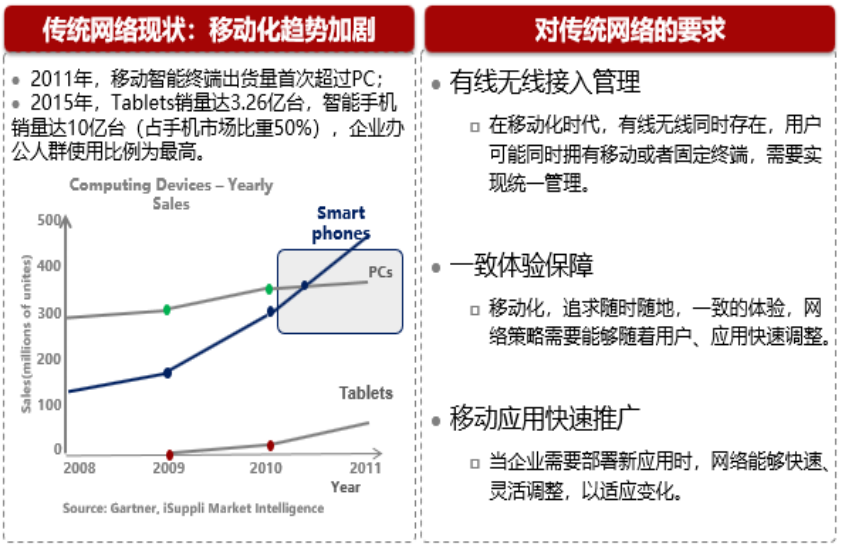
Agile Controller 产品特性介绍

前言

- 随着网络新技术快速发展，用户对采用任意终端设备，随时随地接入网络有了强烈诉求，但是传统企业园区网络是以IP为中心的网络，不同的办公地点规划不同的IP地址段，并且根据IP地址范围定义网络的控制策略，限制用户的网络接入权限。用户要随时随地接入网络，会面临严峻挑战。
- 因此，华为公司推出了Agile Controller产品，Agile Controller可以形象的比喻成智慧的园区大脑，在SDN集中化控制思想的指导下，动态调配整个园区的网络与安全资源，让网络更敏捷地为业务服务，解决用户的诉求。

