光联 SD-WAN 产品使用手册

1. 产品定位和特点

1.1 产品定位

Agile Controller-Campus 是针对 SD-WAN 解决方案场景的管理控制系统，对企业互联业务实现全流程管理，提供了专线业务的自动化部署、智能选路策略配置、VAS 业务管理，企业分支连接公有云，以及即插即用、可视化运维等能力。通过 Agile Controller-Campus 可以实现在多租户网络中独立开展业务开通配置、日常运维等工作。

1.2 产品特点

简单

- 网络部署简单：可实现端到端网络业务自动化部署，支持全系列 CPE 设备（customer premise equipment）即插即用，设备快速上线，无技术门槛。
- 业务开通简单：在 SD-WAN 解决方案中，支持专线隧道快速配置及自动化部署，支持基于应用的智能选路配置，根据关键应用需求，对应用实现差异化网络服务，并对链路质量和应用质量进行检测，根据策略配置优先保障关键应用优质体验。
- 网络运维简单：SD-WAN 控制器能够实时的对全网业务流量，质量，告警和日志等关键信息进行收集并统一呈现，提供友好的网络拓扑和 GIS 地图信息，方便用户对网络运行状况进行全局掌控，及时发现并处理问题。

弹性

- 网络按需扩展：支持超大规模以及跨地域设备接入管理，支持基于应用的智能选路，根据关键应用需求，对应用实现差异化网络服务。
- 管理按需扩展：Agile Controller-Campus 支持多租户，企业网络既可自运维，也可交由 MSP 代维，企业可根据自身能力和业务需求，自由选择网络管理模式。

开放

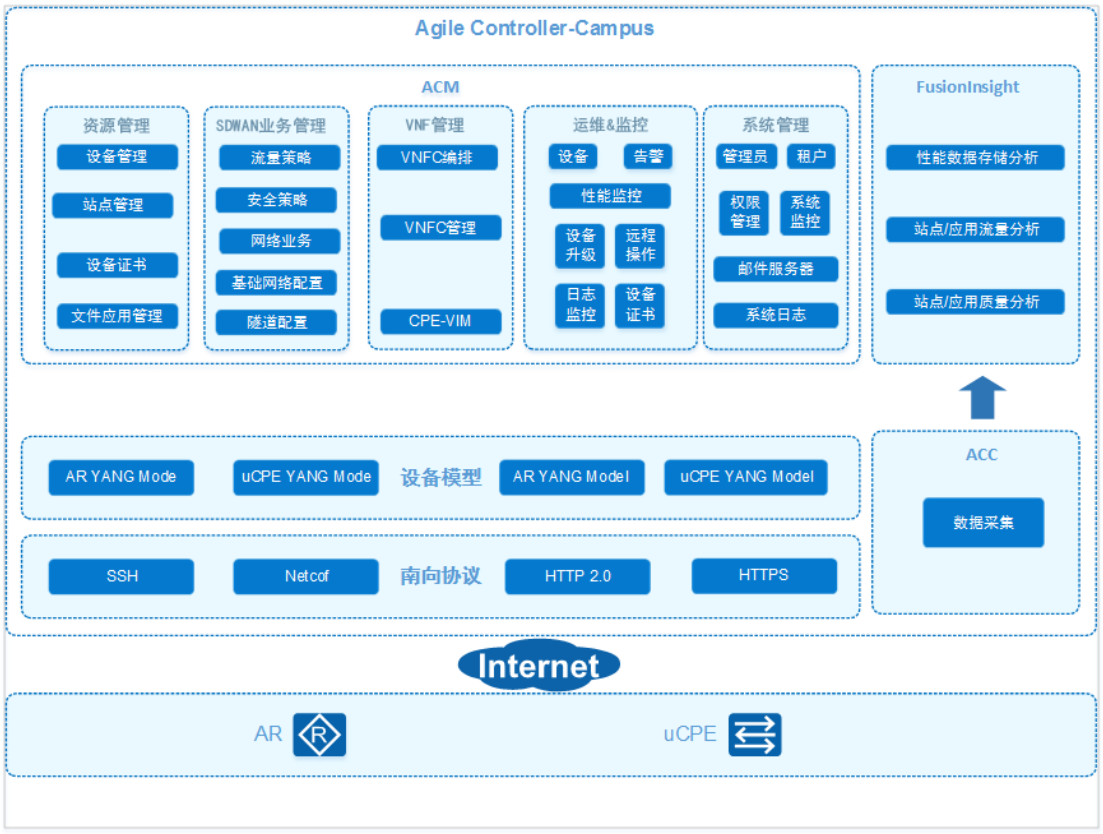
- 第三方 O 层对接：Agile Controller-Campus 提供完整的面向 SD-WAN 业务模型的北向 API，可方便快捷的与第三方协同器进行对接，快速的集成进客户的业务系统。
- uCPE 广泛生态构筑：uCPE 作为按需提供 VAS 服务的平台，覆盖业界主流 VAS 功能，包括安全、语音、广域加速、DHCP、DNS、IPAM、文件共享等。

