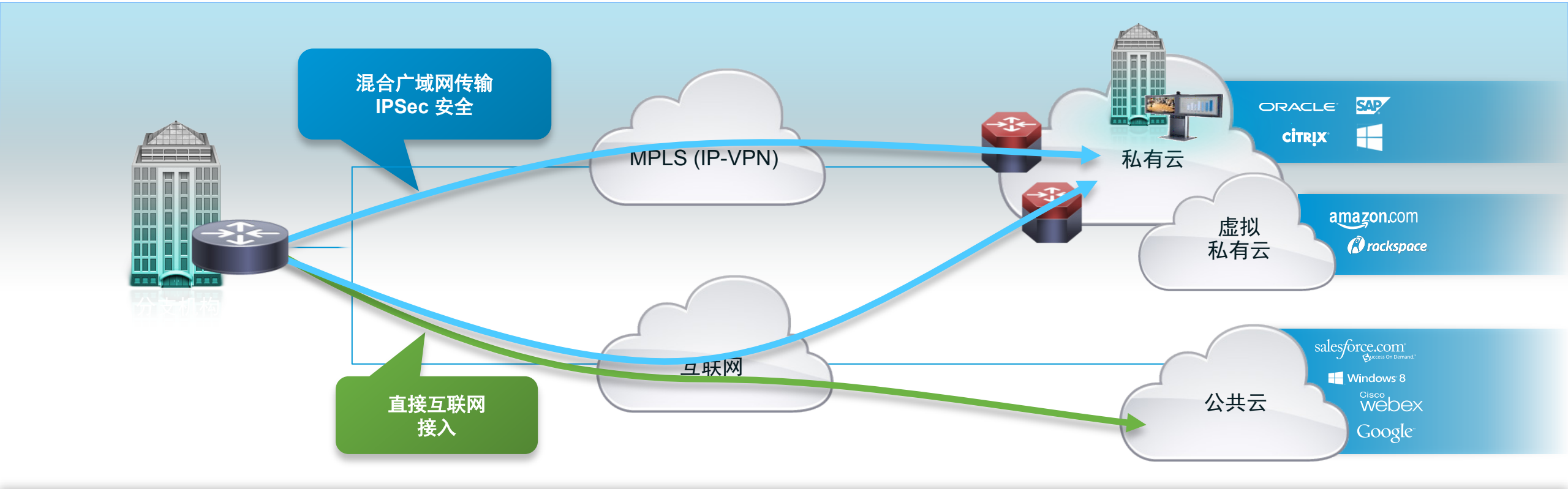
智能广域网：利用互联网

新增功能

- 高度可靠的广域网型互联网
- 用于业务关键型应用的 SLA
- 用于互联网接入的集中安全策略
- 显著降低广域网成本，并且不影响性能

智能广域网：利用互联网

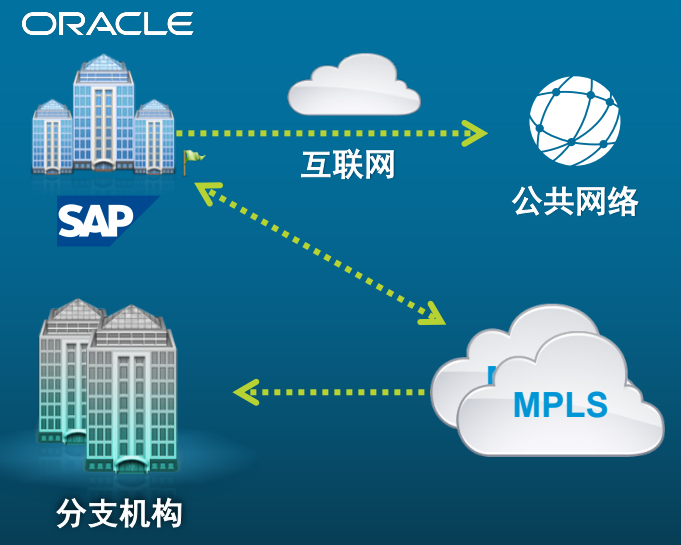
安全的广域网传输和互联网接入



- 用于私有和虚拟私有云接入的安全广域网传输
- 利用本地互联网路径接入公共云和互联网
- 广域网传输能力增加；成本效益提高！
- 提高应用性能（正确流向，各司其职）

智能广域网部署模式

双 MPLS

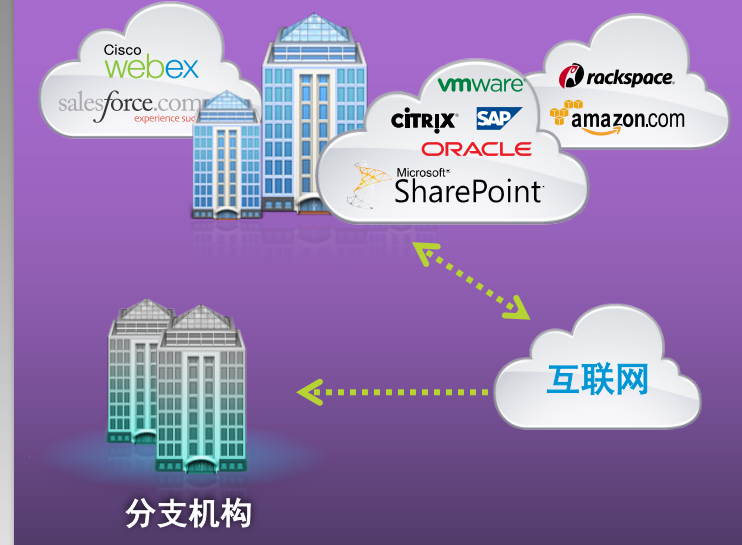


- ✓ 最高 SLA 保证
- – 与 SP 紧密耦合
- ẋ 价格昂贵

混合

- ✓ 关键应用的带宽更宽
- ✓ 平衡的 SLA 保证
- – 价格适中

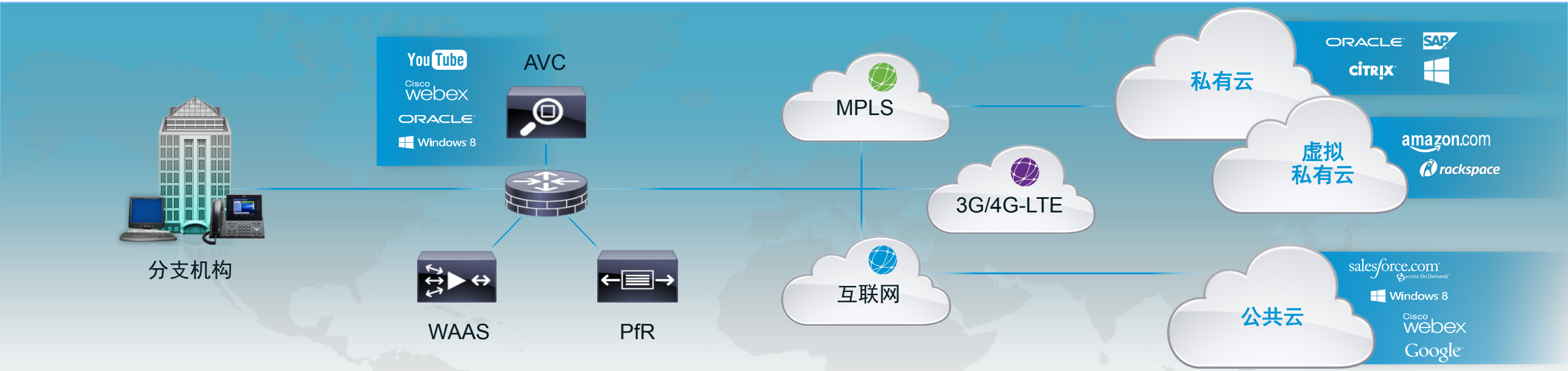
双互联网



- ✓ 最优惠的价格/最佳的性能
- ✓ SP 灵活性最大
- – 企业负责 SLA

一致的 VPN 覆盖确保过渡安全

智能广域网解决方案组成部分



控制与管理自动化

与传输方式无关

- 一致的运行模式
- 简化提供商迁移
- 可扩展的模块化设计
- Ipsec 路由覆盖设计

智能路径控制

- 基于策略的动态应用最佳路径
- 实施负载平衡以充分利用带宽
- 提高的可用性

应用优化

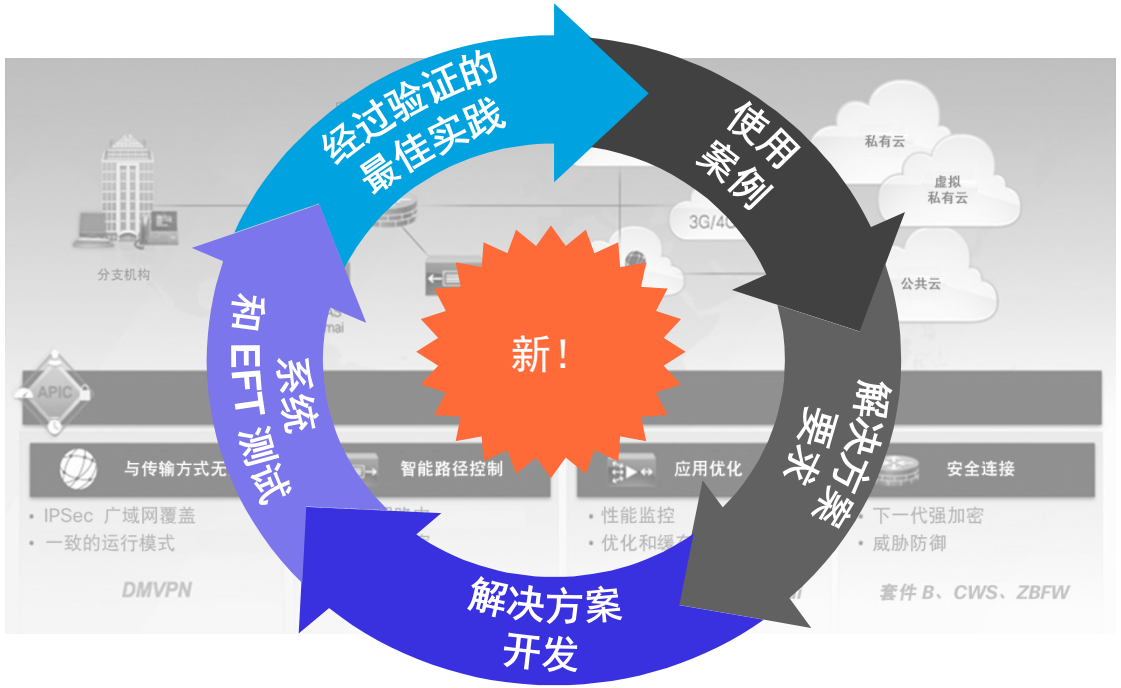
- 通过性能监控实现应用可视性
- 应用加速和带宽优化

安全连接

- 经过认证的强大加密
- 全面的威胁防护
- 用于保护直接互联网接入的云托管安全

IWAN：一种架构和系统方法

- IWAN 是一种解决方案架构
  - 解决网络问题
  - 依据使用情况驱动
  - 系统开发方法
- 符合规定、经过测试、可互通。
  - 有限的范围和复杂性
  - 确保自动化和质量
- 实现业务成果
  - 降低广域网成本。增加带宽
  - 提高和保护应用性能
  - 直接互联网接入
  - 访客接入卸载
  - 减少运营支出



IWAN 愿景和战略

智能虚拟化 → 自动化 → 云集成 → 服务虚拟化 → 自学习网络

预测性、
自我导向性

虚拟路由器、虚拟服务与应用协调

ACI 策略、云间移动、优化、AMP

安全、简单、集中的策略自动化

安全的 VPN 覆盖、传输方式不限、带宽效率、应用 SLA

IWAN 愿景和战略
IWAN 框架的系统开发演进

智能虚拟化 → 自动化 → 云集成 → 服务虚拟化 → 自学习网络





IWAN 框架

- 与传输方式无关的设计
- 智能路径控制
- 应用优化
- 安全连接
- 管理和协调

提供新使用案例的同时逐步进行改进

与传输方式无关的设计

简化基于互联网的广域网

灵活安全的广域网设计，可使用任何传输方式

动态多点 VPN (DMVPN)