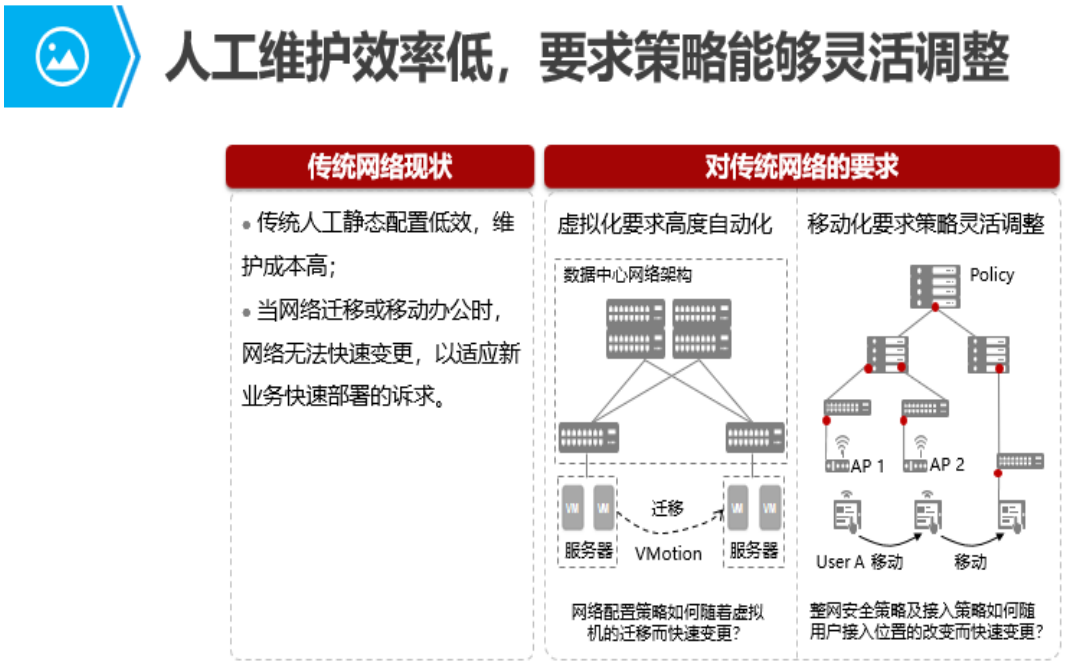
移动化趋势加剧，要求一致的业务体验



- 传统网络的现状：
- 随着移动化趋势加剧，用户在不同的位置接入，会获得不同的 IP 地址。使用基于 IP 地址做网络接入权限的策略控制，

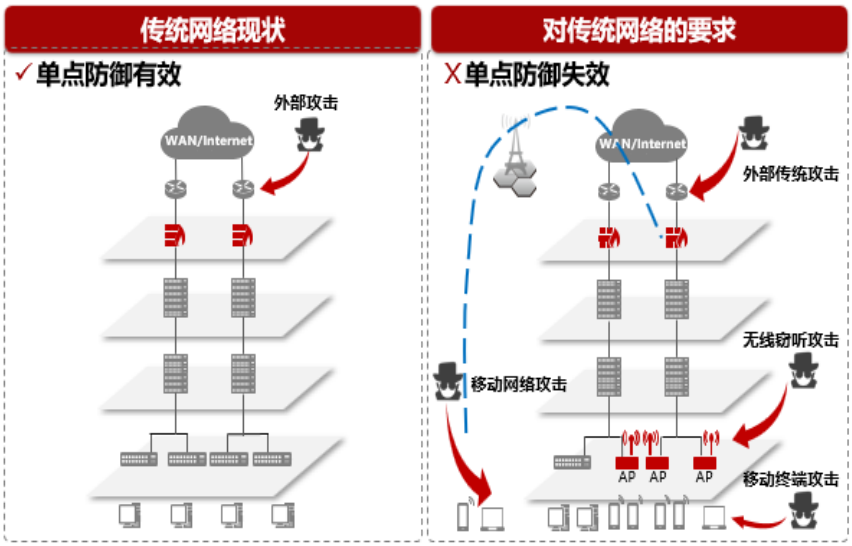
为终端用户提供一致的接入体验非常困难。

- 对传统网络的要求：
- 提供基于用户的统一控制，解决移动用户访问权限的问题，实现“策略随行、资源随动、体验随身”的要求。



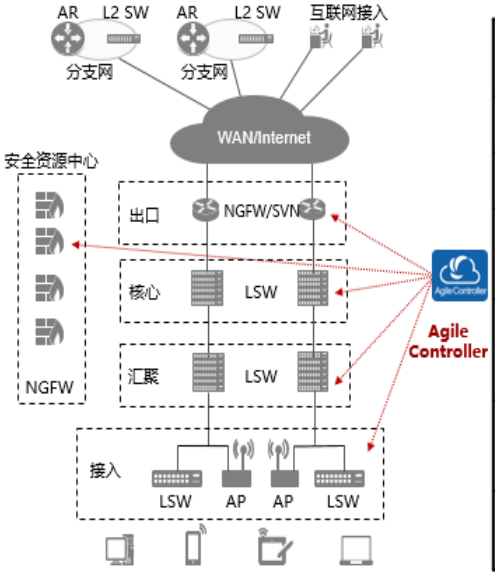
- 传统网络的现状：
- 传统情况下，企业会针对不同的用户做一些网络控制策略，这些策略都是 IT 人员手工或者利用网管系统在网络设备上静态配置的，当发生大量的用户移动时，需要对策略手工进行调整，方法低效，实施难度大，而且容易导致网络配置错误，耗费了 IT 维护人员的大量工作量；
- 当开通新业务时，网络无法快速变更，无法适应新业务快速部署的诉求。
- 对传统网络的要求：
- 管理能够实现高度自动化，缩短部署周期；
- 当网络迁移或移动办公时，策略能够灵活调整。