2. 产品系统与安装组网架构

2.1 Agile Controller-Campus 系统架构

Agile Controller-Campus 是基于华为统一控制器平台架构，支持分布式的大型系统，主要系统架构如图 1 所示。

图 1 Agile Controller-Campus 系统架构图



组件介绍

Agile Controller-Campus 主要包含 ACM、ACC 两个组件，这两个组件都支持集群部署。

ACM

ACM（Agile Controller Manager）是 Agile Controller-Campus 的管理系统，面向系统管理员、MSP 管理员和租户管理员。支持设备管理、用户管理、网络业务管理、网络安全策略、网络监控、系统租户管理、日志管理等特性。

ACC

ACC（Agile Controller Collector）是 Agile Controller-Campus 的数据采集系统，支持采集设备的告警和性能数据，提供给大数据平台作存储分析。

FusionInsight

FusionInsight 是 Agile Controller-Campus 的大数据分析系统，主要对从设备采集的数据进行分析、业务可视化、运维监控等。

FusionCompute

FusionCompute 是云操作系统软件，主要负责硬件资源的虚拟化，以及对虚拟资源、业务资源、用户资源的集中管理。它采用虚拟计算、虚拟存储、虚拟网络等技术，完成计算资源、存储资源、网络资源的虚拟化。同时通过统一的接口，对这些虚拟资源进行集中调度和管理，从而降低业务的运行成本，保证系统的安全性和可靠性，协助运营商和企业构筑安全、绿色、节能的云数据中心能力。