与传输方式无关

简化广域网设计

- 通过任何运营商服务服务轻松实现多宿主
- 单一路由控制平面，最小化提供商 Peer 对接

灵活

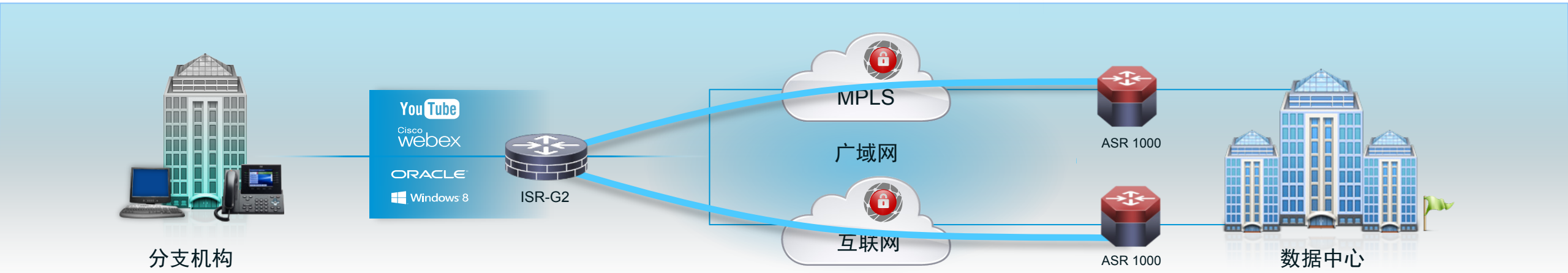
动态全网状连接

- 一致的设计覆盖所有传输方式
- 自动站点间 IPsec 隧道建立
- 用于新分支的零接触控制中心配置

安全

久经验证的强大安全性

- 经过认证的加密和防火墙以确保合规性
- 可扩展设计，硬件具有高性能加密



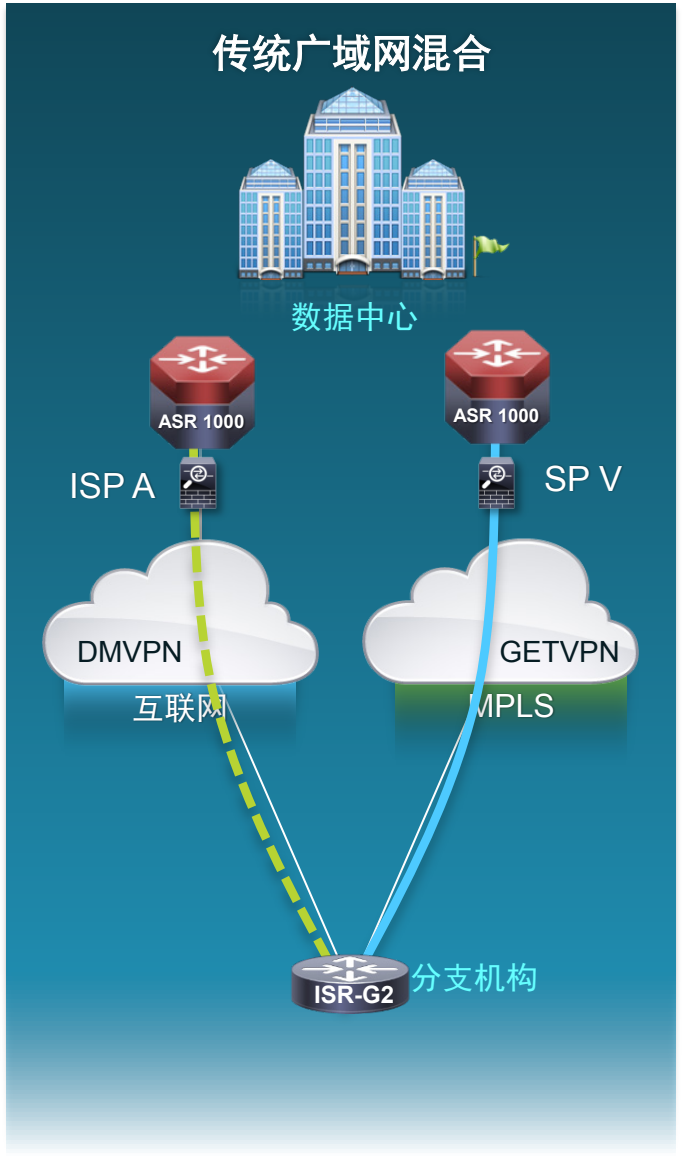
混合广域网设计

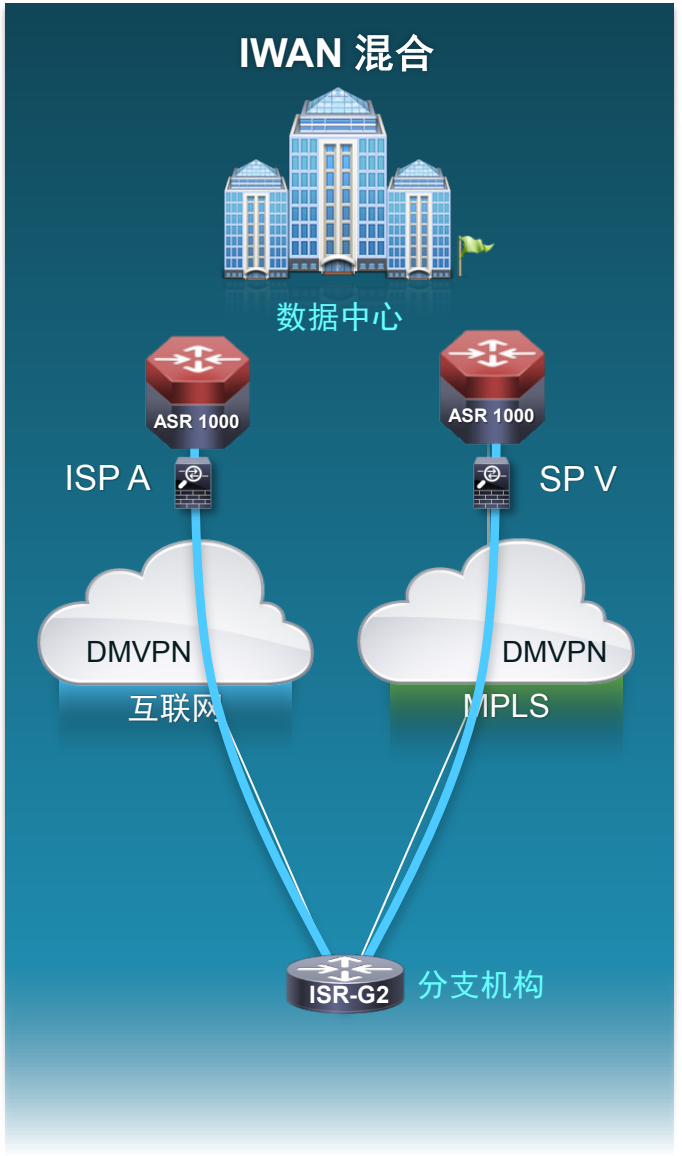
传统广域网与智能广域网

主用/备用
广域网路径
主要与备份

两种 IPsec 技术
GETVPN/MPLS
DMVPN/互联网

两个广域网路由域
MPLS：eBGP 或静态
互联网：iBGP、EIGRP 或 OSPF
路由重分布
路由过滤环路防止



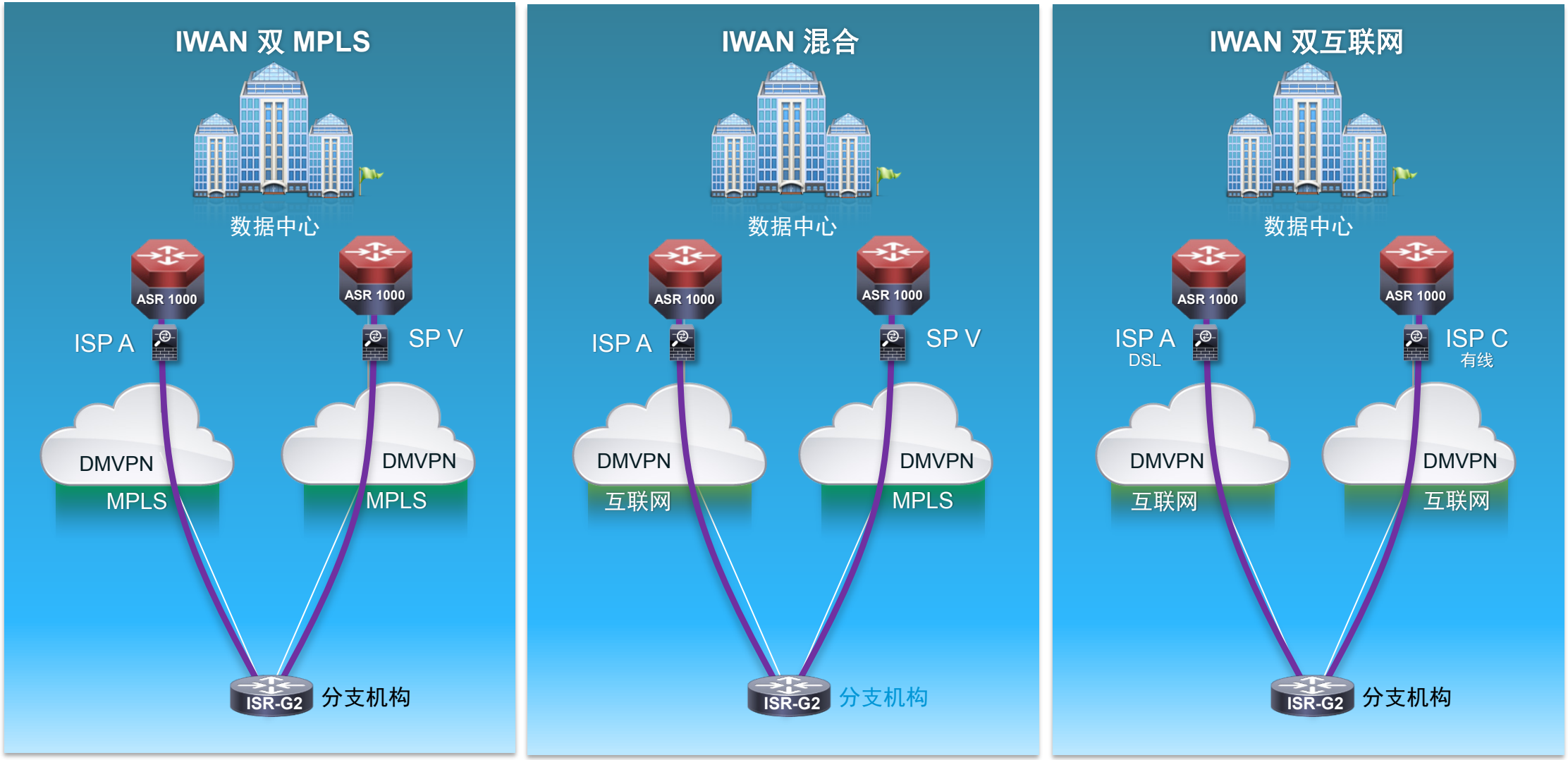


主用/主用
广域网路径

一个 IPsec 覆盖
DMVPN

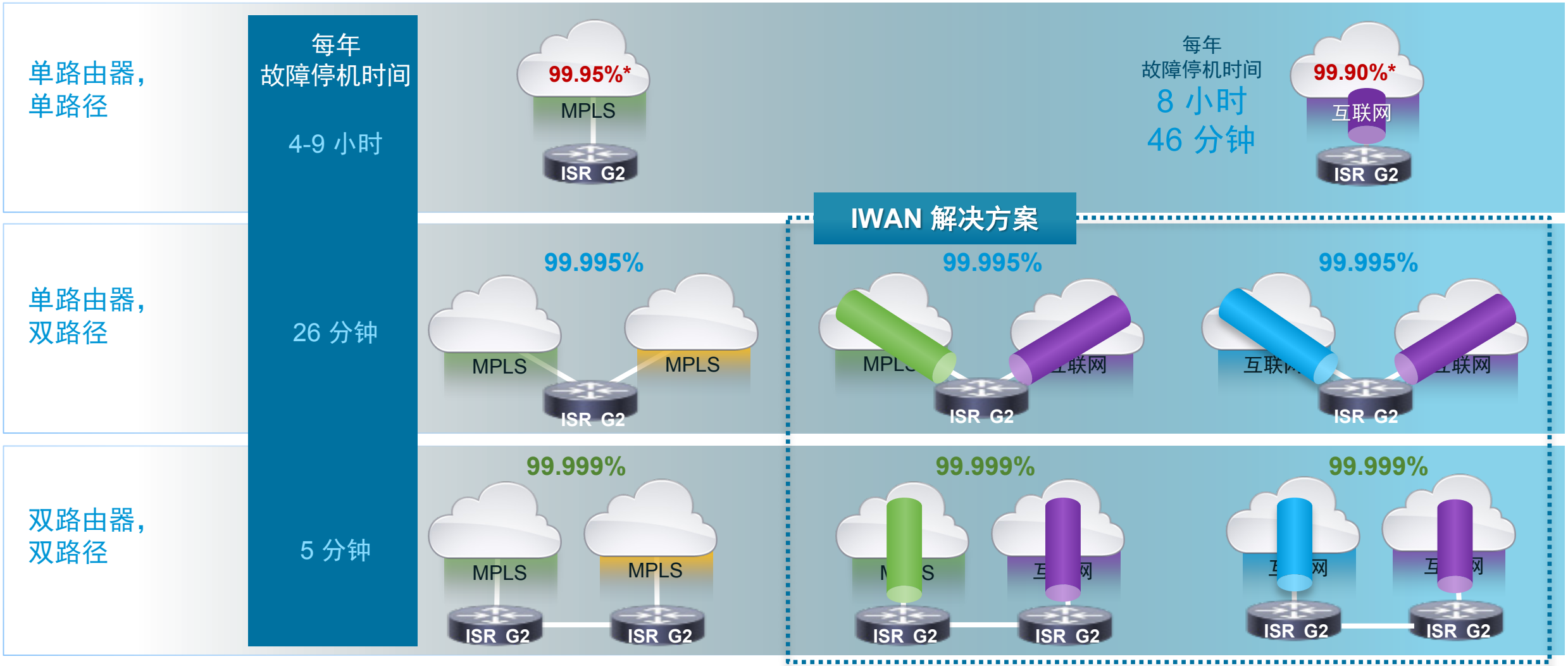
一个广域网
路由域
iBGP、EIGRP 或 OSPF

与 IWAN 传输方式无关
一致的部署模式简化操作



通过思科智能广域网构建高可用性广域网

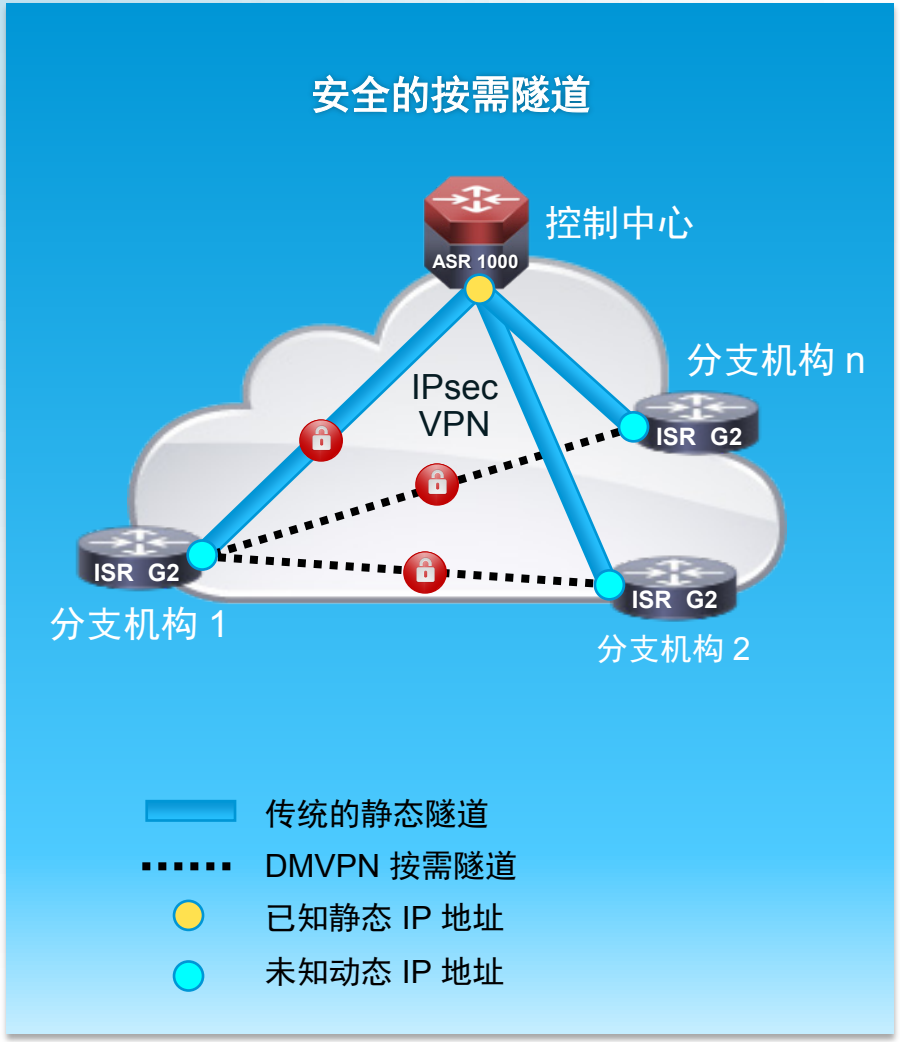
冗余和路径多样性问题



* 每年典型的 MPLS 和企业级宽带可用性 SLA 及故障停机时间，用思科高级服务部 DAAP 工具计算。

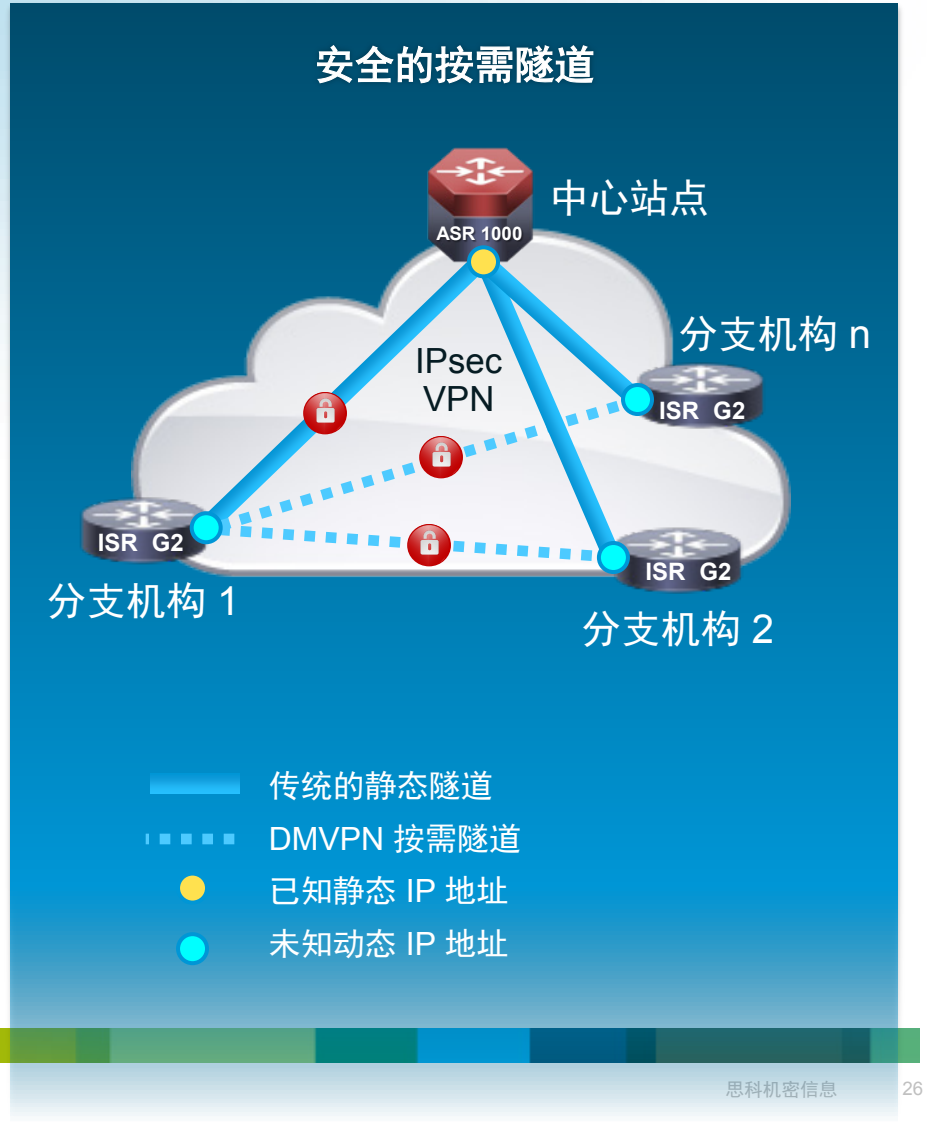
智能广域网传输独立的设计
配有动态多点 VPN (DMVPN)

- 久经验证的 IPsec VPN 技术
  - 大规模广泛部署
  - 基于标准的 IPsec 和路由
  - 高级 QOS：分层、每个隧道、自适应
- 灵活性与恢复能力
  - 覆盖任何传输方式：MPLS、运营商级以太网、互联网、3G/4G..
  - 控制中心与分支拓扑和动态网状拓扑
  - 多重加密、密钥管理、路由选项
  - 多个冗余选项：平台、控制中心、传输方式
- 安全
  - 行业认证的 IPsec 和防火墙
  - NG 强加密：AES-GCN-256（套件 B）
  - IKE 版本 2
  - IEEE 802.1AR 安全的唯一标识符
- 简化的 IWAN 部署
  - 经过验证的规范性 IWAN 设计
  - 自动调配 - Prime、APIC、Glue



OTT 广域网设计
配有动态多点 VPN (DMVPN)

- **分支机构的分支站点建立一个通往中心站点的隧道，并通过该隧道注册到中心站点**
- IP 路由为每个站点交换前缀信息
- BGP 或 EIGRP 通常用于扩展
- **将 WAN 接口 IP 地址用作隧道地址后，提供商网络不需要路由客户内部的 IP 前缀**
- 数据流量流过 DMVPN 隧道
- 当流量位于分支站点时，中心站点帮助分支建立一个站点间隧道
- **应用每个隧道的 QOS 以防中心站点超订用分支站点**



什么是动态多点 VPN?

DMVPN 是一种思科 IOS 软件解决方案，用于通过简单、动态、可扩展的方式建立 IPsec + GRE VPN

依赖于久经验证的两种技术

- 下一跳解析协议 (NHRP)
  - 创建到实际（公共接口）地址的分布式 VPN（隧道接口）映射数据库
- 多点 GRE 隧道接口
  - 单个 GRE 接口支持多个 GRE/IPsec 隧道和端点
  - 简化配置规模和复杂性
  - 支持动态隧道创建

主要功能

- 减少配置和无接触部署支持：
  - 访客协议（IP(v4/v6) 单播、组播和动态路由协议）
  - 传输协议 (NBMA)（IPv4 和 IPv6）
  - 与动态分配的传输地址远程对等连接
  - 动态 NAT 后面的分支路由器；静态 NAT 后面的中心路由器
  - 用于部分/全网状扩展的动态分支到分支隧道
  - 适用于 MPLS；VRF 和 MPLS 中通过隧道交换的 GRE 隧道和/或数据包
  - 各种网络设计和选择

DMVPN 演进

IWAN 1.0

IWAN 2.0

第 1 阶段

- **中心与分支功能**
- 分支上的 p-pGRE 接口，中心上的 mGRE
- 中心上的配置更精简且更少
- 支持动态寻址的 CPE (NAT)
- 支持路由协议和组播
- 分支不需要完整的路由表；可在中心上汇总

第 2 阶段

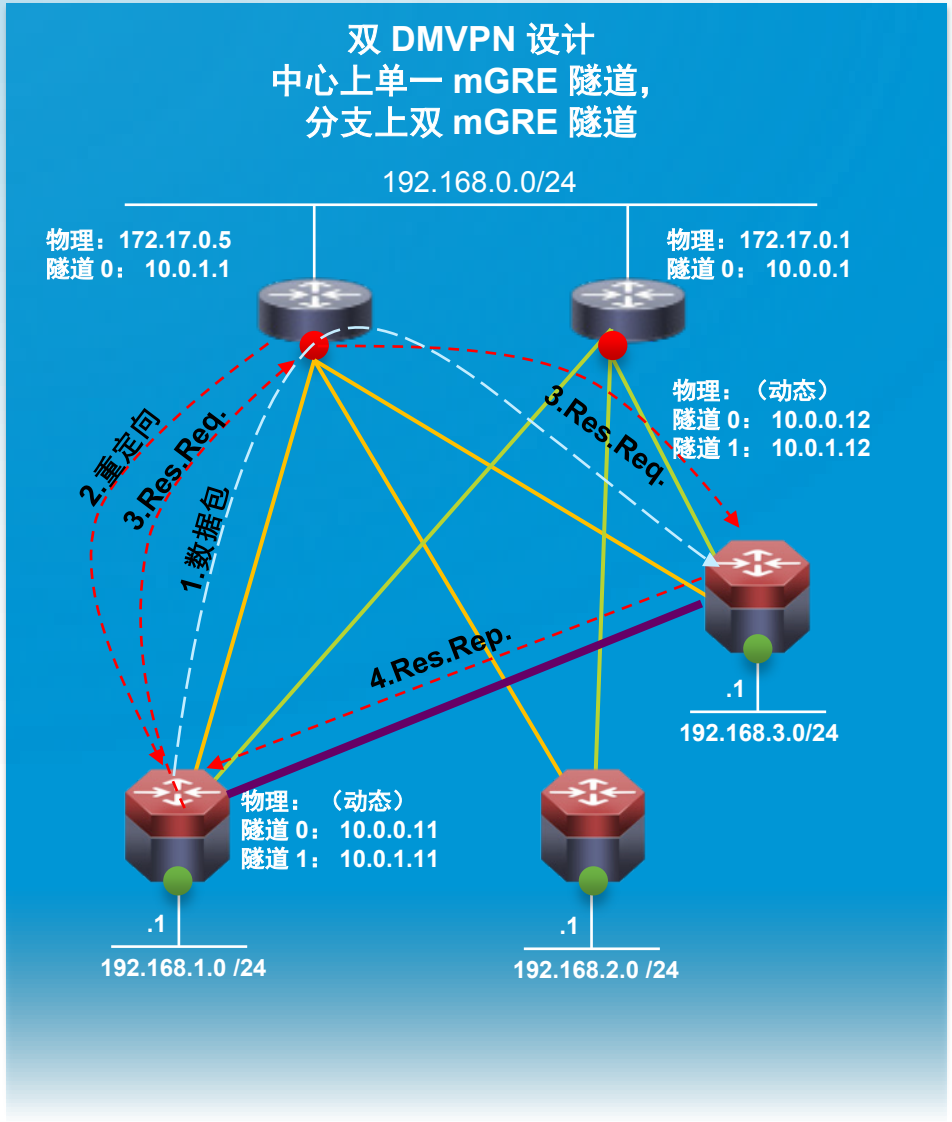
- **分支到分支功能**
- 分支上的 mGRE 接口
- 直接分支到分支的数据流量可减少中心上的负载
- 菊花链设计
- 分支必须有完整的路由表 - 没有汇总
- 分支到分支的隧道由分支本身触发
- 路由协议规模限制

第 3 阶段

- **规模更大且网络设计选项更多**
- 分层设计
- 分支不需要完整的路由表；可以汇总
- 分支到分支的隧道由中心触发
- 无路由协议限制

DMVPN 运作原理

- 分支建立一个到中心的动态永久 GRE/IPsec 隧道，但该隧道不通往其他分支。它们注册为 NHRP 服务器（中心）的客户端，并注册它们的 NBMA 地址
- 双活冗余模式 - 每个分支到两个或多个中心
- 所有配置的中心都有效，且是分支的路由邻居
- 路由协议路由用于决定流量转发
- 分支先通过中心将一个数据包发送到另一个分支后面的目标（专用）子网，然后中心向其发送一个 NHRP 重定向。
- 该重定向触发分支发送一个 NHRP 查询，以查询目标分支后面的数据包目标地址
- 目标分支发起一个到源分支（源分支现在知道其 NBMA 地址）的动态 GRE/IPsec 隧道，并发送 NHRP 回复。
- 在 mGRE 接口上构建动态分支到分支隧道
- 当流量停止时，删除分支到分支隧道



添加强加密：分支机构到总部套件 B 支持

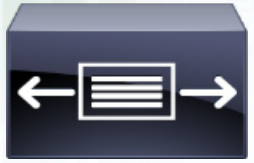
威胁格局正在发生变化

- 必须保护通信和 IT 基础设施免受网络攻击和利用
- 攻击者有耐性且资金充足
- 计算的发展不断推动采用更高的加密强度

ISR 和 ASR1K 平台

- 面向未来：满足未来 20 年的安全性和可扩展性要求
- 效率和规模：硬件加密加速

	旧加密 灾害	思科 套件 B	商品 路由器
AES， 3DES	1GB 加密限制		
HMAC- MD5	理论上的劣势		
DH， RSA	重大风险		
RSA	重大风险		
MD5， SHA1	碰撞攻击		
熵	重大风险		
TLS1.0， IKEv1	已知缺陷，缺少认证加密	IKEv2	