接入方式丰富，传统单点防御失效



- 传统网络的现状：
- 传统网络接入方式，位置固定，攻击点和攻击手段单一；
- 移动化后，办公场所无限扩展，接入终端非常丰富，导致攻击点和攻击手段多样化。
- 对传统网络的要求：
- 将安全设备抽象成安全资源中心，根据需要将用户流量引至安全中心进行处理，提升安全资源利用率，增强全网安全防护能力。

Agile Controller - 智慧的园区大脑



功能组件	功能描述
接入控制组件	提供基于5W1H的策略管理，支持MAC/802.1X/ Portal/SACG认证
访客管理组件	提供访客账号自助注册管理，支持Portal页面内容自定义和页面推送
业务随行组件	基于安全组的策略矩阵与VIP体验保障，让网络资源跟随人移动，保障策略一致，体验一致
业务编排组件	将原来物理设备的能力，抽象成虚拟服务概念，对用户屏蔽具体的物理形态和位置，针对具体的业务，引流至这些业务需要处理的服务结点
安全协防组件	收集安全日志与事件，通过大数据关联分析，识别高危资产和区域，评估全网安全态势，帮助用户实施全网防护和主动防御
终端安全组件	提供丰富的安全策略，提升终端安全等级，阻止不安全的终端以及不满足企业安全策略的终端接入网络

- Agile Controller 系统是智慧的园区大脑，在 SDN 集中化控制思想的指导下，动态调配整个园区的网络与安全资源，让网络更敏捷地为业务服务。提供如下主要功能：
- 提供统一的策略引擎，在整个组织内实施统一访问策略，实现基于用户身份、接入时间、接入地点、终端类型、终端来源、接入方式（简称 5W1H）的认证与授权；
- 提供全生命流程的访客管理，支持个性化定制 Portal 登录界面，基于用户接入位置等因素推送个性化页面，帮助用户快速接入网络，提升企业品牌形象，降低 IT 运维的压力；
- 提供基于优先级的权限规划方式，在 5W1H 策略控制的基础上，实现全网策略的自动部署和状态监测，确保全网策略一致，让用户自动移动时享受一致的业务体验；
- 提供业务编排能力，将安全设备抽象成安全资源中心，根据需要将用户流量引至安全中心进行处理，提升安全资源利用率，增强全网安全防护能力。