服务器

华为服务器是华为公司针对互联网、IDC（Internet Data Center）、云计算、企业市场以及电信业务应用等需求，推出的具有广泛用途的机架服务器。

华为服务器适用于 IT 核心业务、云计算、虚拟化、高性能计算、分布式存储、大数据处理、企业或电信业务应用及其它复杂工作负载。

华为服务器具有低能耗、扩展能力强、高可靠、易管理、易部署等优点。

2.2 Agile Controller-Campus 安装组网架构

SD-WAN 解决方案

最小集群

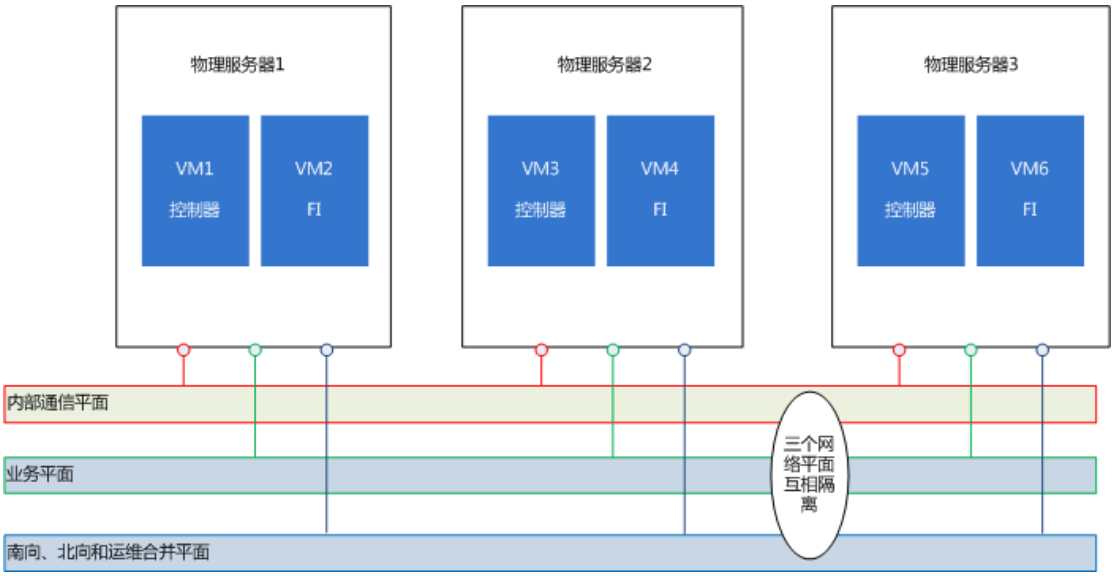
最小集群部署情况下，控制器集群组件、FI 各自占用一个 VM，都是最小集群部署。

使用虚拟机时，Agile Controller-Campus 支持两网络平面、三网络平面和四网络平面三种网络平面划分的方案。

可划分的网络平面如下：

- 内部通信平面：用于 Agile Controller-Campus 各业务节点之间的通信，以及节点与 FusionInsight、数据库的通信。
- 业务平面：用于 Agile Controller-Campus 的南北向业务发放，例如通过 LVS 将业务分发到多个 ACM。
- 北向和运维平面：用于 Agile Controller-Campus 的北向业务接收，例如通过 Web 访问 Agile Controller-Campus 的管理面。
- 南向平面：用于 Agile Controller-Campus 的南向业务接收，例如通过 Netconf 协议与设备通信。

图 1 三平面组网图



通过虚拟机部署 Agile Controller-Campus 集群时，典型部署场景为 Agile Controller-Campus 整体部署在三台物理服务器上。

如图 1 所示，Agile Controller-Campus 连接到了三个网络平面：内部通信平面、业务平面及南向、北向和运维合并平面。

3. SD-WAN 解决方案概述

3.1 方案背景

传统企业通常将应用（E-mail、文件共享、Web 应用等）部署在总部数据中心，并通过租用运营商 MPLS 专线，将分支机构连接到数据中心。运营商承诺专线业务的 SLA（Service-Level Agreement），满足企业在各分支机构部署各种应用的需求。

但是，传统 MPLS 专线网络存在租用费用昂贵、开局周期长、新增业务部署复杂耗时长等问题，无法满足快速开通、灵活部署的企业网络需求。另外，由于云计算的引入，更多企

业将应用部署向云端迁移，使得分支出口流量急剧增加，进一步加剧企业的 WAN 网络成本。

企业尝试通过 Internet 将分支机构和总部进行连接，企业租用 Internet 链路（xPON、xDSL、LTE/3G 等）的成本，通常是 MPLS 专线成本的 1/3 到 1/2，并且业务发放周期短，租用灵活。但该方案需要在分支部署复杂的 CPE 设备，维护难度较大，这一问题对多分支网点的企业（例如银行、零售连锁）更为突出。

为了应对上述问题，华为推出了 SD-WAN（Software Defined WAN）解决方案。通过在 WAN 网络中部署 Agile Controller-Campus 控制器，集中管理 CPE 设备、零配置开局，缩短业务开通时间，从而帮助企业应对云服务带来的挑战，做到业务随需而变。

3.2 方案架构

华为 SD-WAN 解决方案致力于解决企业传统专线带来的成本高、响应慢和运维难的问题，提供高性价比、随需而变、云端可视化运维的企业专线业务，重塑企业专线全流程的业务体验。它包括基础架构层、SD-WAN 控制器层和上层应用层。

华为 SD-WAN 解决方案架构分为 3 个部分。

- 基础架构层

  通过 EVPN 隧道技术构建 Overlay 网络。每个 CPE 支持一个或多个 WAN 连接，企业分支侧 CPE 通过 MPLS 链路，实现分支与总部的高效互联。