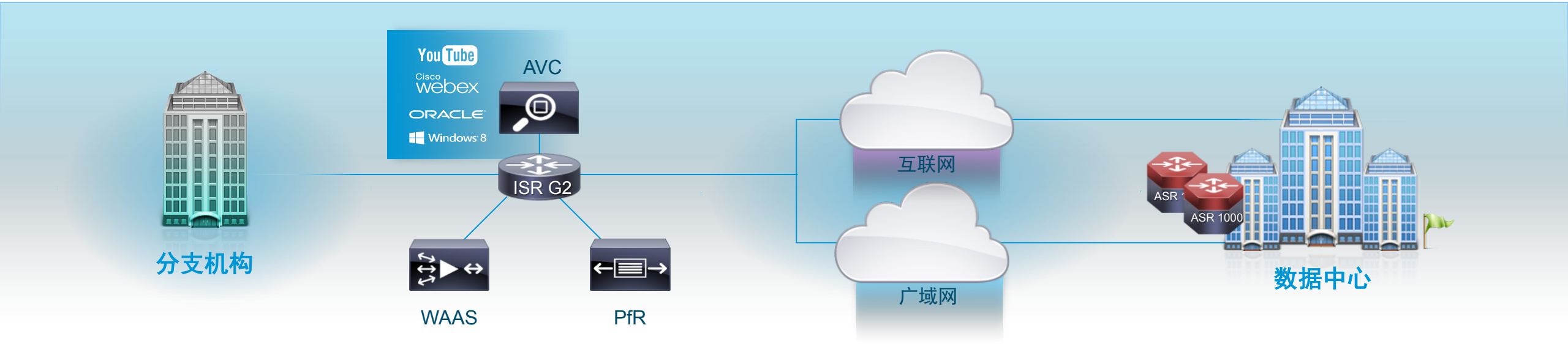
智能路径控制

提高应用交付和广域网效率

充分利用您的广域网投资

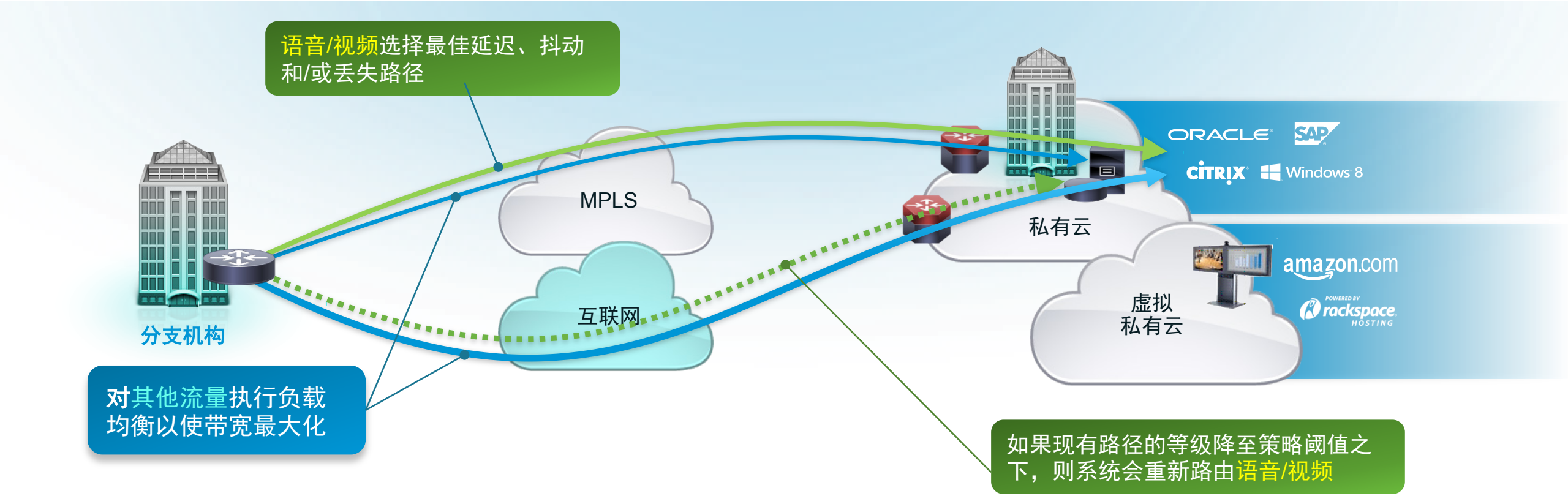
智能路径控制的优势

降低 广域网成本	充分利用 所有广域网带宽	提高 应用性能	降低 广域网成本
启用基于互联网的广域网	基于负载、电路成本和路径偏好高效分布流量	每个应用的最佳路径，基于延迟、丢失、抖动测量结果	保护运营商免受黑洞和限电影响



用 PfR 进行智能路径控制

语音和视频使用案例



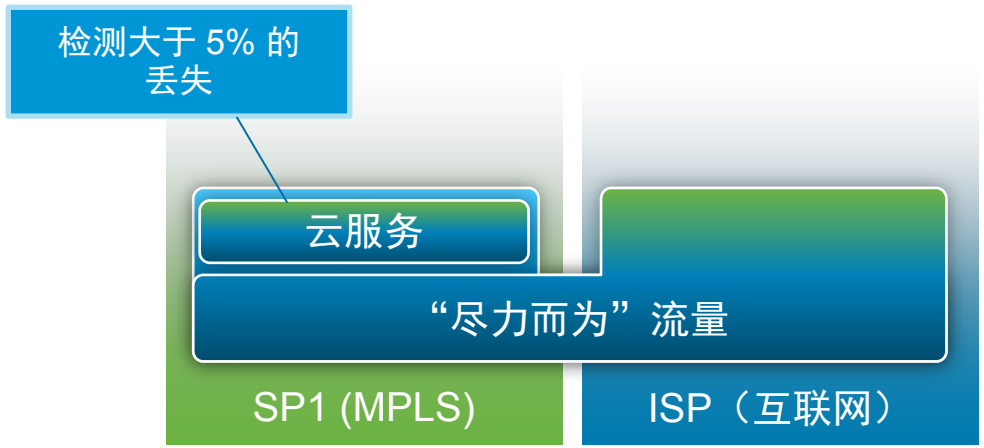
- PfR 根据应用性能策略监控网络性能和路由应用
- PfR 根据链路利用水平均衡流量负载以有效利用所有可用广域网带宽

PfR 增强传统路由

PfR 的作用

保护关键应用，同时提高带宽使用率

混合 IWAN



双互联网广域网

云服务和负载均衡策略

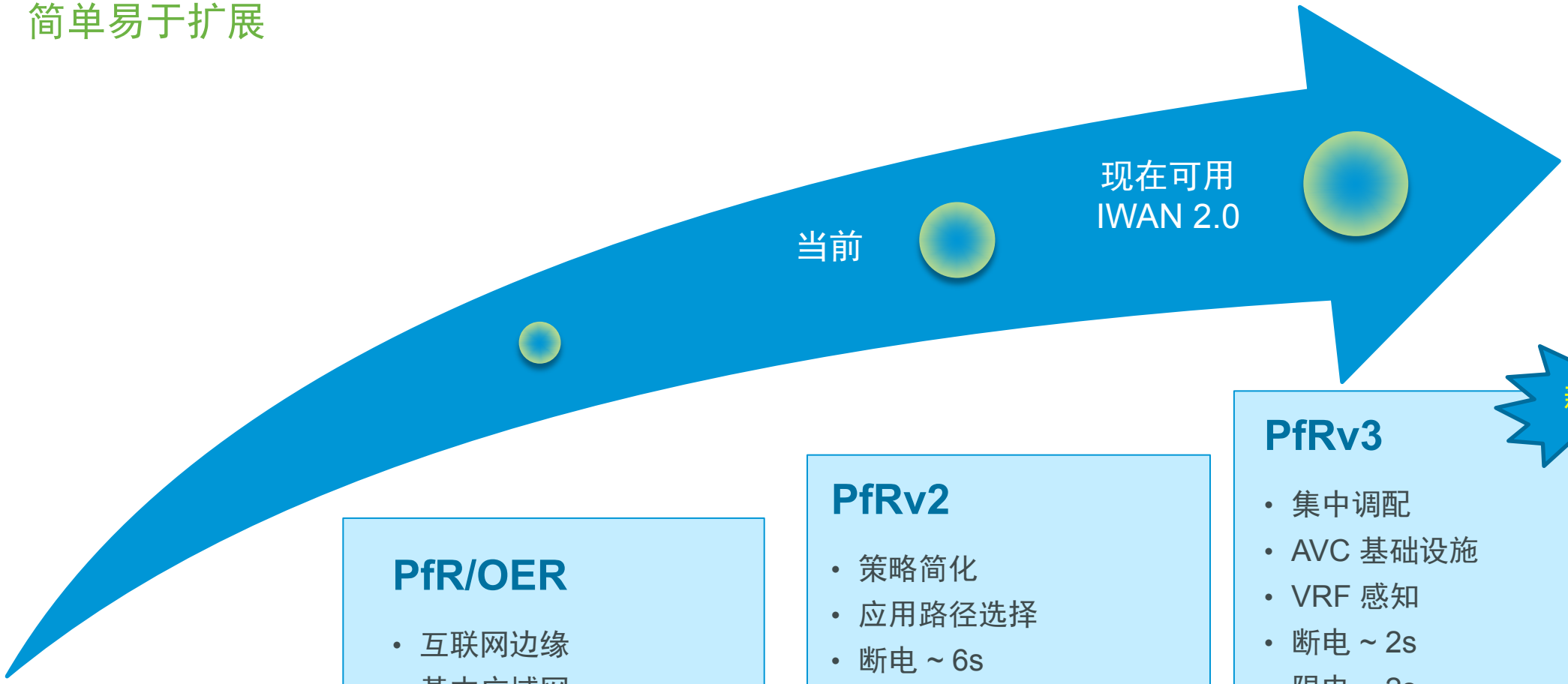
- 保护业务云应用免受限电影响
  丢失小于 5%
- 关键应用的首选路径：SP1 (MPLS)
- 通过让所有广域网路径、MPLS +互联网负载共享流量提高广域网带宽效率

多媒体和关键数据策略

- 保护语音和视频质量
  延迟小于 150 ms；
  抖动小于 20 ms
- 保护 VDI 应用免受限电影响
  丢失小于 5%
- 语音和视频首选路径 SP-A
- VDI 首选路径 SP-B
- 通过负载共享提高利用率

PfR 演进

简单易于扩展



PfR/OER

- 互联网边缘
- 基本广域网
- 调配/站点/策略
- 1000s 行配置

PfRv2

- 策略简化
- 应用路径选择
- 断电 ~ 6s
- 限电 ~ 9s
- 规模 500 个站点
- 10s 行配置

PfRv3

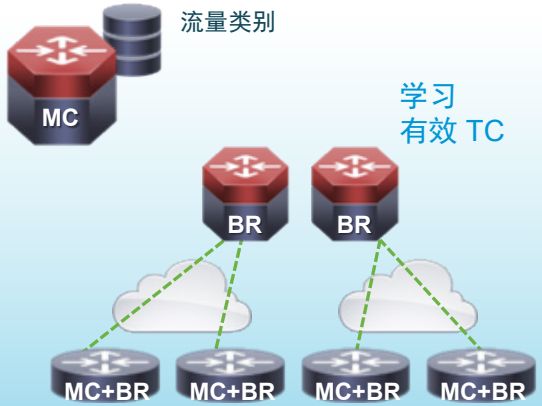
新的

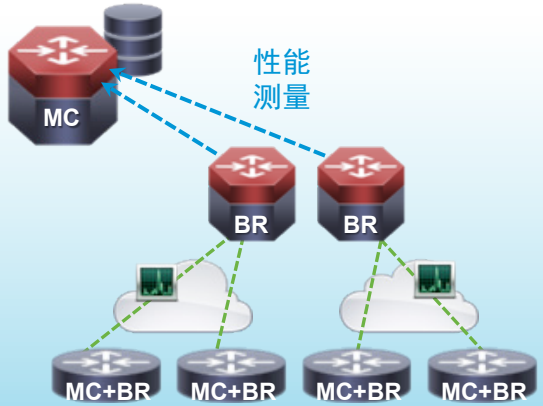
- 集中调配
- AVC 基础设施
- VRF 感知
- 断电 ~ 2s
- 限电 ~ 2s
- 规模 2000 个站点
- 仅限中心节点配置

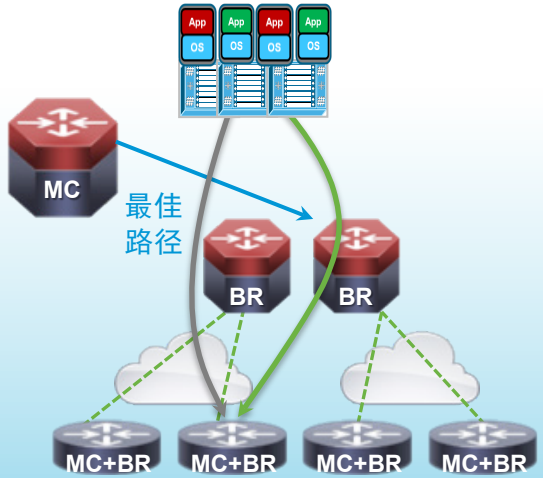
互联网边缘

PfR 工作原理

关键操作







定义您的流量策略

根据应用或传输分类器识别流量类别

了解流量

ISR G2 和 ASR 根据您的策略定义了解流经边界路由器 (BR) 的流量类别

测量

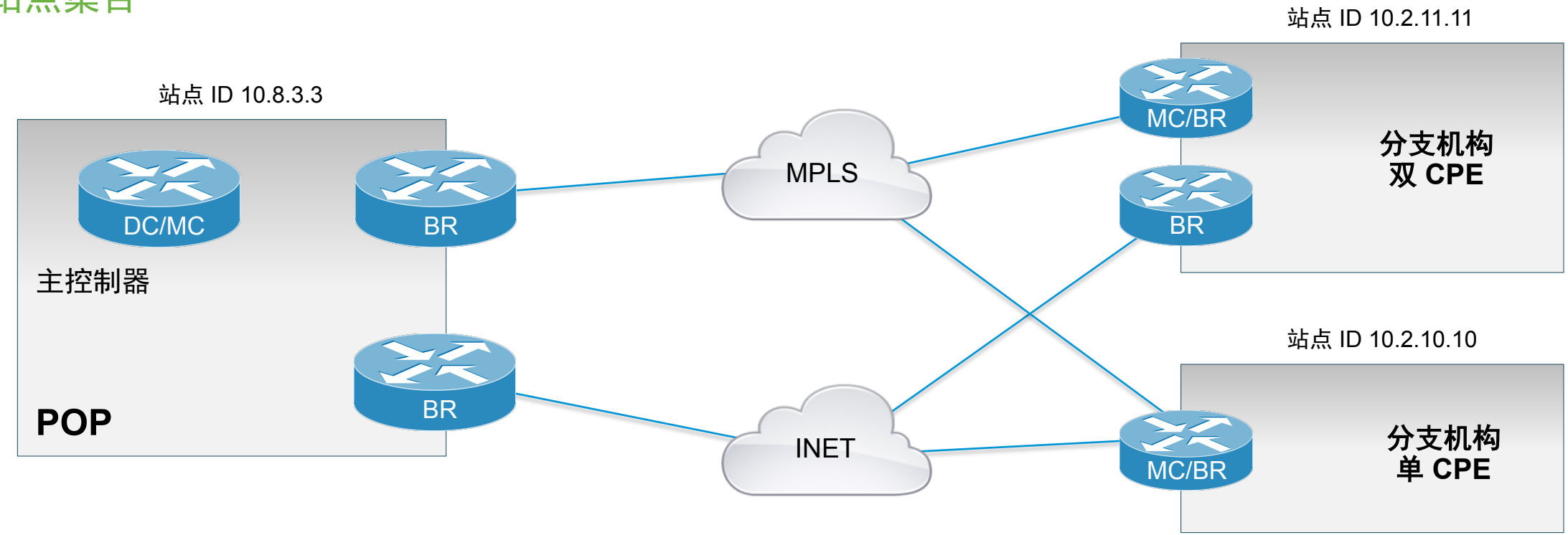
主动或被动测量流量和网络性能并向主控制器报告指标

路径执行

主控制器根据您的流量策略定义控制路径变化

IWAN 域

站点集合



- 广域网边缘的对等和协调
- 网络发现应用
- 广域网边缘测量应用性能，并向对等体发送性能反馈
- 建议规模：2000 个站点

性能路由 v3 路由控制器
组件

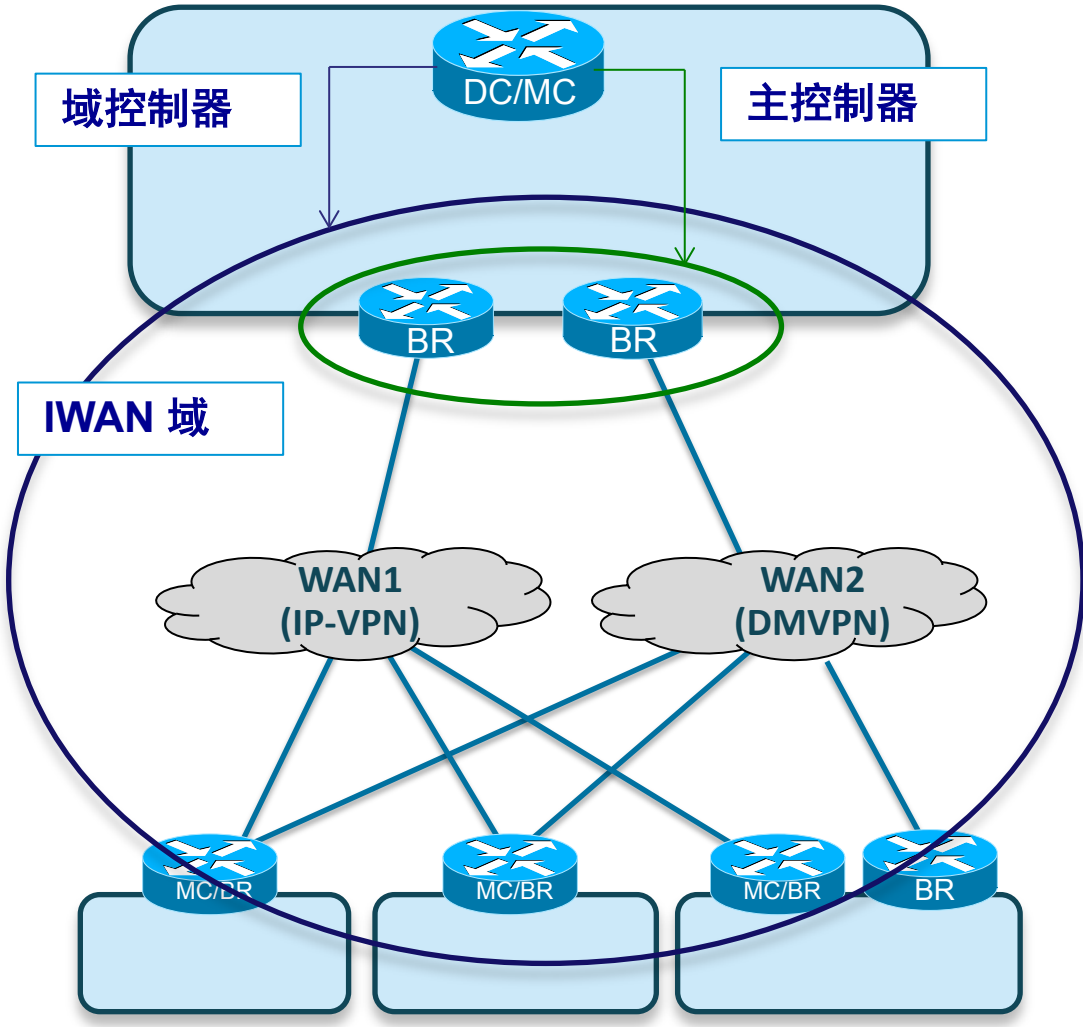
域控制器 (DC)
- 发现对等体
- 广告策略和服务；拓扑发现
- 每个域一个，与 MC 组合。