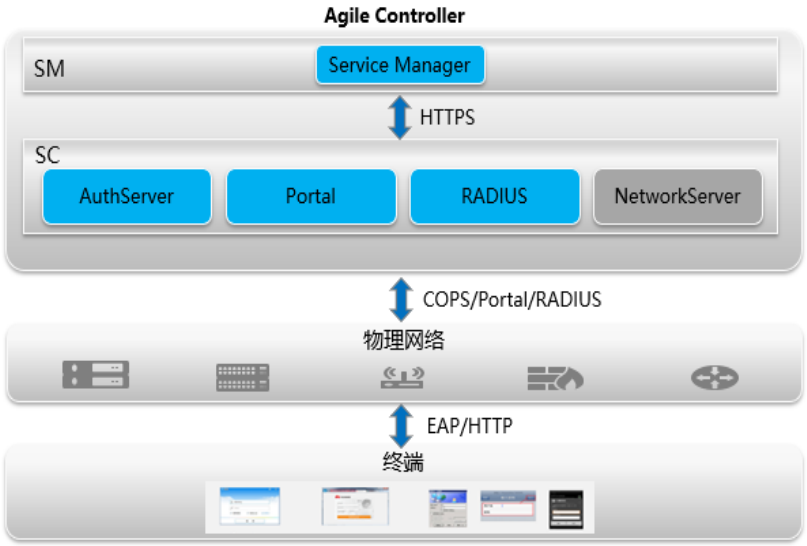
Agile Controller产品架构

- 服务器侧：
- MC（Management Center）：作为 Agile Controller 的管理中心，负责制定总体策略，包括：安全接入控制、终端安全管理、补丁管理、软件分发和 License 管理，并将这些策略下发给各个 SM 节点，同时对 SM 实施情况进行监控；
- SM：业务管理器承担业务管理的角色，系统管理员通过 WEB 管理界面，可以完成准入控制、用户管理和业务随行等管理工作的配置。作为 Agile Controller 系统的管理器，业务管理器将管理其下的各个业务控制器，向已经连接的业务控制器发送实时指令，完成各种业务；
- SC：业务控制器集成有标准的 RADIUS 服务器、Portal 服务器等，负责与网络接入设备联动实现基于用户的网络访问控制策略。业务控制器主要负责完成如下几项业务：
- 与交换机、路由器、WLAN、防火墙等网络接入设备联动，进行全网网络访问策略的统一管理和自动部署，当用户身份认证通过后通知网络接入设备切换用户的网络访问权限；
- 与编排设备联动，下发业务流编排策略，将指定的业务

流引流至安全资源中心里的下一代防火墙（Next Generation Firewall，简称 NGFW）进行处理。

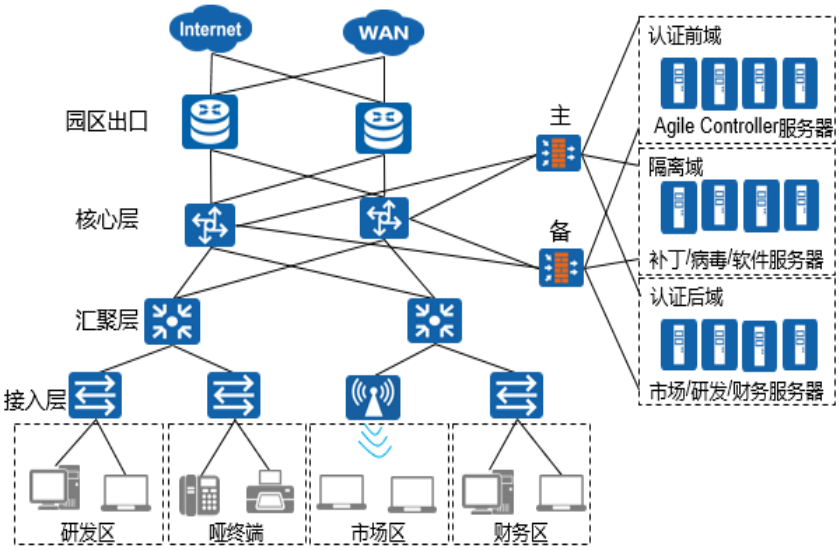
- 网络接入设备用于接入控制和其他业务如安全防护、上网行为管理等的处理。
- 用户侧使用客户端接入网络进行认证。客户端通常使用 EAP/HTTP 协议进行认证。

Agile Controller准入组件架构



- SM 承担业务管理的角色，系统管理员通过 Web 管理界面完成配置管理工作。作为 Agile Controller 的管理器，SM 管理其下的各个 SC，向已经连接的 SC 发送实时指令，完成各种业务配置。
- SC 作为 Agile Controller 的业务控制器，负责用户的业务控制以及与网络设备联动：
- AuthServer 组件用于对开启 COPS 协议的网络设备进行准入控制；
- Portal 组件用于对开启 Portal 协议的网络设备进行准入控制；
- RADIUS 组件用于对开启 RADIUS 协议的网络设备进行准入控制；
- NetworkServer 组件在准入控制中不涉及。
- 物理网络用于接入控制和其他业务如安全防护、上网行为管理等的处理。
- 用户使用客户端接入网络进行认证。客户端通常使用 EAP/HTTP 协议进行认证。