- SD-WAN 控制器

作为 SD-WAN 最核心的部分，实现 CPE/uCPE 设备的统一管理，业务自动下发和 Overlay 网络的统一控制。南向通过 HTTP2.0 通道以及 NETCONF 协议管理 CPE 设备，北向开放 RESTful 接口以 SD-WAN Portal 形式与上层应用层实现互联对接。

- 上层应用层

  主要包括运营商 OSS/BSS、第三方 Portal、第三方 App Store、第三方 Orchestration，通过 Agile Controller-Campus 提供的 Open API 机制，实现与 Agile Controller-Campus 的互联对接。只有和 Agile Controller-Campus 对接的应用发送的对接消息符合 Open API 接口定义，才可以成功对接，对于发送的消息不符合 Open API 接口定义的应用，需要定制 Open API 接口才可以实现对接。

3.3 方案价值

华为 SD-WAN 解决方案可以给用户带来显著的价值。

- 灵活安全的 WAN 接入，支持多种不同广域链路，节约网络租用成本

  支持 MPLS 链路与 Internet 链路灵活组合的混合接入方式，在保证关键业务质量的同时可节约 WAN 带宽租用成本。

- 即插即用开局，4 个步骤 1 小时内完成业务开通

  1. 控制器发送邮件给站点的开局人员。
  2. 站点开局人员通过邮件开局。
  3. CPE 设备自动注册到 Agile Controller-Campus 请求业务下发。

4. 由 Agile Controller-Campus 自动完成业务部署。

- 业务可控可视，降低运维成本

  采用业务感知 SA（Service Awareness）技术实现 6000+应用识别。采用 TCP FPM（TCP Flow Performance Monitor）、IP FPM（IP Flow Performance Monitor）技术实现基于应用的质量检测。采用 IP FPM 技术实现链路的质量检测。采用智能策略路由 SPR（Smart Policy Routing）技术实现基于应用质量进行智能的链路切换。

- 高效连接公有云

  越来越多的企业 IT 资产正在迁移或即将迁移到各种公有云上，为了保证企业业务的完整性，华为 SD-WAN 能够高效地连接公有云，实现云接入的自动化和良好体验。

- 完整的安全防御体系，业务安全无忧

  CPE 设备采用多核设计，拥有高性能 CPU，具有丰富的身份认证方式，提供强大安全的接入能力。支持 IPSec、MPLS 多种 VPN 技术提供端到端防护，支持防火墙功能，提供硬件、管道、应用多层级全方位安全保障。

- 开放平台架构，灵活扩展所需增值业务

  CPE 设备基于 NFV（Network Function Virtualization）架构提供 vWoC（virtualised WAN Optimization Controller）、vFW（virtualised Firewall）

等多种增值业务 VAS（value-added service），支持 VAS 自动加载，集中运维管理。CPE 设备提供开放接口，支持第三方 VAS 扩展。

控制器支持 uCPE 的 Open API，实现 uCPE 的 VNF（virtualized network function）生命周期管理。

- 转控分离的架构

  在新的 EVPN 隧道方案中，控制面和转发面的分离，通过部署独立的控制组件，实现对网络路由和拓扑的灵活控制，有效提升了网络可扩展性，可支持大规模的企业组网和复杂的网络拓扑。