主控制器（路由控制器）
- 验证、报告和路由控制器
- 无需数据数据包转发/检测
- 确定最佳路径，并命令 BR 执行

转发路径：边界路由器 (BR)
- 在转发路径中获得网络可视性（了解、测量）
- 执行 MC 的决定（路径执行）

监控：
- 统一监控 - 被动
- 智能探头

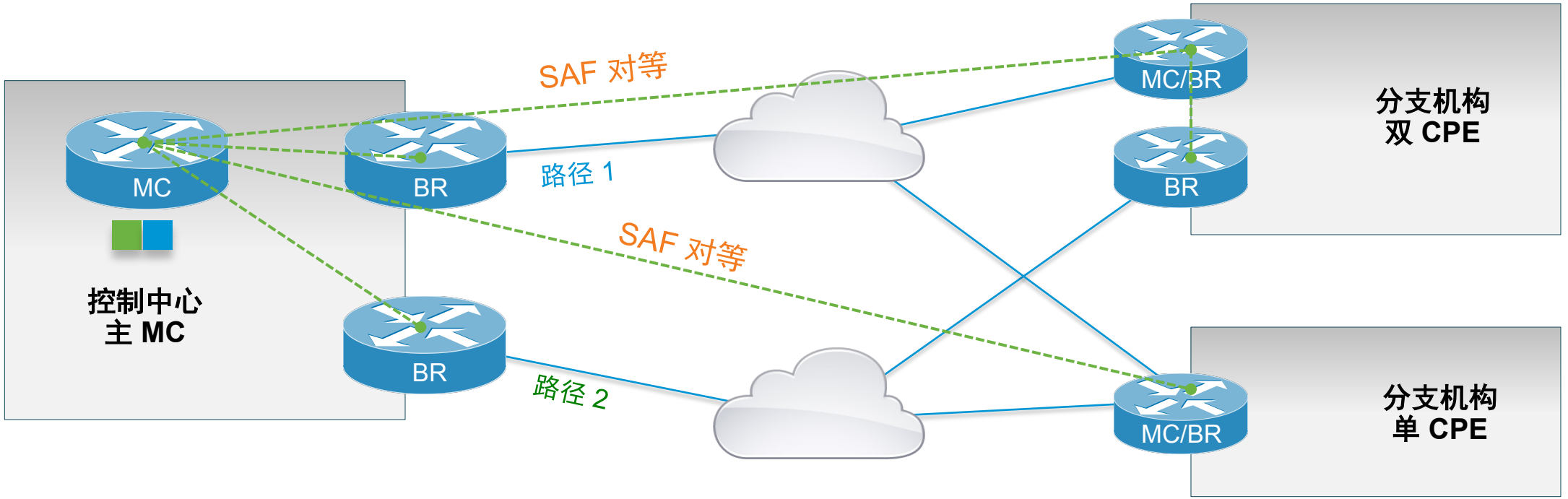
优化：
- 可抵达、延迟、丢失、抖动、
- 链路利用率、负载均衡、路径偏好



规模：建议最多 2000 个站点

IWAN 域

SAF 对等



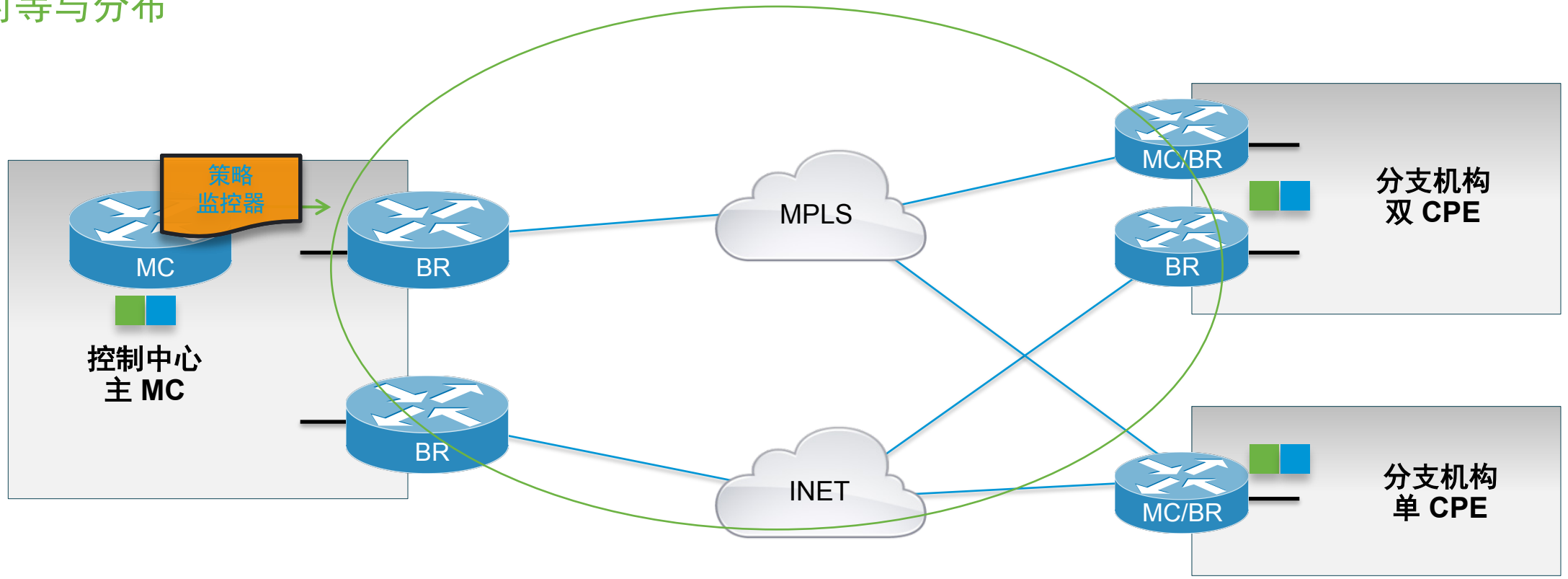
- 自动发现：
  - 策略与监控器
  - 站点和前缀/站点映射
  - 外部接口

```
domain one
 vrf default
  master branch
   source-interface Loopback0
   hub 10.8.3.3
```

策略
监控器

IWAN 策略与监控器

对等与分布

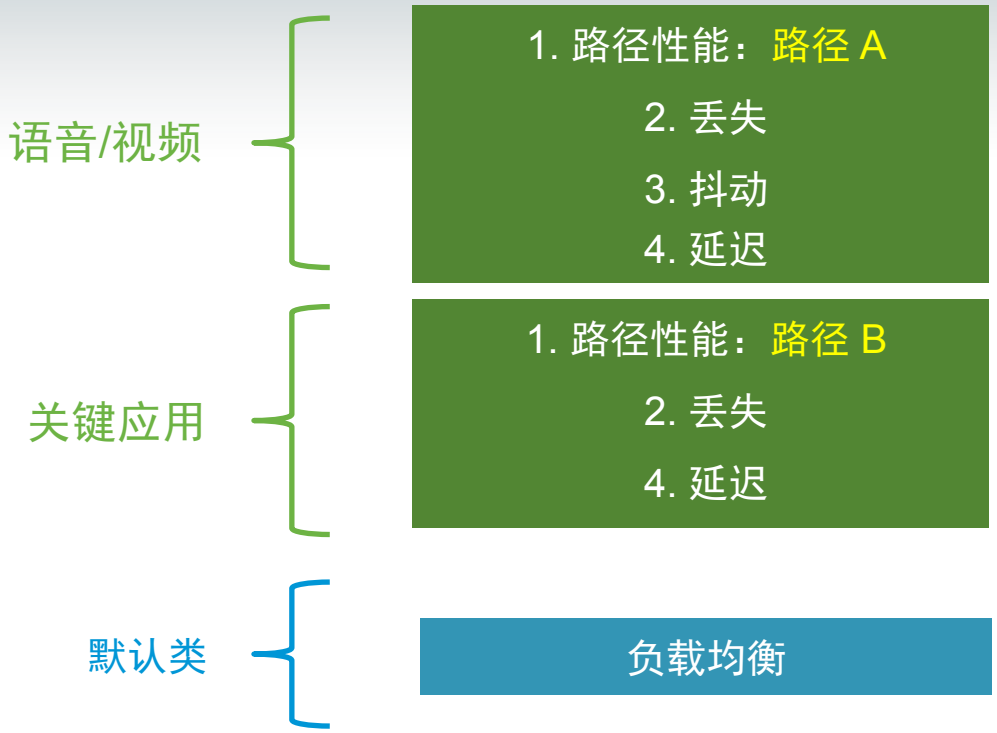


- 在控制中心 MC 上配置域策略和监控实例。
- 然后用对等基础设施将其分布到分支机构站点

定义应用性能策略

- 为各个通信类别选择您的策略操作
- 根据弹性指标选择替代路径

示例：



内置策略模板

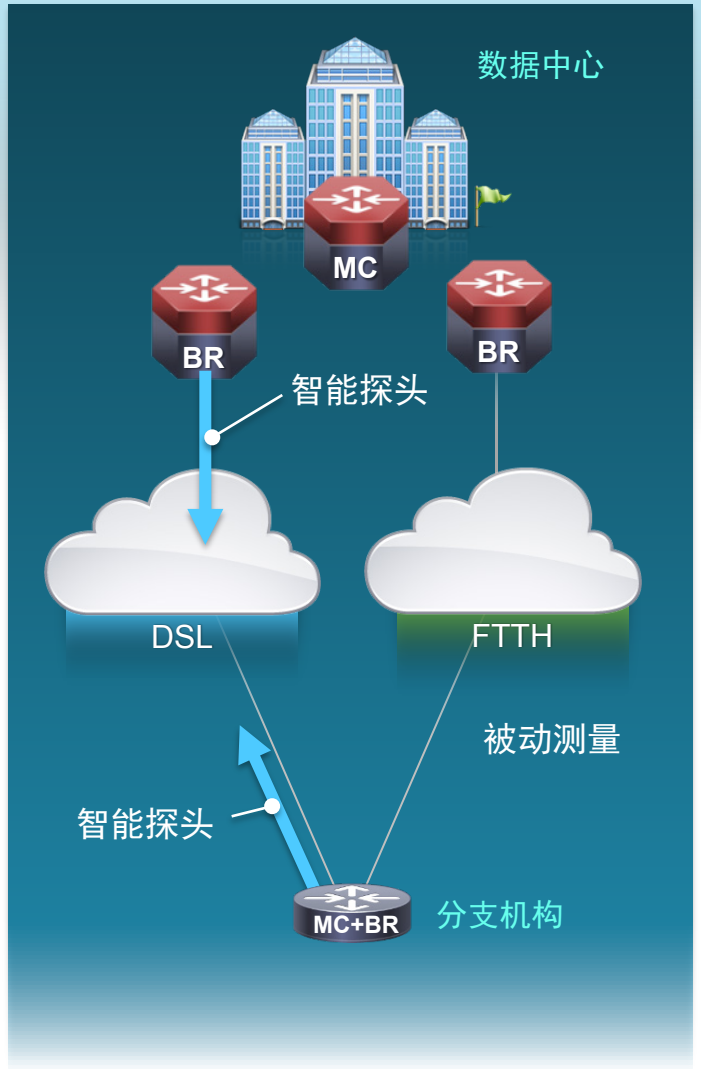
预定义模板	阈值定义
语音	优先级 1 单向延迟阈值 150 阈值 150 (msec) 优先级 2 数据包丢失率阈值 1 (%) 优先级 2 字节丢失率阈值 1 (%) 优先级 3 抖动 30 (msec)
实时视频	优先级 1 数据包丢失率阈值 1 (%) 优先级 1 字节丢失率阈值 1 (%) 优先级 2 单路延迟阈值 150 (msec) 优先级 3 抖动 20 (msec)
低延迟数据	优先级 1 单路延迟阈值 100 (msec) 优先级 2 字节丢失率阈值 5 (%) 优先级 2 数据包丢失率阈值 5 (%)

预定义模板	阈值定义
批量数据	优先级 1 单路延迟阈值 300 (msec) 优先级 2 字节丢失率阈值 5 (%) 优先级 2 数据包丢失率阈值 5 (%)
尽力而为	优先级 1 单路延迟阈值 500 (msec) 优先级 2 字节丢失率阈值 10 (%) 优先级 2 数据包丢失率阈值 10 (%)
Scavenger	优先级 1 单向延迟阈值 500 (msec) 优先级 2 字节丢失率阈值 50 (%) 优先级 2 数据包丢失率阈值 50 (%)

测量网络和应用性能

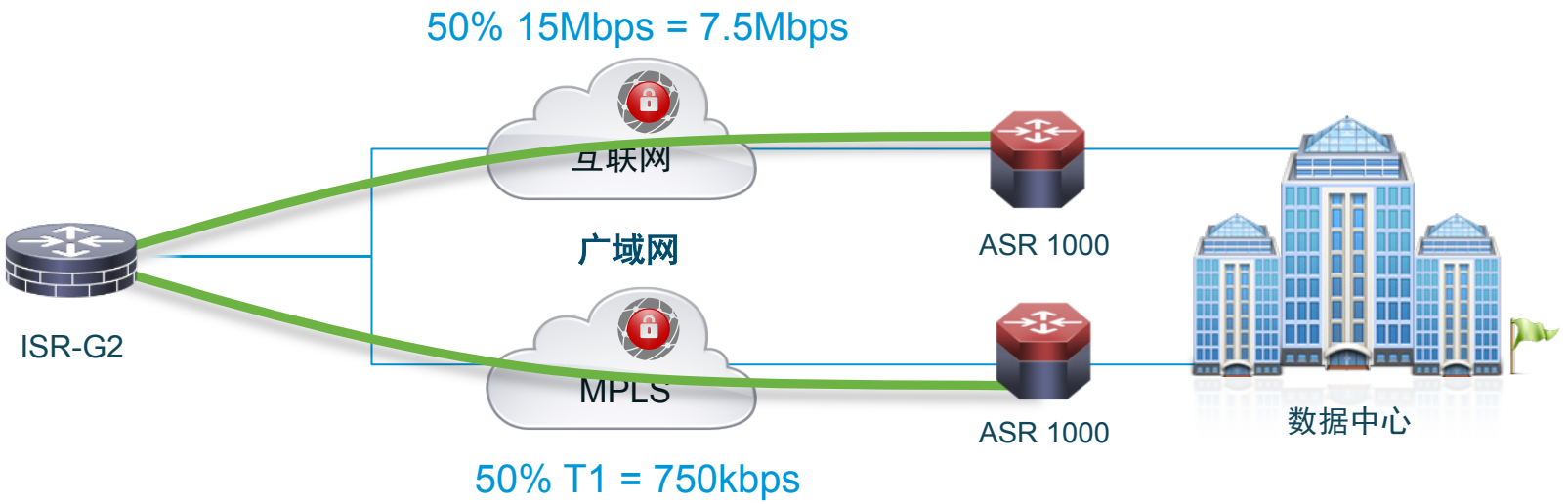
- 被动测量
  - 用于媒体、数据或“尽力而为”应用
  - 统一监控引擎（AVC 基础设施）
- 智能探头
  - 当没有用户流量时
  - 智能开/关
- PfR 自动启用性能监控器
  - 无需相关知识或配置经验
- MC 性能数据库用于确定策略实施操作

目标前缀	DSCP	应用 Id	延迟	抖动	丢失	入口 BW	出口 BW	BR	退出
10.1.1.1/32	EF		60	100	0	20	400	BR1	Gi1/1
10.1.10.0/24	AF31		110	15	0	52	60	BR1	Gi1/2
…	0		89	26	1	34	10	BR2	Gi1/1



负载均衡
最大化链路利用率以增加可用带宽

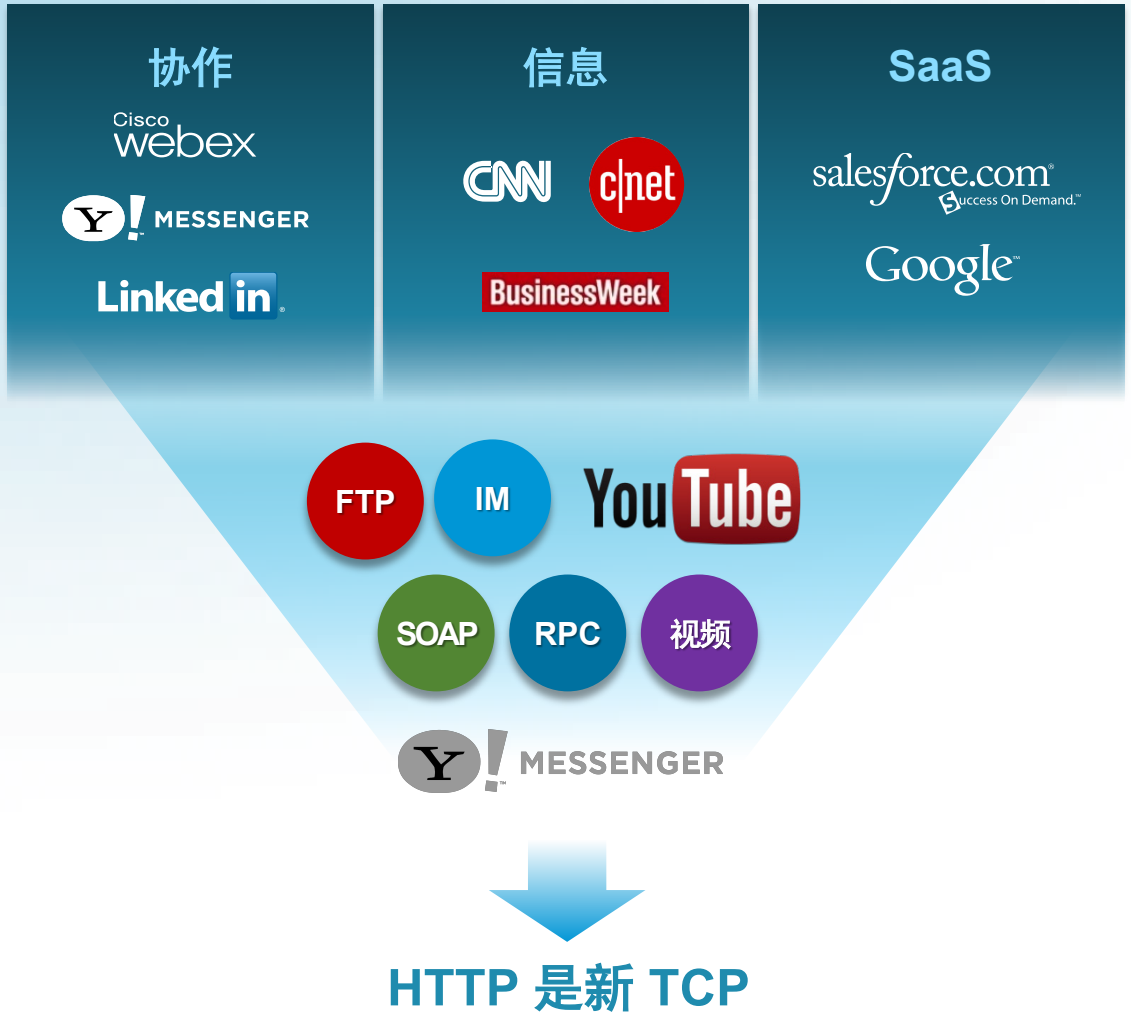
- 默认情况下，为默认类别启用外部链路负载均衡
- 在定义的百分比范围内，PfR 跨一组链路分布流量以保持高效利用率水平。
  默认利用率范围为 +/- 20%
- 外部链路可以有不同的可用带宽，
  例如，Int 1/0 = 1.5Mbps，Int 1/1 = 15Mbps
- 负载均衡默认值无法更改
  - 利用率范围为 20%
  - 最大利用率 = 链路容量



优化应用性能

现在的网络是一个 IT 盲点

- 静态端口分类已不再能够满足需求
- 越来越多的应用是不透明的
- 加密和混淆的使用越来越多
- 应用包含多个会话（视频、语音、数据）
- 如果用户体验未满足业务需求会怎么样？