3.4 典型应用

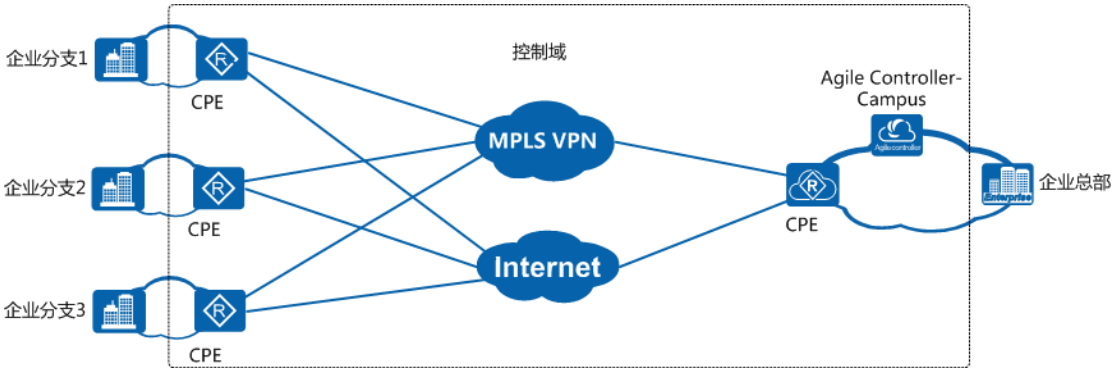
华为 SD-WAN 解决方案提供两种组网方案。

- 企业自建 SD-WAN 互联方案，此方案适用于大企业自建的轻量级 SD-WAN 网络场景。
- 运营商转售 SD-WAN 多租户方案，此方案适用于管理服务提供商 MSP（Managed Service Provider）和传统电信运营商的多租户场景。

企业自建 SD-WAN 互联

如图 1 所示，像金融、零售连锁、加油站这类具有大量分支的大型企业，可以在企业总部部署自己的 Agile Controller-Campus，组建企业自己的 SD-WAN 网络，自助管理企业的 SD-WAN 业务。

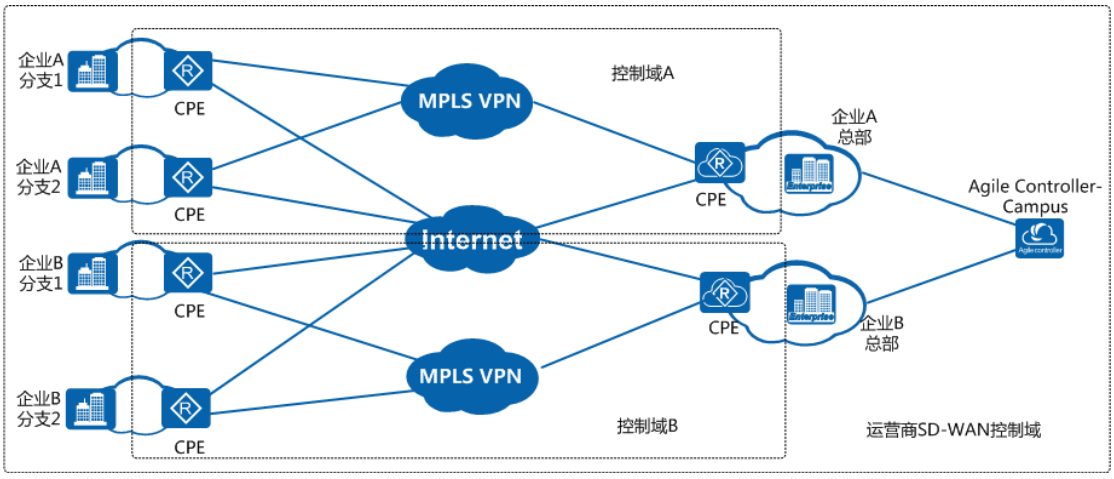
图 1 企业自建 SD-WAN 组网图



运营商转售 SD-WAN 多租户

运营商提供统一的 Agile Controller-Campus 为多个企业提供 SD-WAN 服务。企业可以作为租户，租用运营商提供的 SD-WAN 服务，企业租户可以管控本企业范围内所有站点的 SD-WAN 业务，但是无法看到其他租户的 SD-WAN 业务。如图 2 所示，企业 A 租户仅可以对控制域 A 范围内的 SD-WAN 业务进行管控，企业 B 租户仅可以对控制域 B 范围内的 SD-WAN 业务进行管控，企业 A 和企业 B 相互之间不可见，企业可以通过运营商分配的租户权限对自己的企业网络的 SD-WAN 业务进行管控，也可以托管给运营商，由运营商对企业网络的 SD-WAN 业务进行管控。