IWAN –应用优化
通过应用可视性与可控性 (AVC) 实现

思科 AVC

无探头

- 丰富的数据收集 – Flexible NetFlow
- 无需额外硬件、AX 许可证
- 许多报告工具选项

智能容量规划

- 每个应用每个站点水平的报告
- 更好的信息可提高计划准确性

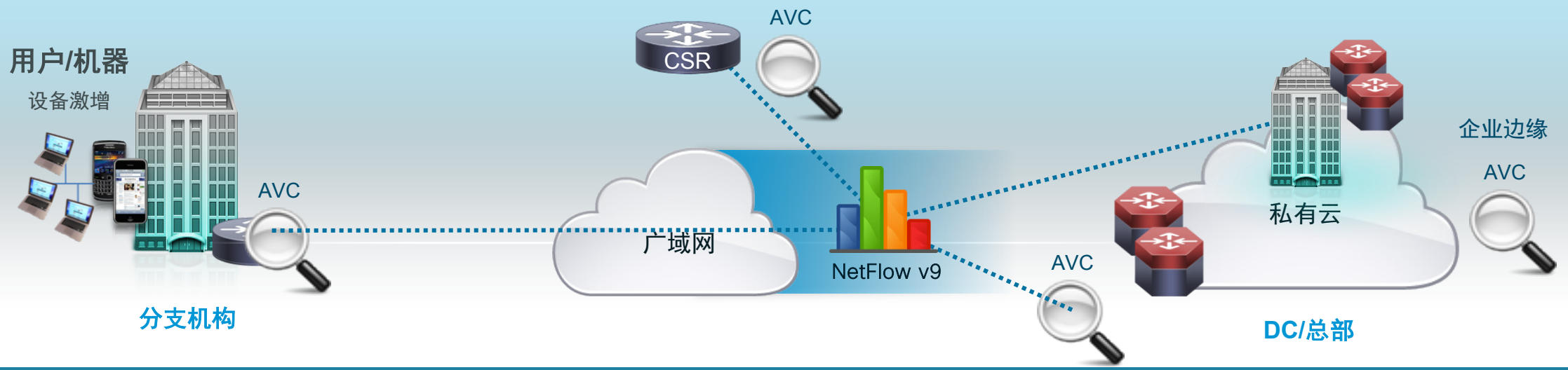
与业务一致的隐私实施

- 直观的应用策略
- 识别 http 内特定的云应用：

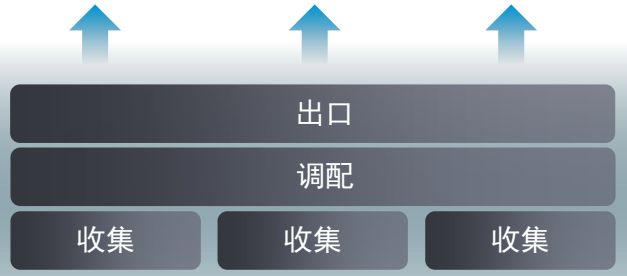
60% 的 IT 专业人员称云性能是关键挑战

IWAN 的应用性能监控

跟踪和报告应用流和性能



NetFlow v9 导出/IPFIX 导出



NetFlow/IPFIX 记录
（相同调配，相同格式）

- 流量统计数据记录
- 应用响应时间记录
- 媒体监控记录
  （应用、抖动、丢失等等）

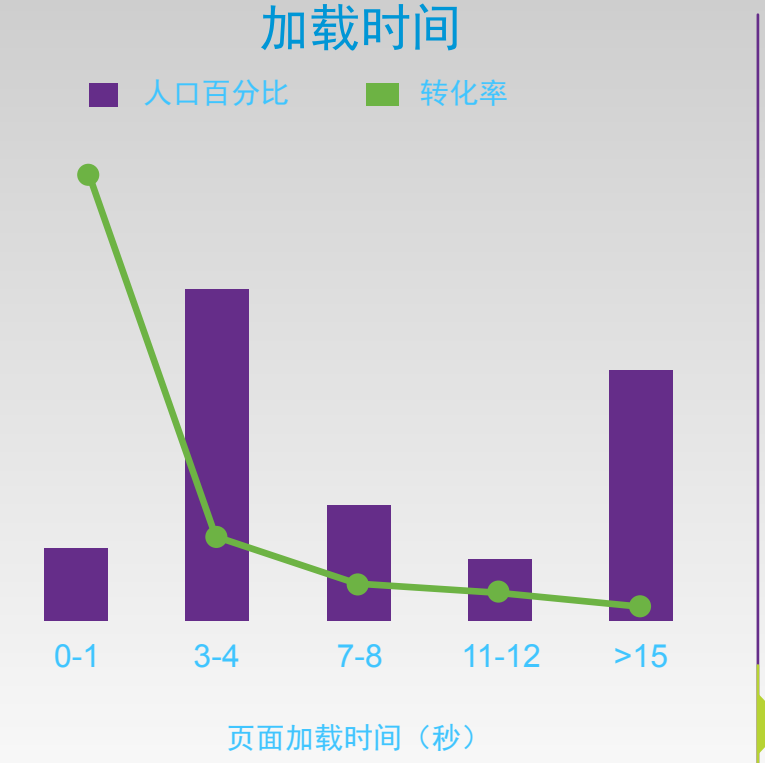
合作伙伴工具生态系统

InfoVista
Plixer
ActionPacked
CompuWare
CA Technologies
Living Objects
Glue

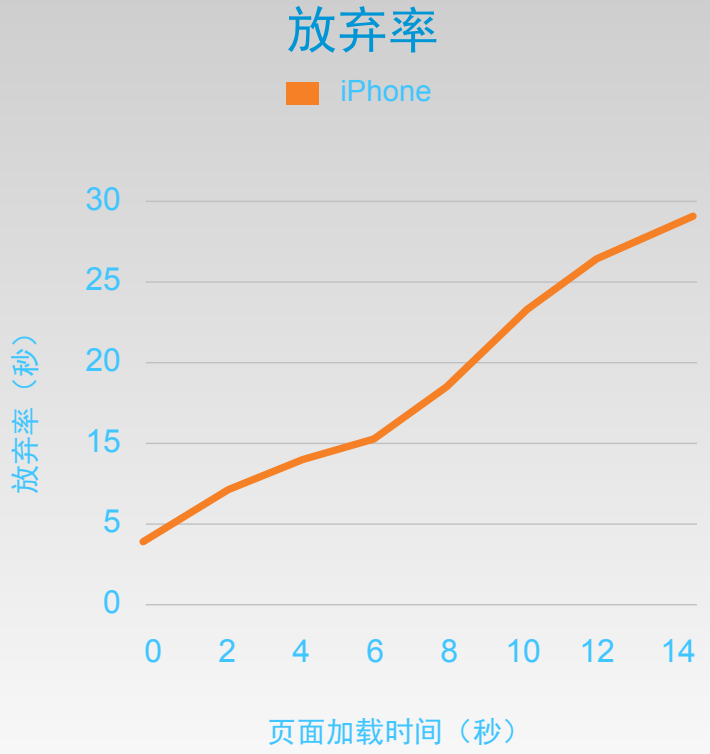
应用性能影响企业工作效率

收入损失

来源：Walmart

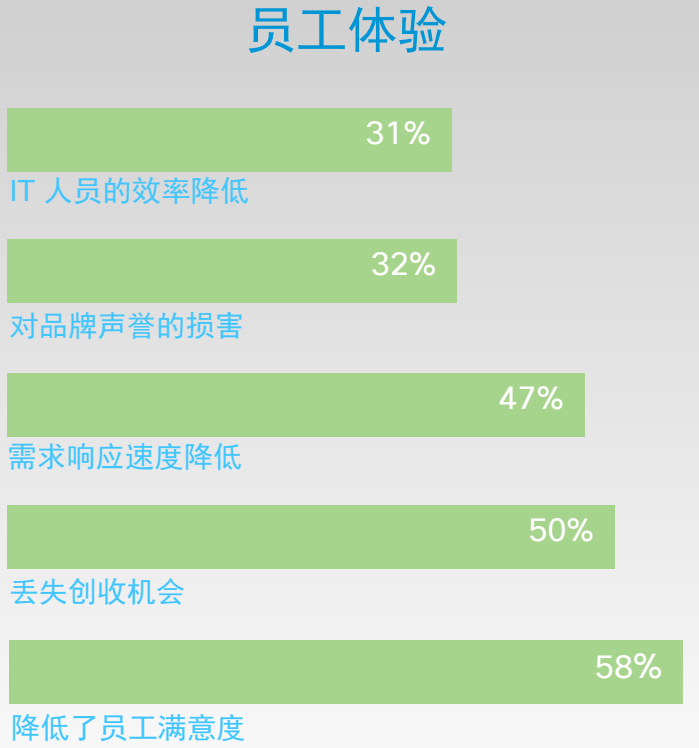


来源：Akamai



员工工作效率

来源：Aberdeen Group



较慢页面

转换率低

员工体验

客户满意度

Cisco WAAS

增强用户体验，提高广域网效率

问题

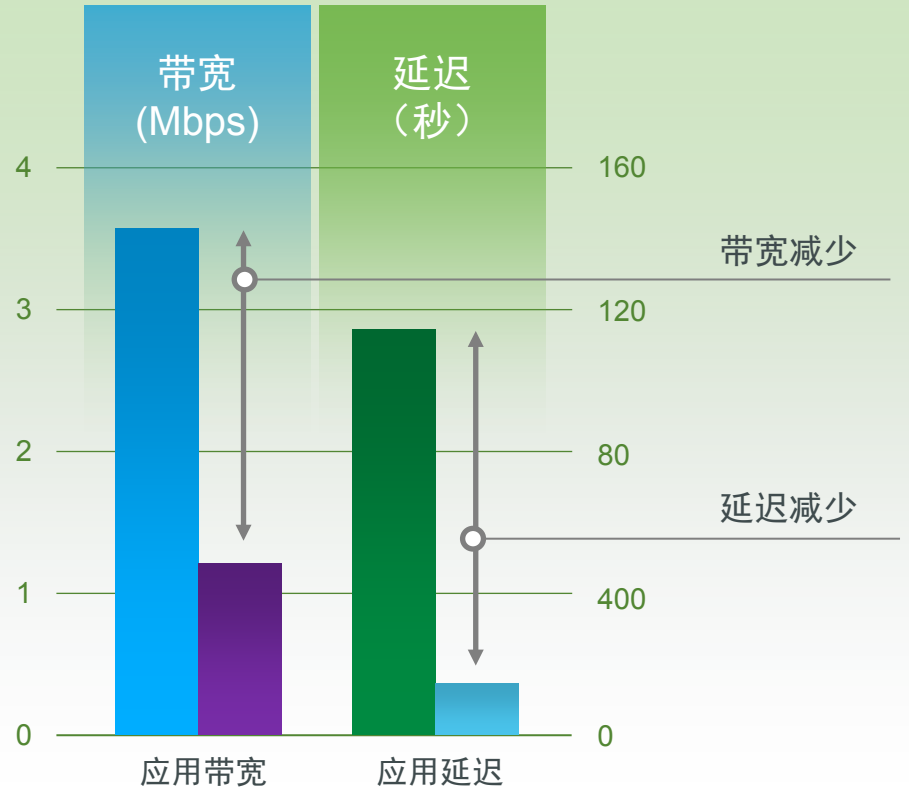
- 应用延迟
- 广域网带宽效率低下

解决方案

- 减少负载

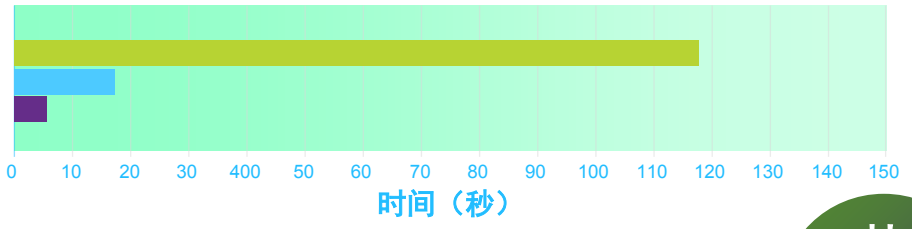
  消除数据冗余 (DRE)、压缩和 TCP 优化
- 应用优化

  较少的协议消息和元数据缓存



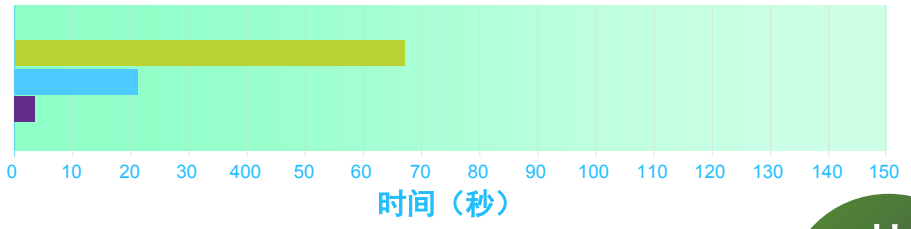
优化和增强成千上万的应用程序
AX 包括 Cisco WAAS 广域网优化

邮件（5MB 的附件）



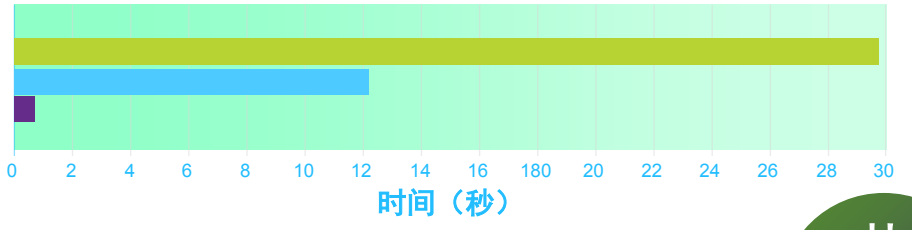
快 24 倍

文件服务（5MB 的文件）



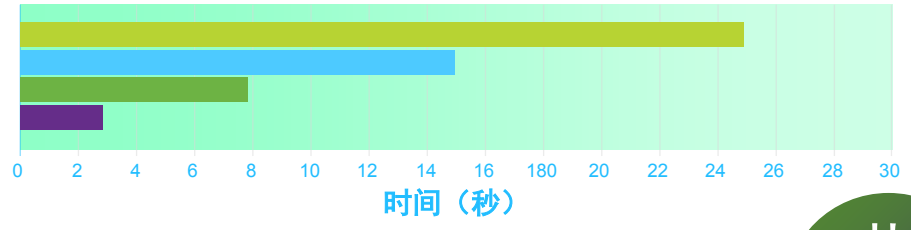
快 17 倍

Microsoft SharePoint（5MB 的文档）



快 30 倍

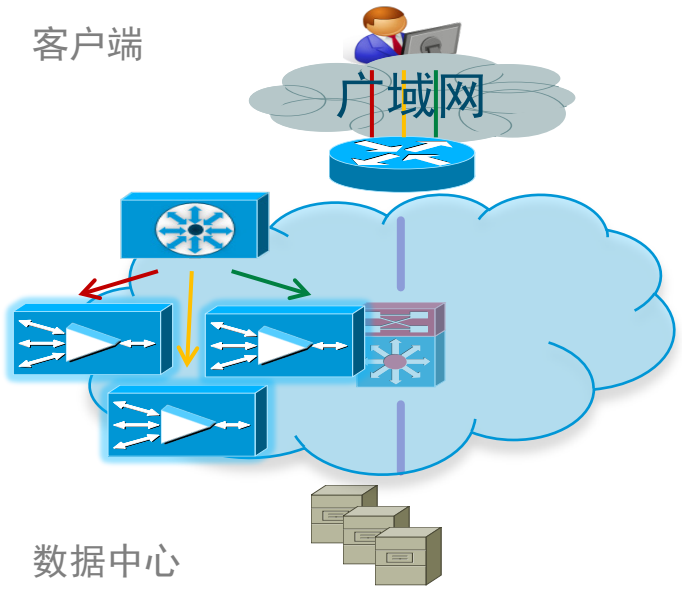
CITRIX® VDI (Citrix)



快 3-8 倍

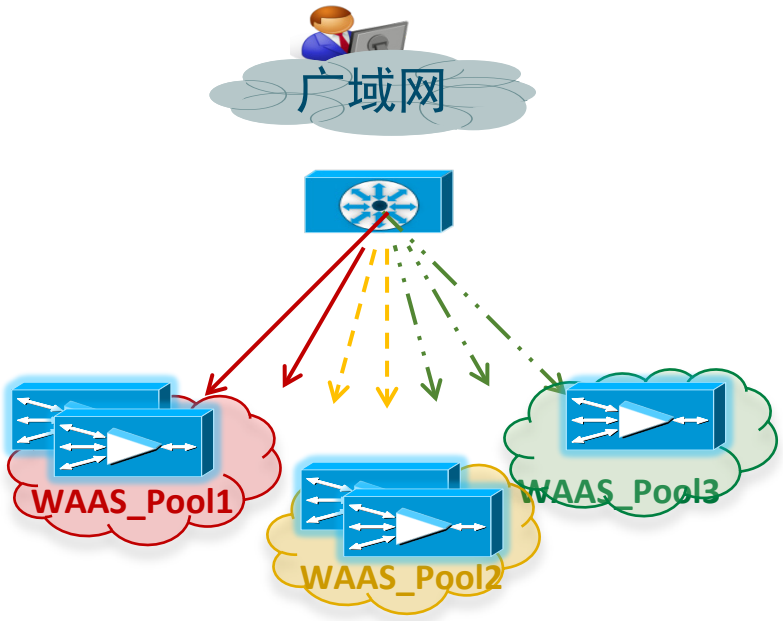
Cisco AppNav 虚拟化技术

将广域网优化资源虚拟化成**带业务驱动绑定的弹性资源池。 极大简化** WAAS 部署和管理



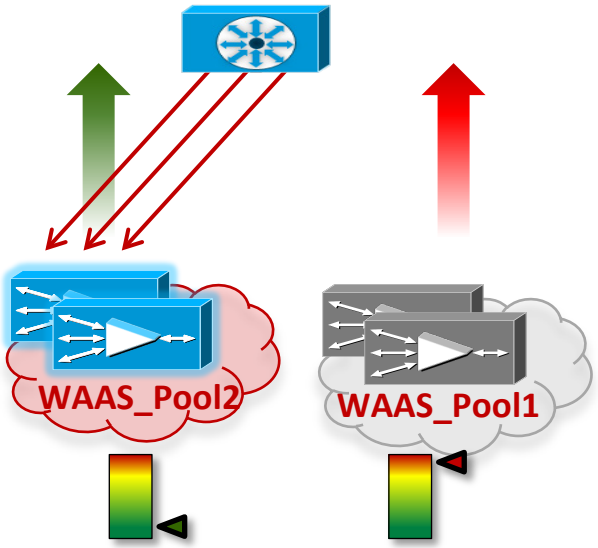
抽象性

- ✓ 混合外形
- ✓ 从拓扑分离



分区

- ✓ 流量分类
- ✓ 逻辑分组
- ✓ 基于应用、分支机构、服务器

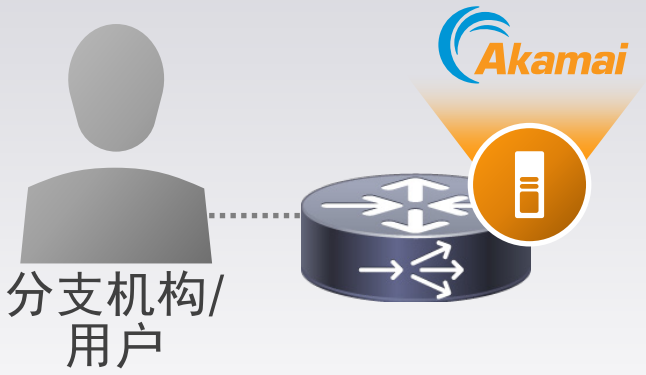


弹性

- ✓ 动态资源创建
- ✓ 基于负载的响应
- ✓ 云弹性

思科和 Akamai 规划图：
实现下一代优化

最后一英里优化



全渠道
丰富的内容交付
增强的体验

企业级互联网广域网

更高的应用性能
MPLS 的低成本替代

服务感知交换矩阵

完整的网络流量优化
用于 SAAS 应用
提高工作效率

2014 年第 2 季度

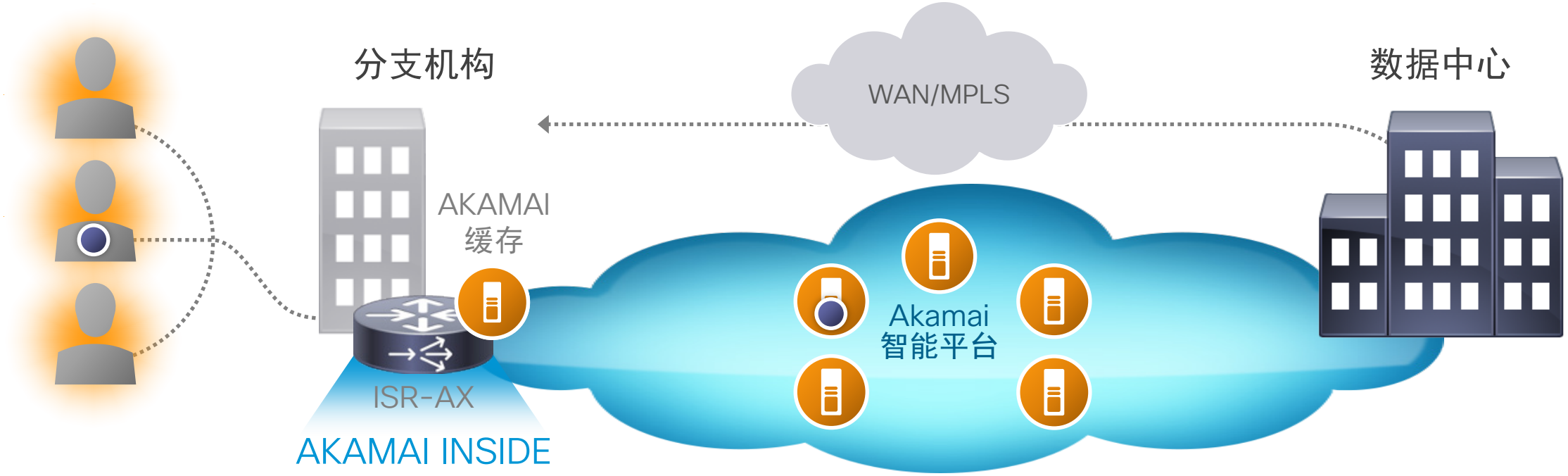
开发中

用边缘缓存将 Akamai 扩展到分支机构

Akamai Inside Cisco

现在可用！

用分支机构中的 AKAMAI 完成最后一英里



优化体验，无论是设备、连接还是云

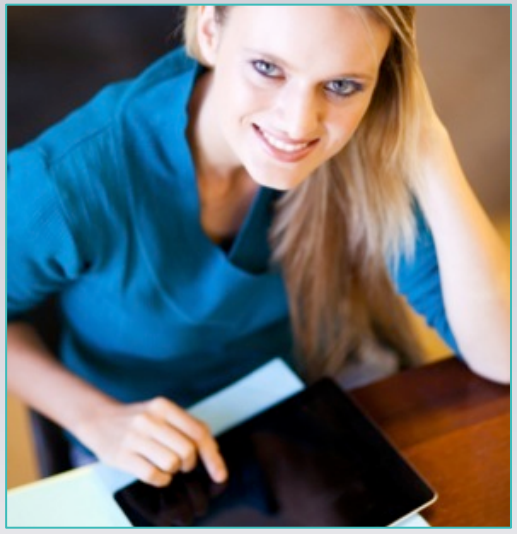
私有、公共、Akamai 云中的所有 HTTP 流量

预先部署 | 动态 HTTP 缓存 (YouTube) | 任何传输方式

零售商应用程序基准评分结果

移动辅助销售

	无 AC	有 AC 第 1 次点击	有 AC 第 2 次点击
ERP 应用	57s	18s	**2s**
修复应用	70s	28s	**<1s**
目录应用	28s	13s	**<1s**



全渠道

	无 AC	有 AC
CompanyA.com	5.44s	2.72s
CompanyB.com	4.25s	2.60s

培训

	无 AC	有 AC
默认质量	144p	**720p（高清自动）**
加载时间（720p 高清）	14s	**<1s**

Akamai 缓存技术

1

透明缓存：有四 (4) 种不同的模式设置

基本

- 遵循 IETF *HTTP 1.1* 指南进行标准对象缓存
- 只有缓存响应明确标记为可缓存

标准

- 默认模式
- 也缓存对象，无明确缓存标记，但有最近更改日期。忽略客户端的“重载”
  报头

高级

- 更具攻击性的缓存媒体文件，且所有对象类型的时间更长（当无明确到期时间时）

绕过

- 关闭配置站点的缓存

2

连接缓存 (CC)：

从 *Akamai 的智能平台*检索内容

3

过多缓存 (OTT)：

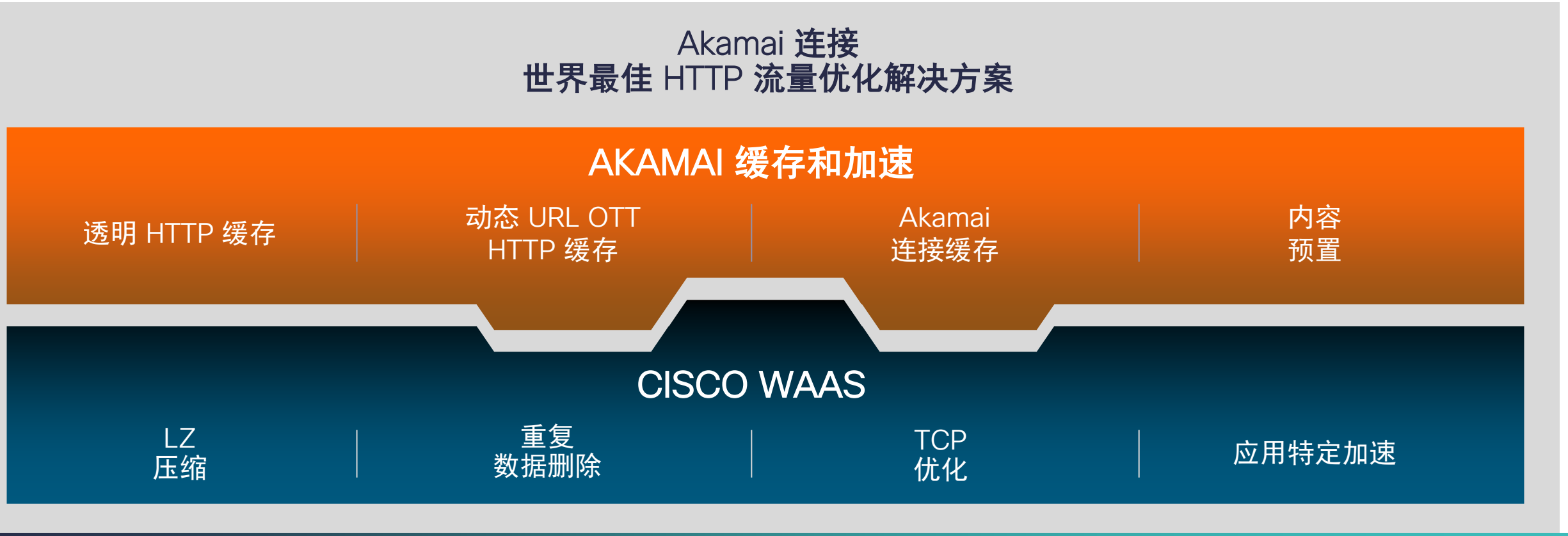
使用预定义配置的第三方网站的缓存内容

4

缓存预热或预先部署：

*预先安排的*网站内容获取和缓存

基于 Cisco WAAS 解决方案
边缘缓存增强用户体验

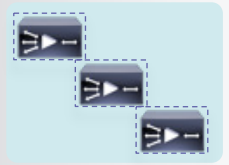


现在支持
Akamai 云 | 单边优化 | 安全的直接互联网接入

思科广域网应用优化服务 (WAAS)
提高应用性能和用户体验

WAAS 设备
- 应用加速
- 分支机构的虚拟刀片
- 可进行一系列部署的可扩展平台

虚拟 WAAS
- 适用于与其他应用一起在 ISR G2 或 ISR 4K 中 UCS-E 上托管
- 私有或虚拟私有云的应用加速
- VMWare ESX/ESXi 和 Cisco UCS® 部署
- 灵活、弹性、多租户的部署
- 物理和虚拟 WAAS 的共同管理



ISR-WAAS

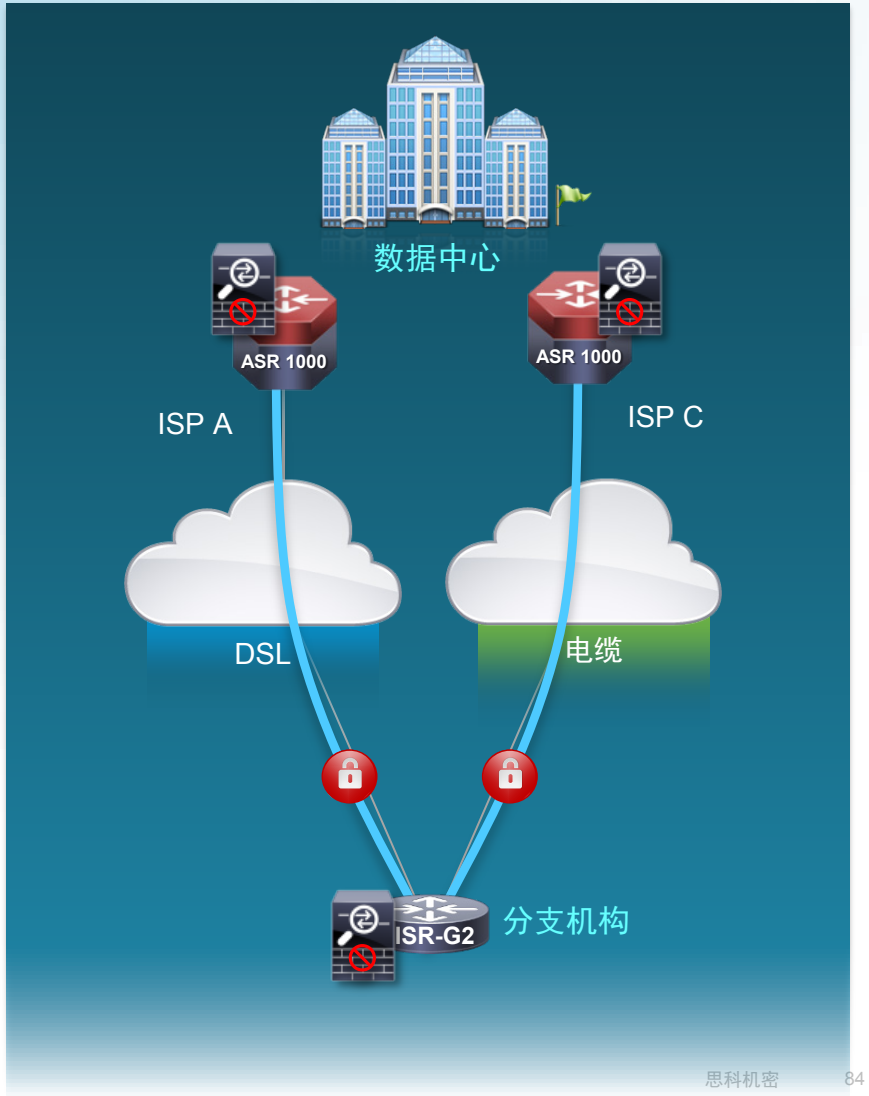
- ISR 4000 上的零足迹集成
- 与其他 WAAS 选项的功能和管理相同
- 安装简单，在 7 分钟内即可顺利启动和运行
- 用 AppNav 无缝增加容量

WAAS 服务就绪引擎
- 集成的 ISR G2
- 应用加速
- 软件按需调配
- 无叉车式升级

保护您的 IWAN

保护 IWAN IPSec VPN 和防火墙

- 第 1 步：安全传输
  - IPSec 与 DMVPN 覆盖
    - 与链路方式无关的安全传输
    - 添加强加密：IKEv2 + 椭圆曲线加密（套件 B）
    - 前门 VRF 设计
- 第 2 步：威胁防御
  - IOS 基于区域的防火墙
  - 最大限度地减少暴露
    - 用于互联网和隧道接口的 DHCP 寻址
    - 不要将隧道地址放入 DNS
- 第 3 步：选择您的性能级别
  - 根据加密服务和广域网带宽按大小对路由器进行排列
    - 头端：ASR1000 或 ISR4400
    - 分支机构：ISR-G2 或 ISR4k

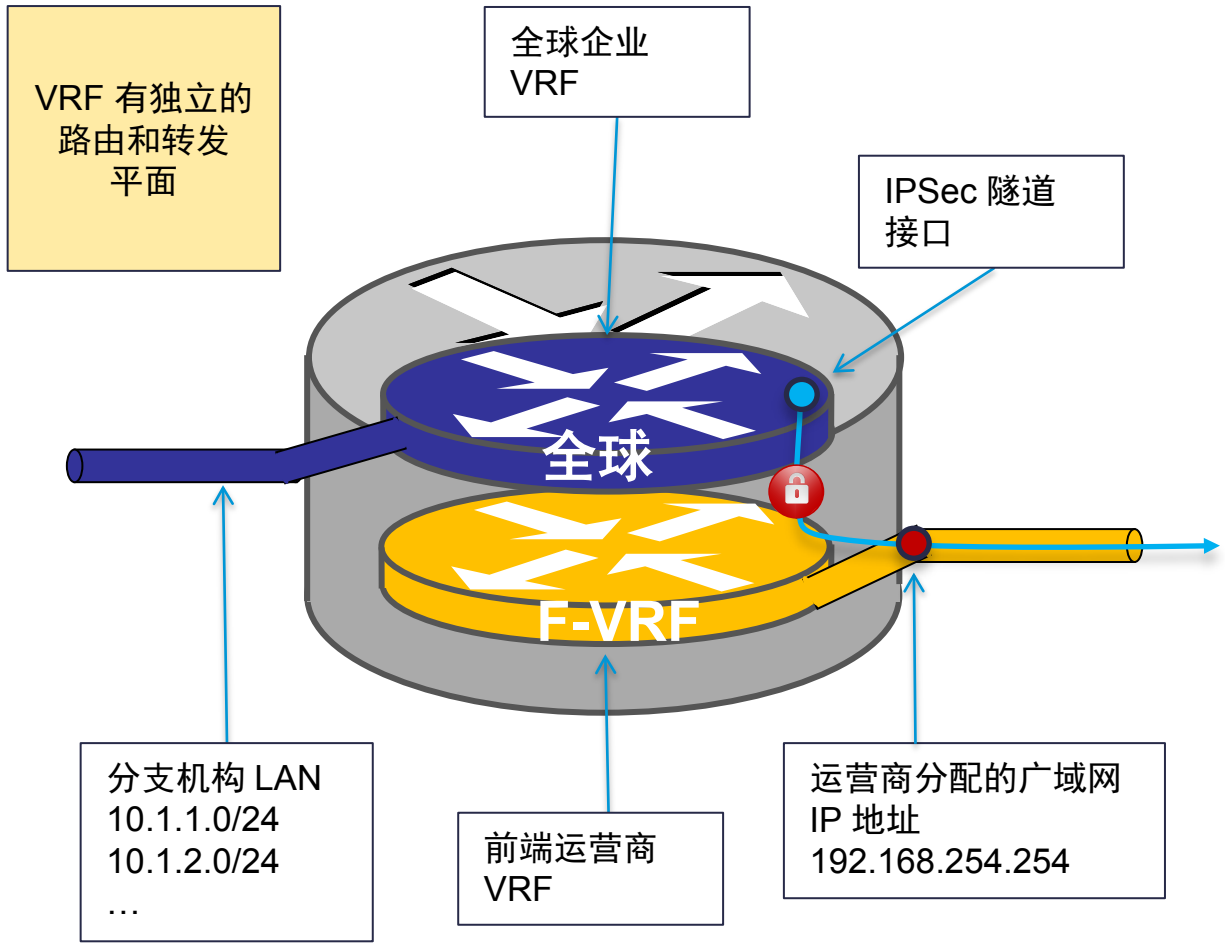


安全传输的要素

- 通常，广域网以受信任的 SP 连接为构建基础
- 信任是基于基础设施的隐私和 SP 控制的基础设施接入
- 用同样的方法确保传输的保密性；无需加密，即可保护数据隐私。
- 通过控制接入最大程度减少基础设施攻击；限制仅接入受信任的对象。
- 企业信息安全假设 SP 确保对 VPN 有访问权限的活动者是受信任的活动者 - 例如，基础设施上的其他租户
- 通过逻辑 VPN 分类对租户进行分隔

用前门 VRF 保护 IWAN 传输

隔离外部网络

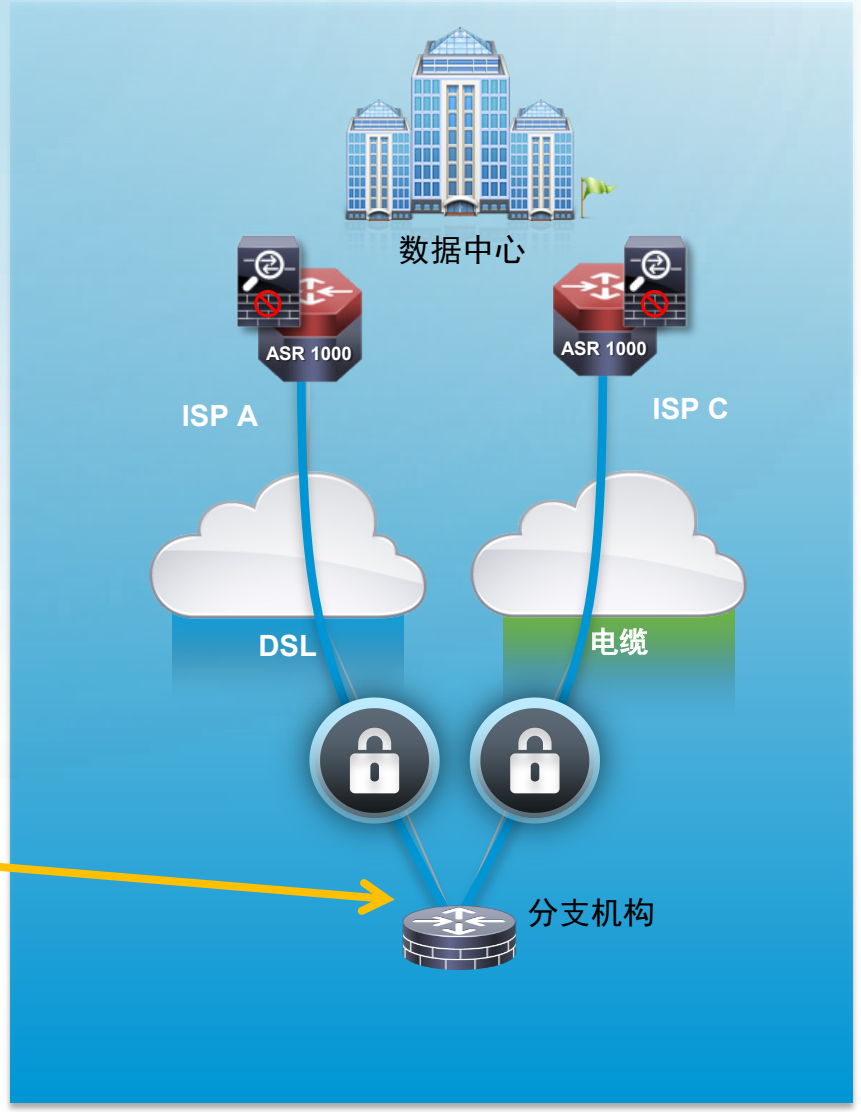


- 虚拟路由转发 (VRF) 可在一个设备上创建多个逻辑路由器
  - 每个 VRF 都有单独的控制/数据平面
  - 默认情况下，VRF 之间没有任何连接
  - 运营商端 VRF（黄色）用于外部网络，全球 VRF（蓝色）用于内部网络
- 运营商 VRF 最大程度减少与威胁的接触
  - 只有运营商 VRF 中有默认路由
  - 运营商分配的 IP 地址隐藏内部网络
  - 运营商 IP 地址用作 IPSec 隧道源
  - 内部全球 VRF 与运营商前端 VRF 之间只允许 IPsec

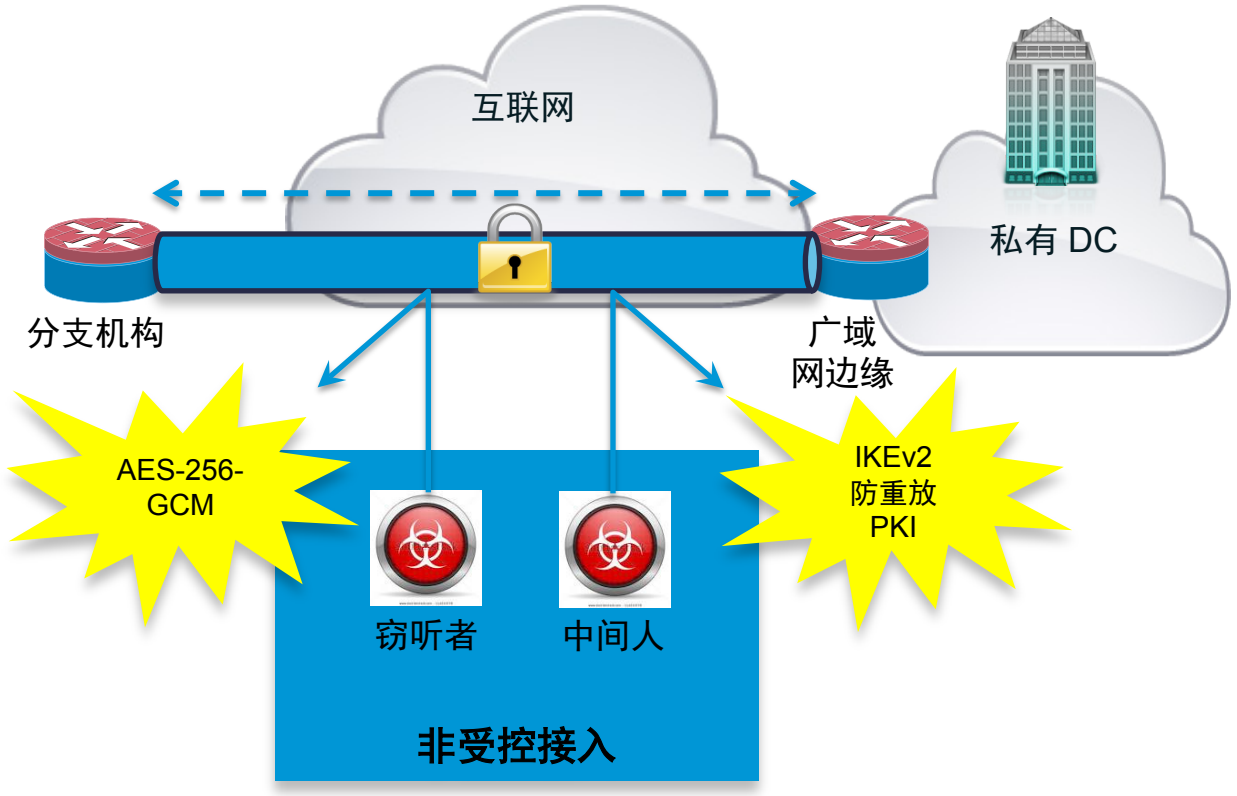
保护面对公众的 IWAN 接口

- 使用 ACL、ZBFW 或 ASA 阻止除 DMVPN 隧道流量之外的所有流量进入路由器
- 如果有直接互联网接入计划，则在分支机构设置基于区域的防火墙 (ZBFW)
- 用于保护互联网接口的典型 ACL

```
interface GigabitEthernet0/0
 ip vrf forwarding INET-PUBLIC1
 ip access-group ACL-INET-PUBLIC in
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
```

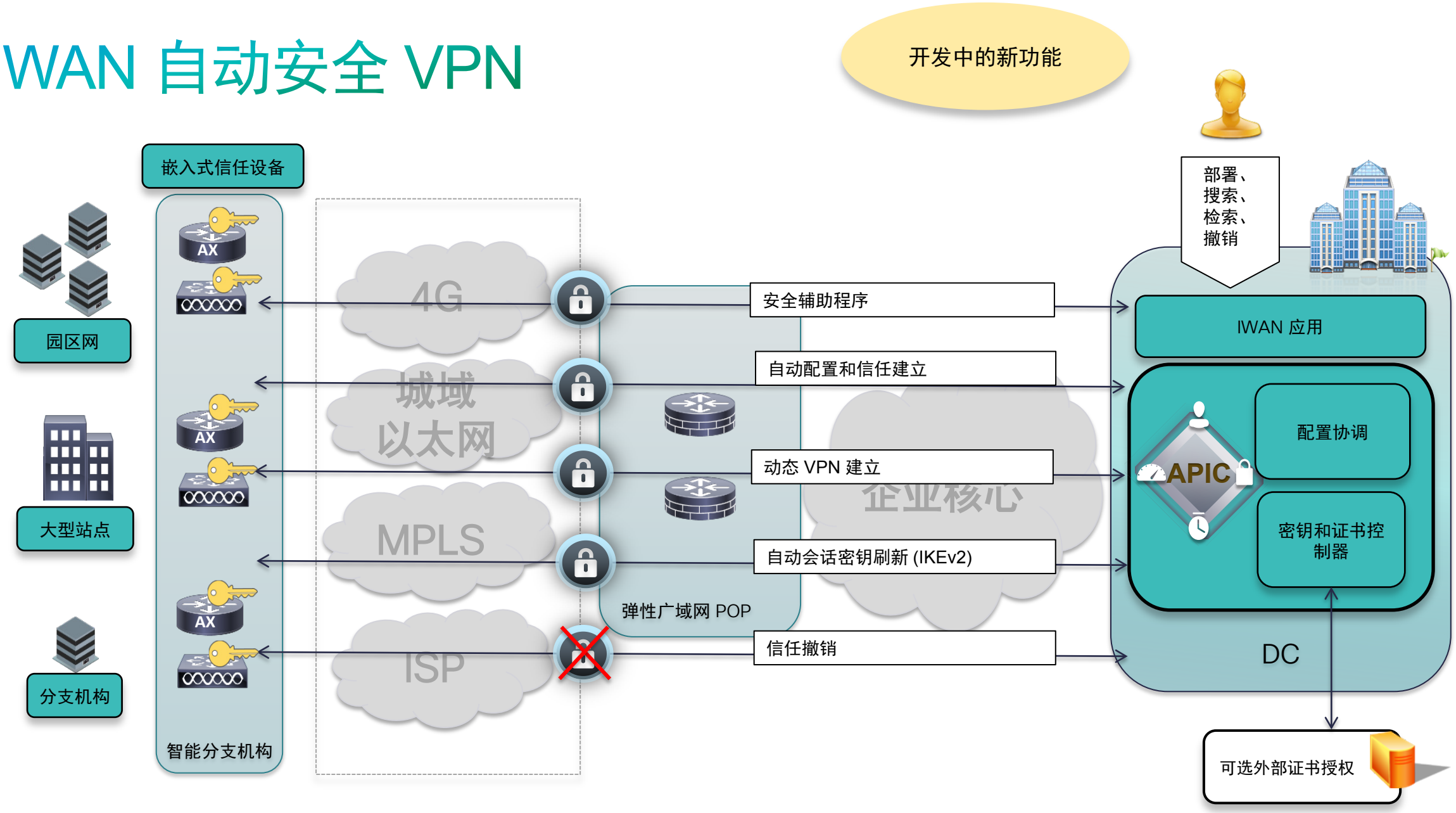


确保机密性
IKEv2 + 强加密



- 通过强大的认证加密和 IPSec 架构保护传输
- 保护免受窃听和中间人攻击
- 用于 192 位安全级别的 256 位的高级加密标准椭圆曲线加密 (AES-256-GCM)
- 通过 IKEv2 进行安全、信任的传输安全设置
- 最强的身份验证和密钥交换算法：
  ECDSA、ECDH 和 SHA-2 (SHA-256/384)
- 用于非保密和最保密信息类别的认证 NSA