图 2 运营商转售 SD-WAN 多租户组网图



4. 功能特性

4.1 设备即插即用

设备的即插即用，URL 即插即用解决方案，也可以叫做邮件开局解决方案，邮件开局是指在使用控制器进行网络管理的场景下，网络管理员在控制器客户端，通过指定开局邮件中的 URL 链接参数完成开局信息配置，并将开局邮件发送到开局邮箱，开局人员在收到开局邮件后，通过浏览器访问邮件中的 URL 链接启动开局流程，设备自动完成开局部署的一种开局方式。

在站点现场开局，通过此功能可以大幅简化站点开局人员的操作流程。

4.2 网络业务配置

4.2.1 网络互通的基本配置

Agile Controller-Campus 针对 AR 设备主要支持如下配置：

- 接入路由器的网络业务配置：
    - 支持 NTP、IPSec 等基础配置。

- 站点互联配置：支持 BGP 路由配置。
- 无线网络配置：支持 SSID、射频配置。
- 有线网络配置：支持以太接口、接口 VLAN 配置。
- IP 业务配置：支持 DHCP 配置、DNS 配置、静态路由配置。
- 路由协议配置：静态路由配置、OSPF 路由配置、BGP 路由配置。

4.2.2 选路策略配置

选路策略配置主要包含以下部分：

- 流量分类配置

  流量分类配置支持基于源 IP、目的 IP、协议、源端口、目的端口、DSCP 标志、应用配置，当前是基于模板方式配置。

- 切换条件配置

  切换条件包括：时延，抖动和丢包三个指标，其中一个指标不满足就会进行切换。支持按流量带宽进行选路控制，可保证高优先级应用不受低优先级应用的影响。

- 主备路径配置

  主备路径基于 transport network 进行选择，主备路径分别可以同时选择多个 transport network，可配置链路的优先级。当主路径存在多个 transport network 时，所有 transport network 对应的物理链路上承载的 overlay 隧道链路质量都满足要求的情况下，优先从高优先级链路选择，当高优先级链路不满足要

求时，自动切换到低优先级链路，当所有主链路不满足要求，则切换到备份链路进行选择。

- 选路高级配置

  应用支持按 WAN 链路带宽负载情况进行选路控制，可保证高优先级应用不受低优先级应用的影响。

4.2.3 Site to Site

控制器支持编排站点与站点间的 VPN。

提供 Hub-Spoke，Full-Mesh 以及 Partial Fullmesh 的组网互通方式。

在 Hub-Spoke 网络中，总部与分支间建立 Hub-Spoke 隧道，分支到分支的数据流经由总部传输。

在 Full-Mesh 网络中，分支与分支机构间可以动态地建立 Spoke-Spoke 隧道，实现分支结构与分支机构之间的直接通信。

在 Partial Fullmesh 网络中，企业的大部分站点之间直接互通，也可实现部分站点之间互联绕行其他站点的场景。

4.2.4 Site to Internet

SD-WAN 解决方案站点上网业务主要支持以下场景配置：

- 本地上网：站点的上网流量从本地 CPE 直接出局上网；

- 集中上网：所有站点的上网流量都通过 overlay 的 EVPN 隧道发送到集中上网的站点后出局上网；
- 混合上网：
    - 集中上网+指定流量本地上网：默认上网流量通过集中上网站点出局，部分指定业务流量通过本地 WAN 侧链路直接上网，比如 Office365 流量；
    - 全部流量本地上网+集中上网：默认所有上网流量从本地出局，当本地上网接口故障，上网流量绕行到集中网关出局。