IWAN 自动安全 VPN



通过 DMVPN 进行 TrustSec SGT

问题陈述

- 用于非 IT 标准设备的 BYOD 支持
- 执行一致的安全政策

解决方案概述

- 用于情景感知防火墙实施的安全组标记 (SGT)
- 通过 DMVPN、FlexVPN、GETVPN 进行安全组标记传输

解决方案特征

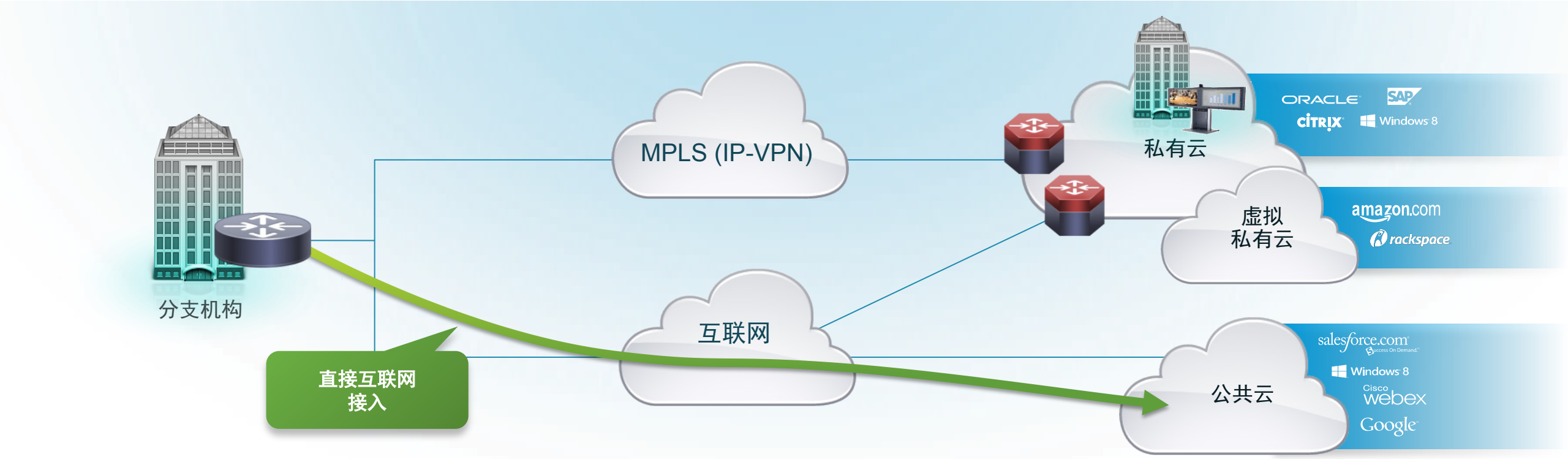
- 基于身份的安全继而；不让外来者进入
- 根据身份控制接入和服务水平
- 用户和设备授权接入

可扩展性

- 100 Gbps FW（ASR1K 与 ESP100）
- 350K CPS 时支持高达 6M 的会话（ASR1K 与 ESP100）

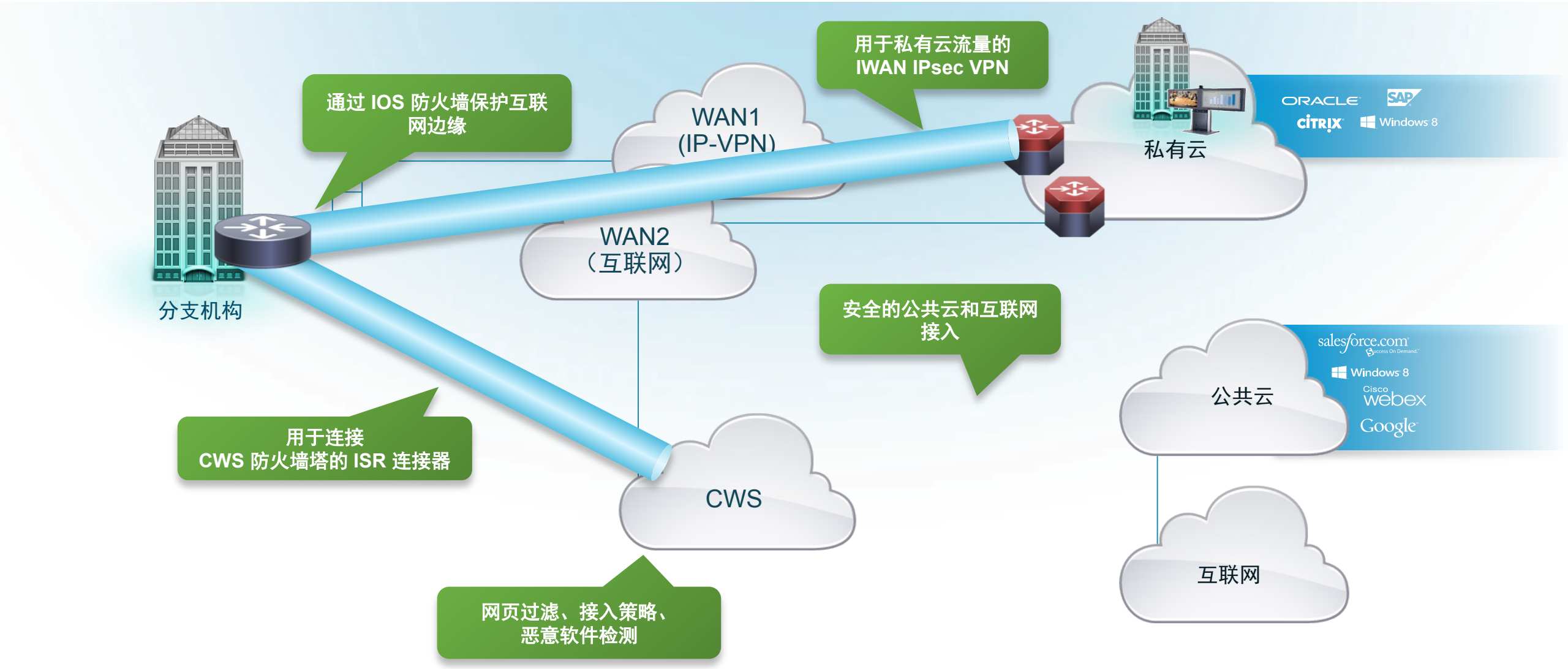
分支机构互联网接入

智能广域网 - 直接互联网接入

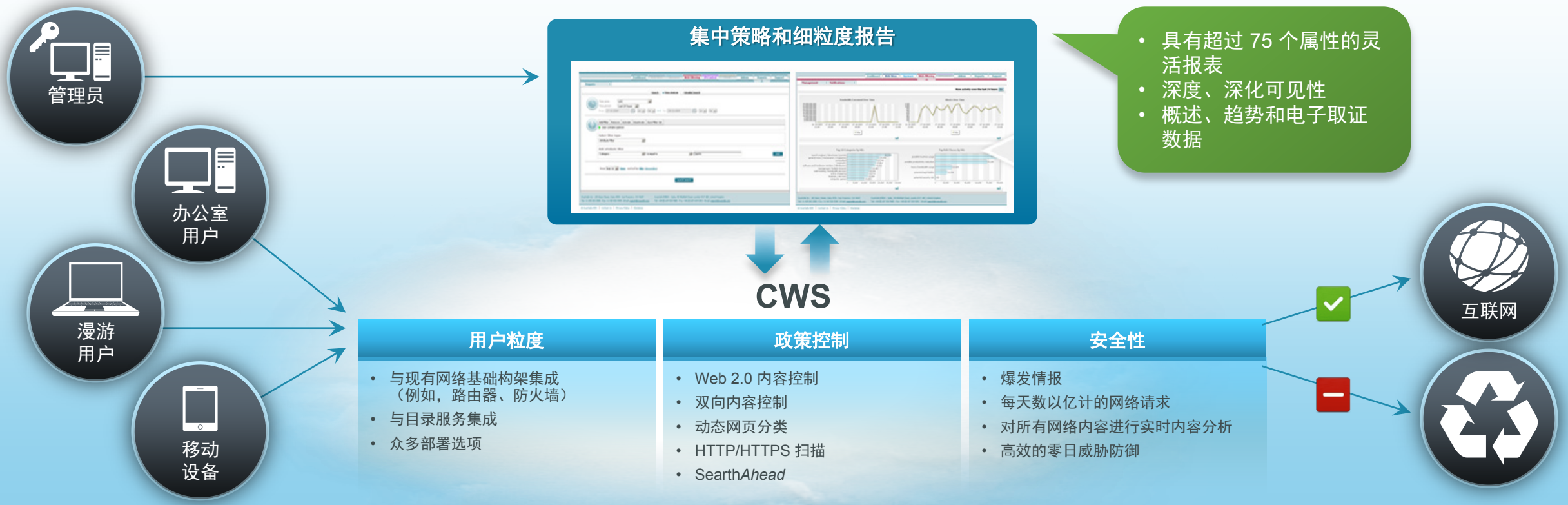


- 利用**本地互联网路径**接入公共云和互联网
- 提高应用性能（正确的流用于正确的地方）

通过 Cisco Cloud Web Security (CWS) 进行安全的互联网接入



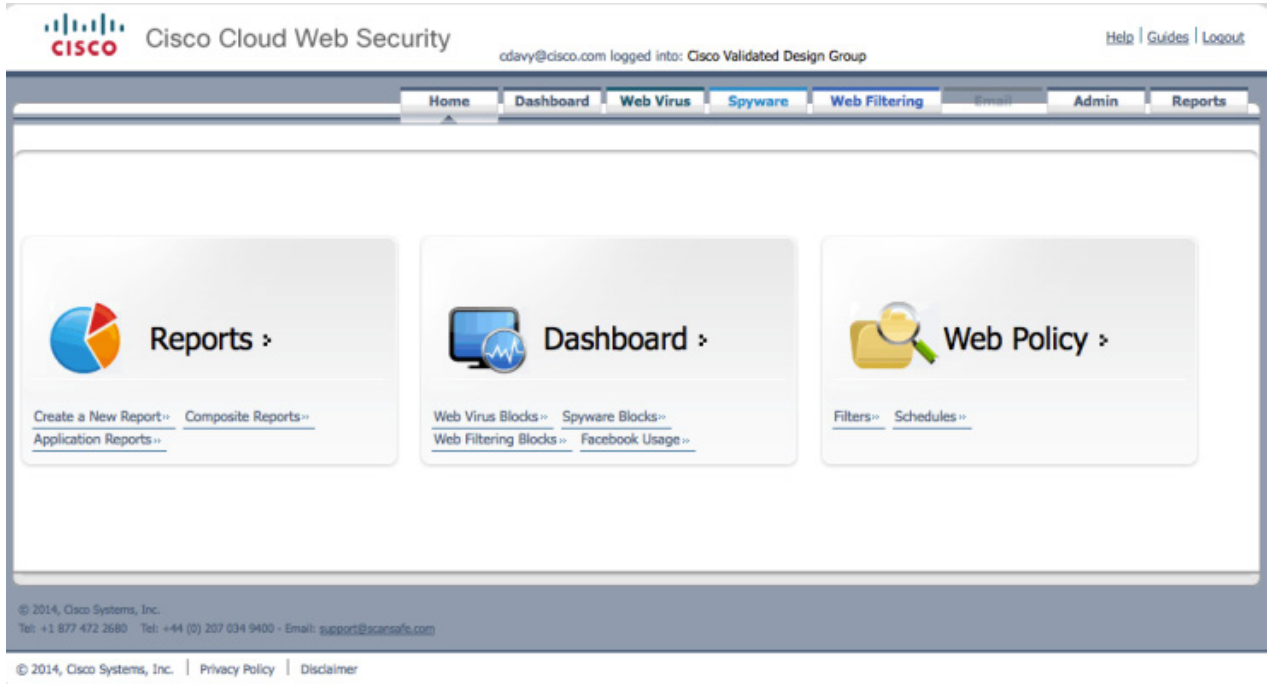
Cisco Cloud Web Security (CWS) 概述



不论用户于何地以何种方式接入互联网，
CWS 均能提供一致的、可执行的高效能的网络安全和策略

云网络安全集中管理

- Cisco ScanCenter Portal

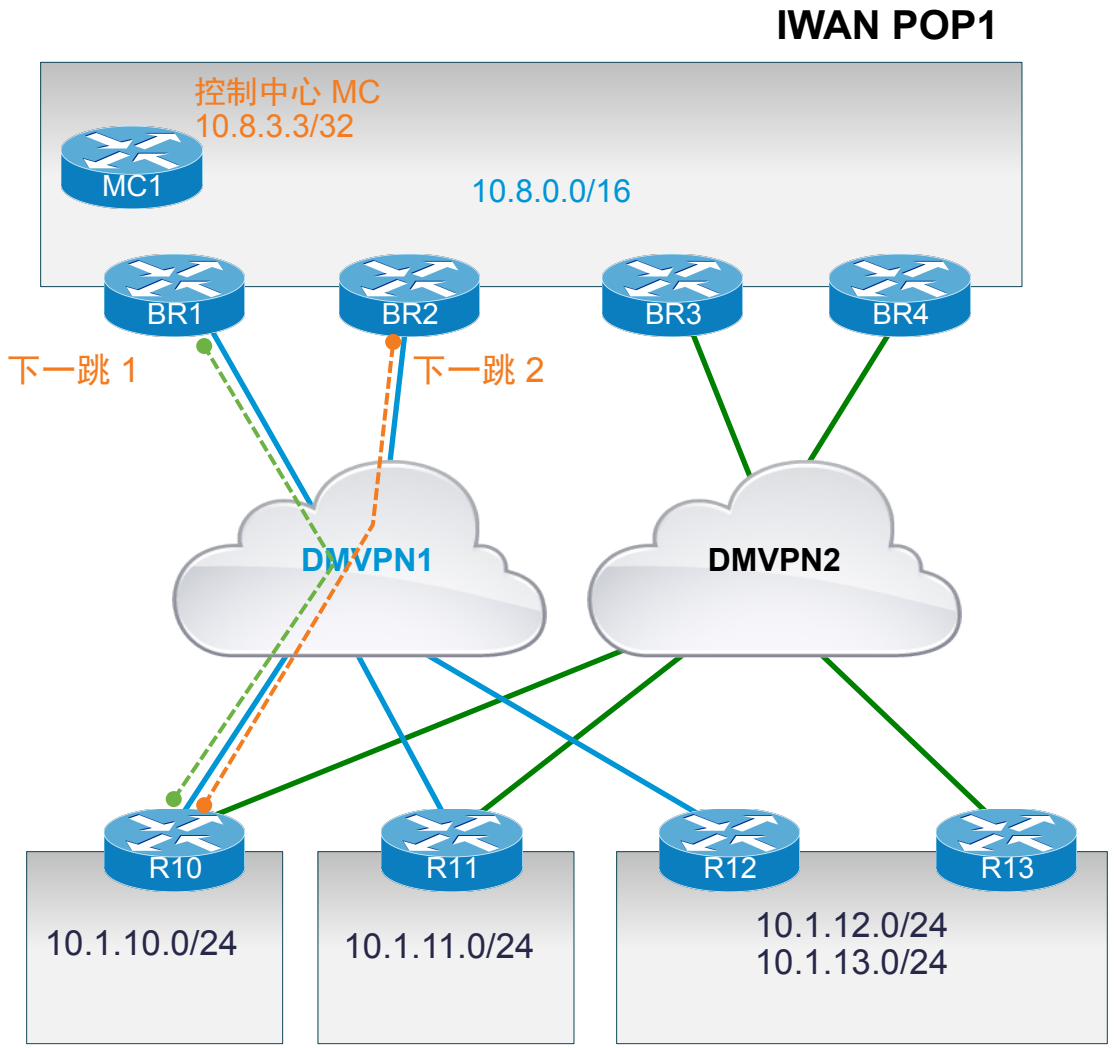


IWAN 2.0 新使用案例

IWAN 2.0 使用案例：水平扩展与冗余

多个 DMVPN 下一跳

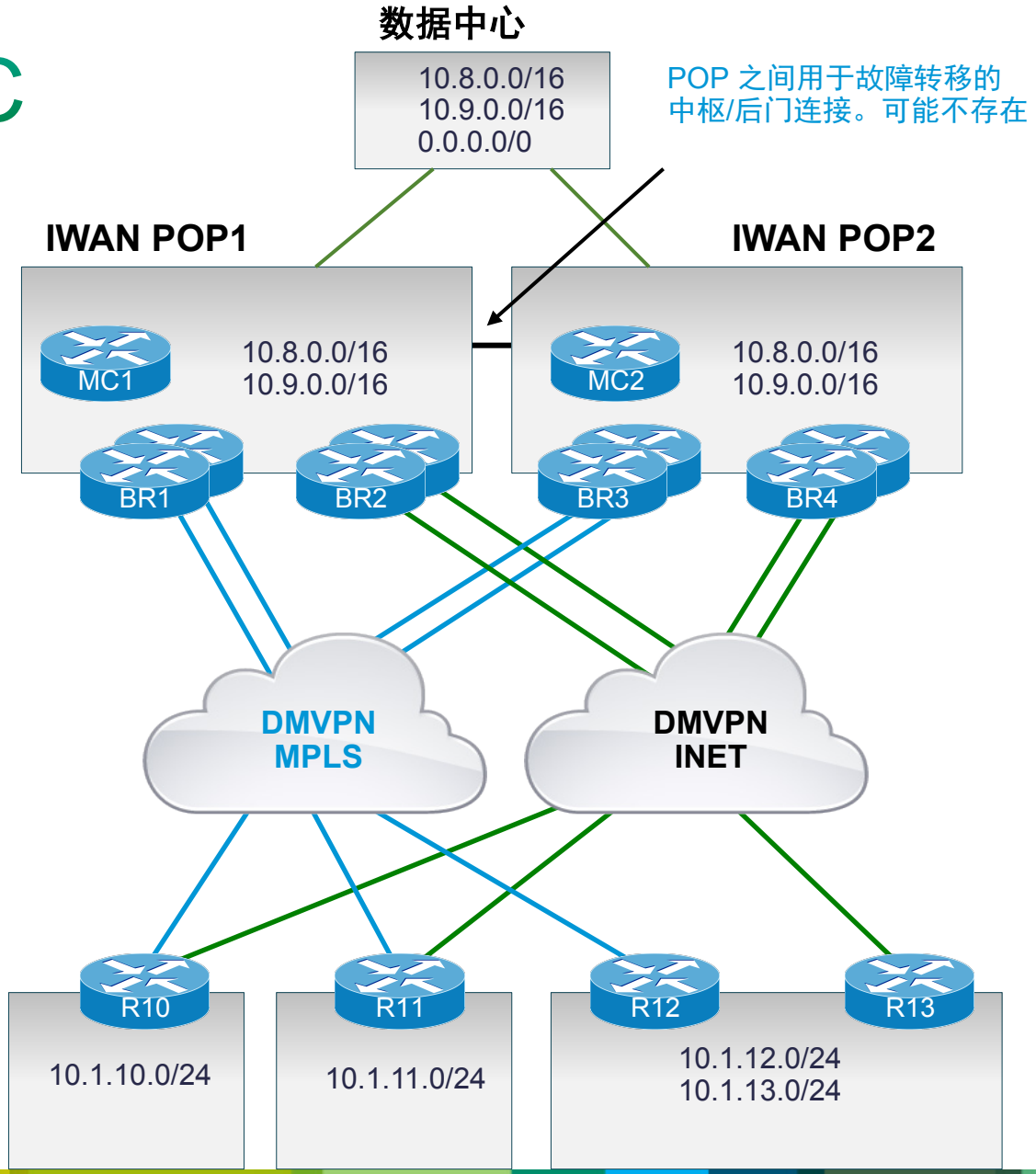
- 每个云有多个 DMVPN 中心用于冗余和扩展
- HA – 如果到远程站点的当前出口出现故障，则切换到同一 (DMVPN1) 网络中的替代出口/信道。
- 此外，切换到替代 (DMVPN1) 网络。
- 规模 – 在一个 (DMVPN) 上跨多个 BR/出口分布流量，以利用所有广域网和路由器容量。
- 只有当一个中心/POP 中的所有出口/信道出现故障或达到最大带宽限制时才会出现跨中心/POP 的融合。
- 针对 Spring XE 3.15 / PI27 发行版



IWAN 2.0 使用案例：Multi-DC

水平扩展，完全冗余

- 2 个（或多个）POP 广告完全相同的一组前缀
- 数据中心可能未与 POP 组合
- 各 POP 的 DC/DMZ 可跨广域网核心获得
- 分支机构可接入跨任一 POP（中心）的任何 DC 或 DMZ。并且，DC/DMZ 可以到达跨多个 POP（中心）的任何分支机构。
- 加密和带宽水平扩展可能要求每个站点的每个 DMVPN 有多个 BR
- 针对 Spring XE 3.15 / PI27 发行版



简化
分支机构部署

思科智能广域网管理

预置管理

Prime 基础设施 2.2

端到端保证应用体验

- **IWAN 的单窗格视图**
- IWAN 部署工作流程
- 即插即用
- DMVPN、QoS、AVC 部署和监控
- 2015 年第 1 季度的 PfR v3
- 许可证包括 IWAN 应用和 APIC-EM 控制器！

专业化管理

LiveAction
Simplifying the Network

应用程序感知网络性能管理

- **与 Cisco AVC 和 PfR 集成**
- 监控和分析应用流量
- 端到端流可视化
- 基于流和应用的故障排除
- 实时修复和验证

基于云的管理

glue™ NETWORKS

自动化部署和生命周期管理

- **消除手动构建广域网**
- 自动化 SD-WAN 协调
- 集中式混合广域网管理
- 快速配置更新和 IOS 升级
- 利用 onePK 和 REST API

IWAN 协调和自动化演进

Prime Infrastructure 即插即用选项

无需 CLI 技能

PnP 1

USB 紧跟引导程序 ISR

- 安装程序连接 LAN/WAN 电缆
- ISR 从 USB 记忆棒加载引导程序配置

PnP 2

Prime 即插即用应用

- 安装程序将 LAN/WAN 电缆和一个 USB 控制台电缆连接到笔记本电脑/iPhone/iPad
- PnP 应用引导路由器

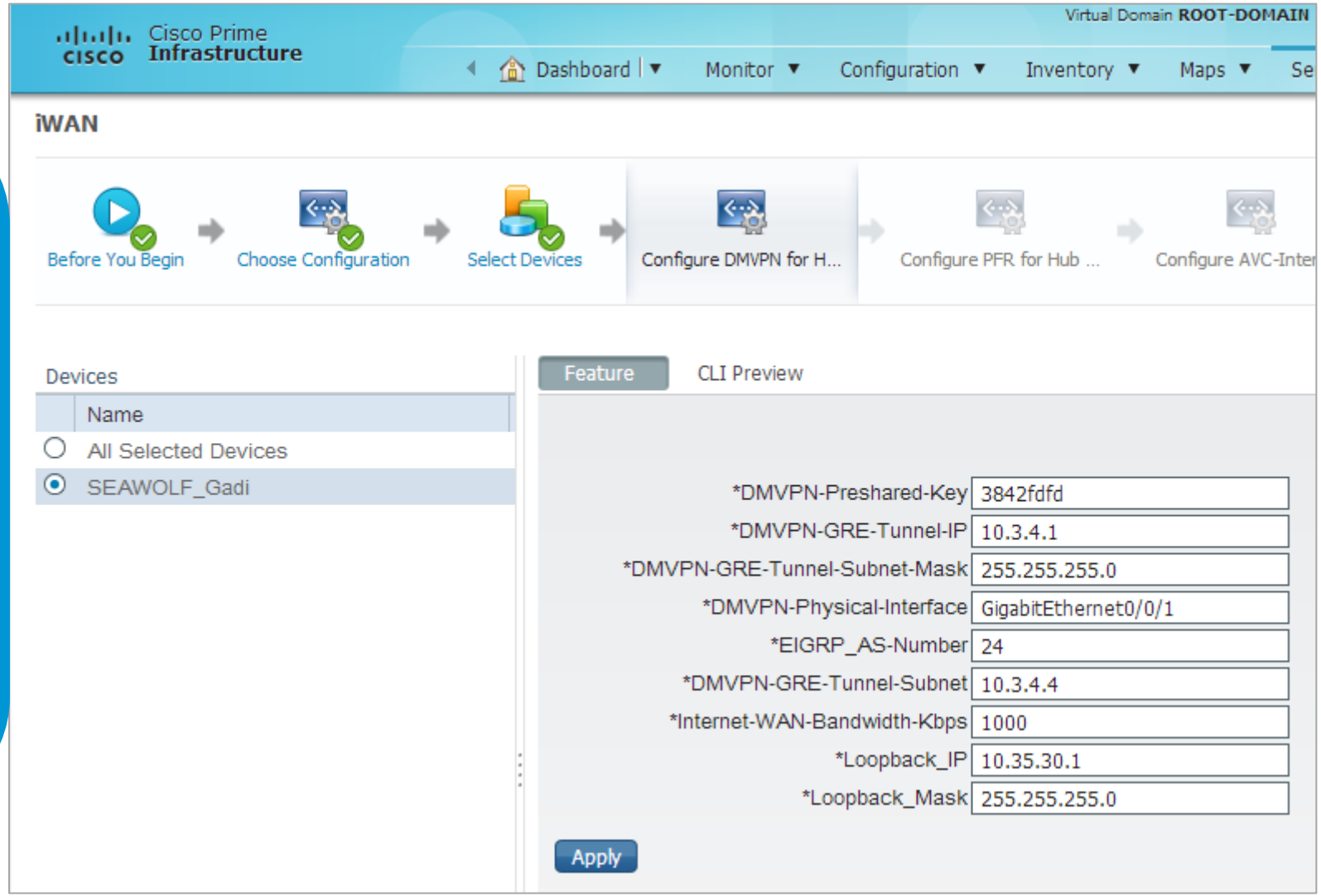
PnP 3

Cisco Configuration Professional Express（ISR 设备 GUI）

- 安装程序将 LAN/WAN 电缆和一台个人电脑连接到一个 LAN 端口
- CCP Express 应用引导路由器

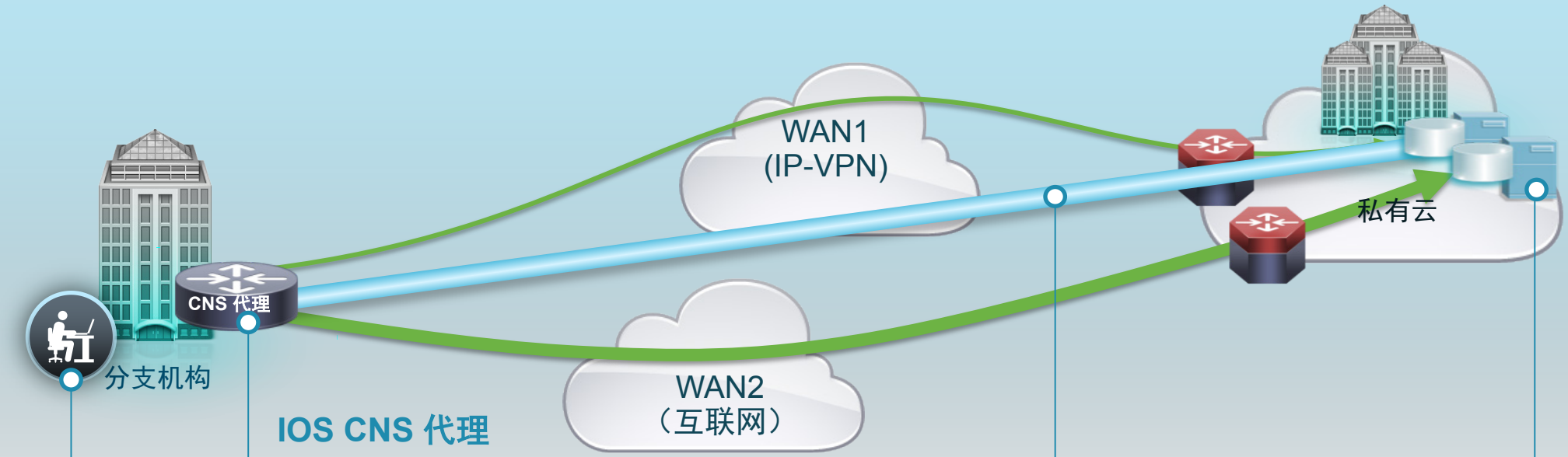
用于 IWAN 的 Prime Infrastructure 2.2

- IWAN 即插即用工作流程向导
- 基于模板的 IWAN 配置
- PfRv3 域、MC 和 BR
- AVC 一键设置
- QoS 调配
- 单路由器分支或双路由器分支
- 基于 CVD，可自定义
- AVC 准备情况评估
- AVC、QoS、PfR* 可视化
- 利用 APIC EM 服务



* PfR 可视化 – 2015 年第 2 季度

IWAN 即插即用与 Prime 应用组件



IOS CNS 代理

使用引导程序配置接入 PnP 服务器

CNS 协议

Cisco PnP 加载 IOS 图像和初始配置的协议

PnP 应用

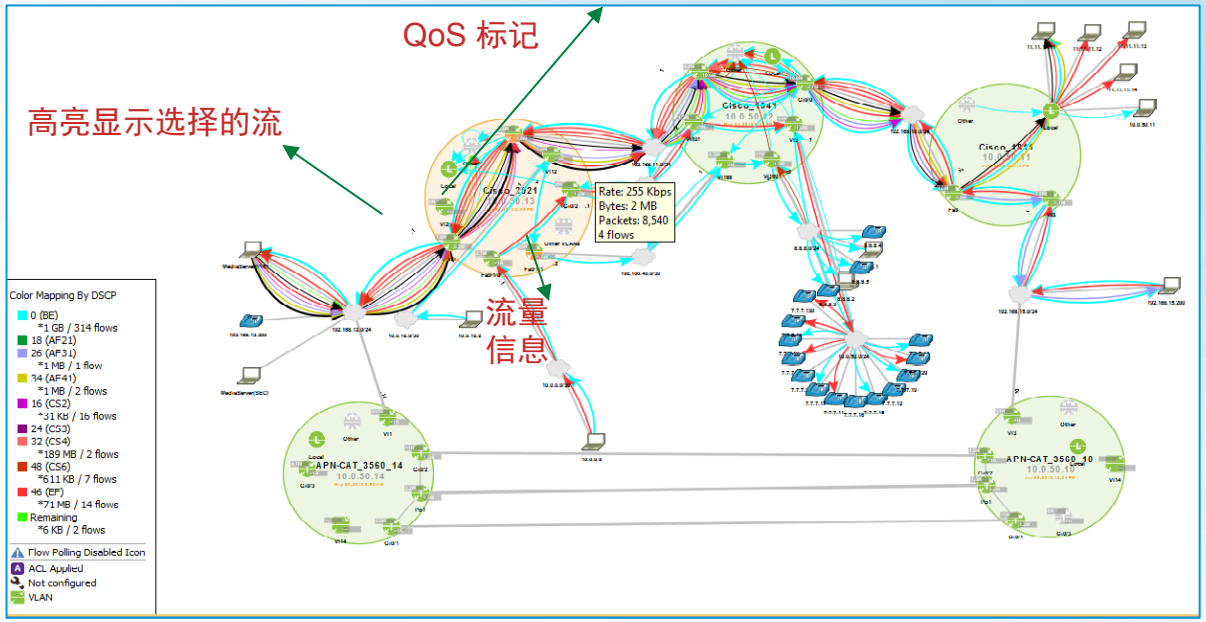
iPhone、iPad 和 Windows PC 的安装应用用于身份验证和启动 IOS 设备

Prime Infrastructure 服务器

管理和分布部署信息（图形、配置和许可证）

LiveAction（之前名为 ActionPacked）
应用感知网络性能管理和 QoS 控制

LiveAction
Simplifying the Network



部署	快速部署/启用： NBAR2、CEF、QoS、AVC、Medianet、IP SLA
分析	已于监控/分析： QoS、NetFlow、PfR、IP SLA、路由、LAN
故障排除	应用性能 广域网：QoS、PfR、路由、IP SLA
解决问题	实时修复和验证 QoS 和应用

端到端流可视化网络态势感知

CISCO Compatible

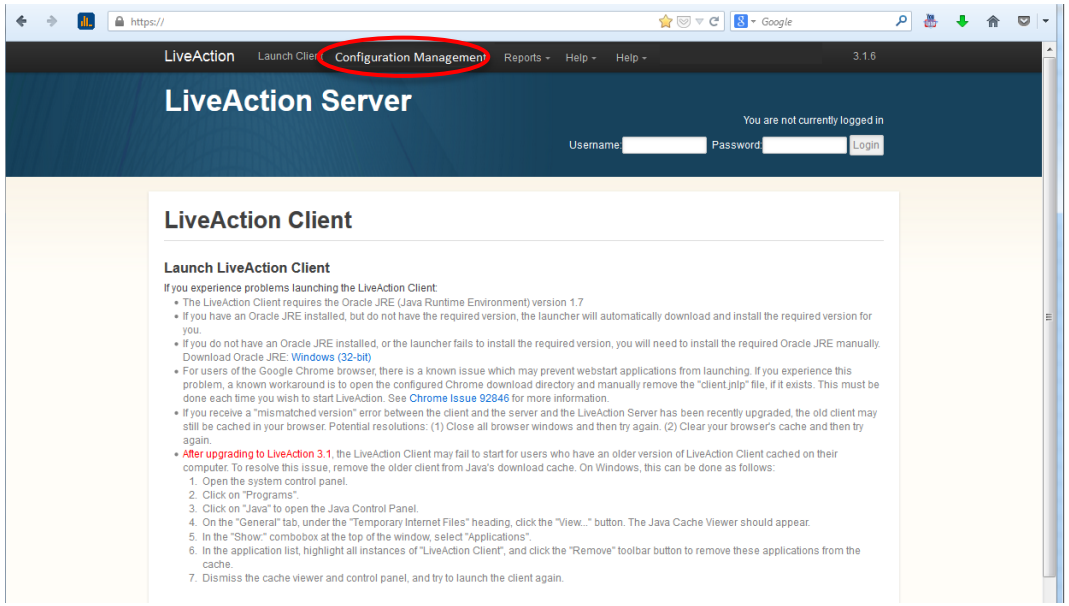
CISCO DEVELOPER Registered

LiveAction PfRv3 管理示例

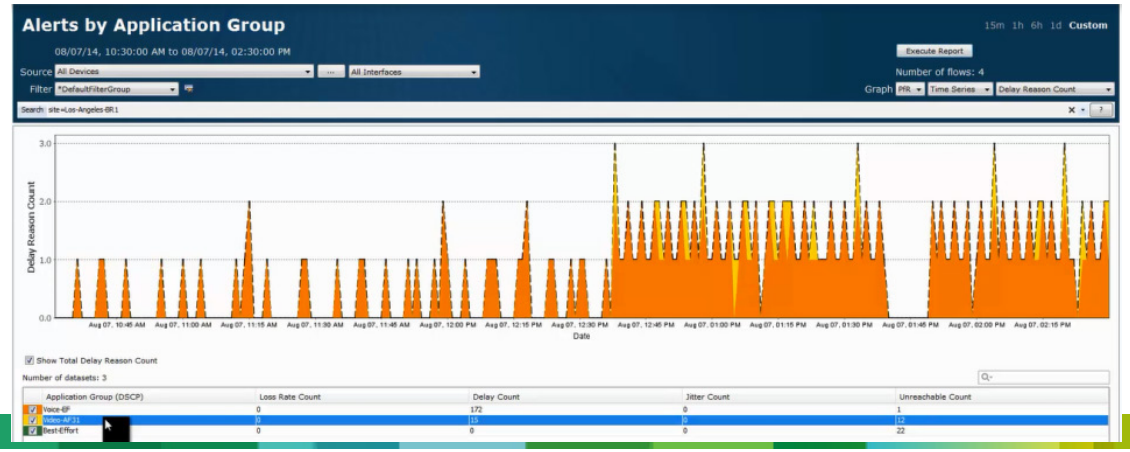
PfRv3 控制面板

搜索

启动配置器



PfRv3 深化



Glue Networks NGWAN/IWAN 协调

gluware™

- 基于云的 SaaS 订阅模式
- 消除手动构建广域网
- 自动化广域网协调和管理
- 快速配置更新和 IOS 升级
- 快速实现下一代和 IWAN 功能
- 为应用感知广域网转发兼容的 SDN 和 OnePK
- 宽带和 MPLS 支持 IWAN 的集中式混合广域网管理

2013 年 第 4 季度发行

CISCO DEVELOPER Solution

CISCO Compatible

构建您的 IWAN

从 Cisco AX 路由器开始

嵌入到路由器中的 IWAN 容量

统一网络

统一服务

简化应用交付

可视性

控制

优化

与传输方式无关的
安全路由

ASR1000-AX

ISR-AX

Cisco AX 路由器 3900 | 2900 | 1900 | 800 | ISR4000-AX | ASR1000-AX

IWAN 分支机构服务路由器

ISR4000 系列 - IWAN AX Ready，下一代分支机构

设备级性能

- 服务感知数据平面
- 弹性服务虚拟化
- 多千兆交换矩阵

以应用为中心

- 应用/用户策略驱动的部署
- APIC_EM 自动化：数分钟内完成部署
- 随增长随投资
- 节约高达 75% 的成本

集成 IWAN 服务

- IOS 防火墙、VPN、IPSec、PfRV3、NBAR2、AVC、AppNav、VRF、MPLS
- 可扩展芯片上服务调配

ISR4451		1-2Gbps
ISR4431		500Mbps/1Gbps
ISR 4351		200/400Mbps
ISR 4331		100/300Mbps
ISR4321		50/100Mbps

IWAN 聚合边界路由器

ASR1000 - IWAN AX Ready，高性能路由器

紧凑、强大的路由器

- 启动服务时，线速性能 2.5G ~ 200G+
- 加密性能 2G ~ 60G+
- 灵活的输入/输出：SPA 和以太网 LC

业务关键恢复能力

- 独立的控制和数据平面
- 硬件和软件冗余
- 在线软件升级

集成 IWAN 服务

- IOS 防火墙、VPN、IPSec、PfRV3、NBAR2、AVC、AppNav、VRF、MPLS
- 可扩展芯片上服务调配

新！

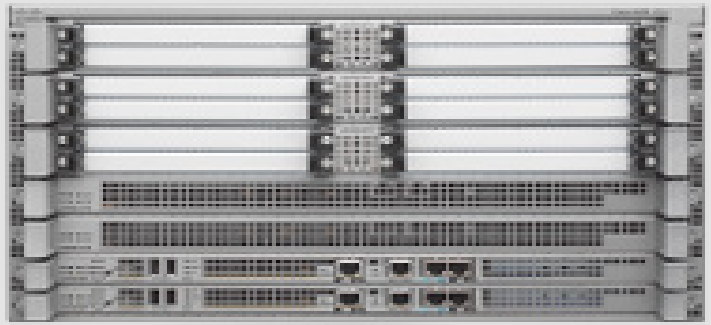
ASR1001-X

- 2.5G 可升级成 5G、10G、20G
- 高达 8G 的加密吞吐量

ASR1002-X

- 5G 可升级成 10G、20G、36G
- 高达 4G 的加密吞吐量

模块化 ASR1006



- 模块化，冗余高达 200G
- 高达 60G 的加密吞吐量

IWAN 路线图概述

新的

	IWAN 1.0 智能虚拟化	IWAN 2.0 自动化 （2014 年第 4 季度）	
域规模	数以百计的分支机构	大规模（2000 个分支机构）	
与传输方式无关	安全 VPN 覆盖 （DMVPN 第 2 阶段）	VPN 可扩展性（DMVPN 第 3 阶段）	
智能路径控制	第 2 代路径控制 – PfRv2	简化的 路径控制 – PfRv3 （集中调配，大规模）	
应用优化	AVC WAAS	自适应 AVC （性能优化） Adv. QoS （自适应整形、本地进入许可） Akamai 连接	
安全连接	IPSec 套件 B 加密 IOS ZBFW 防火墙 云网络安全 (CWS)	密钥管理自动化 （PKI 认证/信任自动化）	
管理	Cisco Prime LiveAction Glue Networks	Prime Infrastructure 2.2： 与传输方式无关的设计 (DMVPN) 应用优化 (AVC), 自动化部署 工作流程向导	APIC-EM EFT： PKI 自动化 逐站点调配 基于 CVD：QoS、AVC、PfR

思科高级服务 IWAN 产品组合

新！

客户情况	您可以销售的服务：
期待探索 IWAN 架构演进	网络架构发现研讨会
想评估当前的分支机构架构，并想制定 IWAN 架构策略	网络架构评估和策略
帮助设计和规划 IWAN 部署策略	网络规划和设计
客户想让思科通过全方位服务管理向 IWAN 解决方案的全部迁移	网络规划、设计和实施服务

为什么选择思科智能广域网？

任意连接，无限体验

- 传输与高度可靠性结合
- 用于业务关键型应用的 SLA
- 用于互联网接入的集中安全策略
- 降低广域网成本，并且不影响性能

谢谢。