4.2.5 Site to Legacy

SD-WAN 解决方案站点与传统站点互访支持配置以下场景：

- 本地互访：站点与传统站点互访流量从本地直接出局；
- 集中互访：所有 SD-WAN 站点访问传统站点的互访流量都集中到一个 SD-WAN 站点统一出局。

4.2.6 Qos

QOS 策略配置主要包含以下部分：

- 流量分类配置

  流量分类配置支持基于源 IP，目的 IP，协议，源端口，目的端口，DSCP 标志，应用，当前是基于模板方式配置。

- 支持设置策略优先级

CPE 根据策略优先级确定生效优先级。优先级值越大级别越低。

- 支持配置队列优先级，级别包含低、中、高。保证带宽可以设置为具体的值也可以设置百分比。
- 支持配置流量带宽限制，可以设置为具体的值也可以设置百分比。

4.2.7 ACL

Overlay ACL 策略

Agile Controller-Campus 支持 ACL 阻断策略

- 增加、删除、修改和查看 ACL 策略
- 支持克隆一条 ACL 策略
- ACL 策略支持使能去使能
- ACL 策略绑定流分类模板
- ACL 策略指定时间生效模板
- ACL 策略支持绑定到站点
- ACL 策略支持站点视图查看站点绑定策略情况
- 支持 ACL 策略提交到设备
- 提交 ACL 策略支持设置预约下发时间
- ACL 策略支持设置策略优先级，队列优先级及限制带宽

Underlay ACL 策略

Agile Controller-Campus 支持 ACL 阻断策略

- 增加、删除、修改和查看 ACL 策略
- 支持克隆一条 ACL 策略
- ACL 策略支持使能去使能
- ACL 策略绑定流分类模板
- ACL 策略指定时间生效模板
- ACL 策略支持绑定到站点
- ACL 策略支持站点视图查看站点绑定策略情况
- 支持 ACL 策略提交到设备
- 提交 ACL 策略支持设置预约下发时间
- ACL 策略支持设置策略优先级
- ACL 支持根据 WAN 接口下发阻断策略

4.2.8 安全策略

URL

Agile Controller-Campus 支持配置 URL 过滤策略并下发到 CPE 设备，通过对用户访问的统一资源定位符 URL（Uniform Resource Locator）进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的。Agile Controller-Campus 已经预先对大量常见的 URL 进行了分类。管理员可以根据系统预置的这些分类控制企业用户禁止或允许访问哪些类别的 URL，同时对这些预定义的 URL 指定控制动作级别。

防火墙

防火墙（Firewall）是一种隔离技术，使内网和外网分开，可以防止外部网络用户以非法手段通过外部网络进入内部网络，保护内网免受外部非法用户的侵入。防火墙策略只在选中站点的域间生效，例如在 trust 域与 untrust 域之间生效。

IPS

入侵防御系统 IPS（Intrusion Prevention System）是一种安全机制，通过分析网络流量可以检测出入侵行为（包括缓冲区溢出攻击、木马、蠕虫等），并通过一定的响应方式对其进行实时中止，从而保护企业信息系统和网络架构免受侵害。

4.3 网络业务监控

4.3.1 SD-WAN 业务监控

SD-WAN 业务支持对站点、站点间的性能数据进行分析，支持对全网的应用进行分析。

- 站点性能分析
    - 全网站点概述
        - 全网站点健康分布情况
        - 全网站点列表数据
    - 站点概览
        - 站点 TOPO 信息
        - 站点访问量趋势
        - 站点 AQM 趋势

        - 站点上、下行带宽利用率趋势
        - 站点 TopN 吞吐量趋势
        - 站点各个链路的上、下行应用流量趋势
        - 站点应用 AQM 最差排行
    - 站点链路
        - 站点链路的吞吐量趋势
        - 站点链路的上、下行带宽利用率趋势
        - 站点链路的质量趋势(时延，抖动，丢包率，LQM)
    - 站点应用
        - 站点应用的质量趋势(时延，抖动，丢包率，AQM)
        - 站点应用的吞吐量趋势
- 站点间性能分析
    - 全网站点间概述
        - 站点间流量排行
        - 站点间 LQM 最差排行
        - 站点间列表
    - 站点间概览
        - 站点间 TOPO 信息
        - 站点间 LQM 趋势
        - 站点间吞吐量趋势
        - 站点间应用流量排行
        - 站点间应用 AQM 分布

        - 站点间应用流量 TopN 趋势
    - 站点间链路
        - 站点间链路的吞吐量趋势
        - 站点间链路的上、下行带宽利用率趋势
        - 站点间链路的质量趋势(时延，抖动，丢包，LQM)
    - 站点间应用
        - 站点间应用列表
        - 站点间单个应用吞吐量趋势
        - 站点间单个应用 AQM 趋势及所在链路 LQM 趋势
        - 站点间单个应用时延、丢包率趋势及所在链路时延、抖动、丢包率趋势
- 全网应用分析
    - 全网应用维度
        - 全网应用的 AQM 分布
        - 全网应用的 AQM 最差排行
        - 全网应用的吞吐量趋势
        - 全网应用的流量 TopN 排行
        - 全网应用列表
    - 单应用维度
        - 单个应用的吞吐量趋势
        - 单个应用的质量趋势(时延，抖动，丢包率，AQM)
        - 单个应用的访客列表

4.3.2 业务告警

- 设备离线告警
- CPU 使用率超过阈值
- CPU 使用率超过严重阈值
- 内存使用率超过阈值
- 内存使用率超过严重阈值
- 设备流量超过阈值
- 设备流量超过严重阈值
- 剩余磁盘不足
- 剩余磁盘严重不足

4.4 网络业务规划

4.4.1 站点规划

Agile Controller-Campus 支持站点管理：

- 增加、删除、修改站点
- 增加、删除、修改 VPN
- VPN 绑定站点和解绑站点

4.4.2 设备管理

Agile Controller-Campus 支持设备管理：

- 增加、删除、修改和查看设备，支持批量导入的方式增加设备
- 增加、删除、修改和查看设备组
- 增加、删除、修改和查看组织，最大支持 5 级组织

4.4.3 应用管理

Agile Controller-Campus 支持应用管理：

- 增加、删除、修改和查看应用组
- 增加、删除、修改和查看自定义应用
- 设备应用组的管理和升级策略

4.5 网络业务维护

4.5.1 文件管理

Agile Controller-Campus 支持文件管理：

- 支持用户通过上传工具进行文件上传功能。
- 支持查询和删除已上传文件。

4.5.2 日志管理

Agile Controller-Campus 支持日志管理：

- 支持查询和展示设备上下线日志，包括设备配置通道、准入通道、性能采集通道的上下线日志。

- 支持配置设备的日志上传策略和第三方日志服务器地址，设备将指定类型日志上传至日志服务器。该特性仅部分 AR 款型支持。

4.5.3 设备维护

- 支持设备升级

  SD-WAN 解决方案支持对设备进行升级，支持按照站点维度配置软件下载时间、设备重启时间与升级路径。

- 支持设备证书管理

  SD-WAN 解决方案支持设备证书的筛选、查看、导出以及向设备提交新证书。

4.6 系统管理

4.6.1 系统管理员

Agile Controller-Campus 中的所有帐号统称为管理员，不同角色的管理员具有不同的权限，其中系统管理员负责对 Agile Controller-Campus 系统的管理和维护。

Agile Controller-Campus 系统默认提供一个系统管理员帐号，该帐号在安装 SD-WAN 控制器时设定，不能删除。控制器系统中可创建多个系统管理员，并给不同的管理员定义不同的角色，从而赋予不同管理员不同的管理对象和操作权限。系统管理员支持：

- 管理系统管理员帐号
- 角色管理，支持自定义角色
- 修改当前帐号密码

- 查看在线用户
- 设置闲置超时时间
- 管理租户，包括创建、删除和修改租户信息
- 配置帐号策略
- 配置密码策略

4.6.2 日志管理

Agile Controller-Campus 提供查看管理员登录安全日志、操作日志及系统运行日志，方便审计和异常处理。

4.6.3 服务器管理

Agile Controller-Campus 支持服务器管理：

- 支持邮件服务器配置
- 支持 SA 服务器配置
- 支持日志服务器配置

4.7 告警管理

告警管理通过提供过滤、查询等功能以及各种可定制的规则，帮助用户快速定位想要关注的告警，从而高效处理这些告警。

告警管理可以实现以下功能：

- 告警查询和监控：支持按不同条件组合过滤、查询、统计和展示告警。

- 告警远程通知：通过邮件方式将上报的告警发送给网络维护人员，方便其及时了解告警信息进而采取相应措施。