园区网准入控制

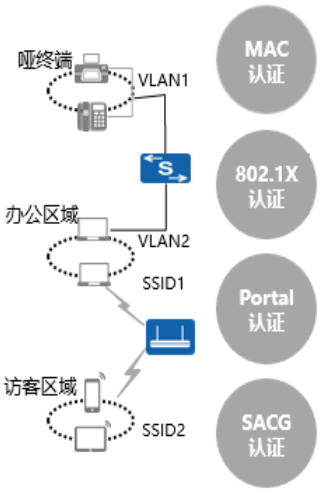


- Agile Controller 系统与 WLAN、华为 Portal 交换机以及标准的 802.1X 交换机配合，提供多维度的网络接入控制功能，能够根据用户的身份、使用终端的类型、当前所处的接入位置、接入时间，以及终端合规性检查的结果，组合起来提供灵活的网络接入授权策略。
- 园区网准入控制部署方案：
- 在接入层交换机/汇聚层交换机或者 AC 开启 802.1X 功能，通过 VLAN、ACL、UCL（敏捷交换机支持）控制权限；
- 再根据各部门的具体需求，结合用户的身份、使用终端的类型、当前所处的接入位置、接入时间等匹配条件，给不同部门之间设备进行准入策略；
- 哑终端不能提供用户名和密码界面，所以哑终端采用 MAC 旁路认证的方式接入网络。
- 认证域分为认证前域，隔离域和认证后域：
- 认证前域是指终端主机在通过身份认证之前能够访问的区域。如图所示，对尚未通过身份认证的终端用户，业务控制器将会通知安全接入控制网关关闭认证后域和隔离域的访问权

限，只开放认证前域的访问权限。

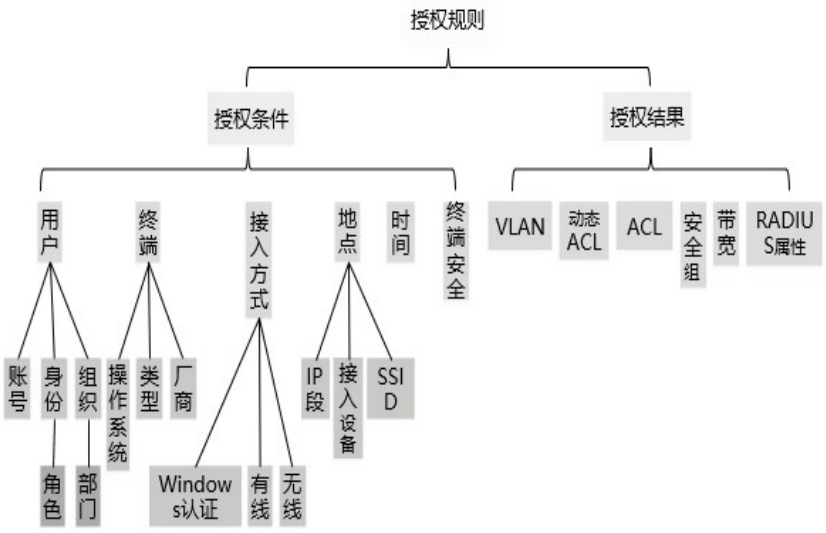
- 不需要进行身份认证即可访问的公共网络资源（如 DNS 服务器、外部认证源、业务控制器、业务管理器等）部署在本区域。

全面的准入控制技术，适用各种网络



- **MAC认证**
  - 用户终端以MAC地址作为身份凭据到认证服务器进行认证。
  - 主要用于IP电话、打印机等哑终端设备。
- **802.1X认证**
  - 使用EAP（Extensible Authentication Protocol）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。
  - 可与华为全系列交换机、路由器及WLAN设备以及第三方标准802.1X交换机联动。
- **Portal认证**
  - 也称为WEB认证，用户可以通过WEB认证页面，输入用户帐号信息，实现对终端用户身份的认证。
  - 可与华为全系列交换机、路由器及WLAN设备联动。
- **SACG认证**
  - 采用USG防火墙旁挂在路由器或者交换机上，通过策略路由控制终端访问。

Agile Controller 准入模型



- 准入模型中，核心是授权条件和授权结果：

- 授权条件是针对接入网络的主体（用户、终端）与一些接入元素（地点、时间、接入方式等）的组合；
- 授权结果是指在设备上通过什么样的方式最终控制用户接入的策略。

访客定义及接入场景

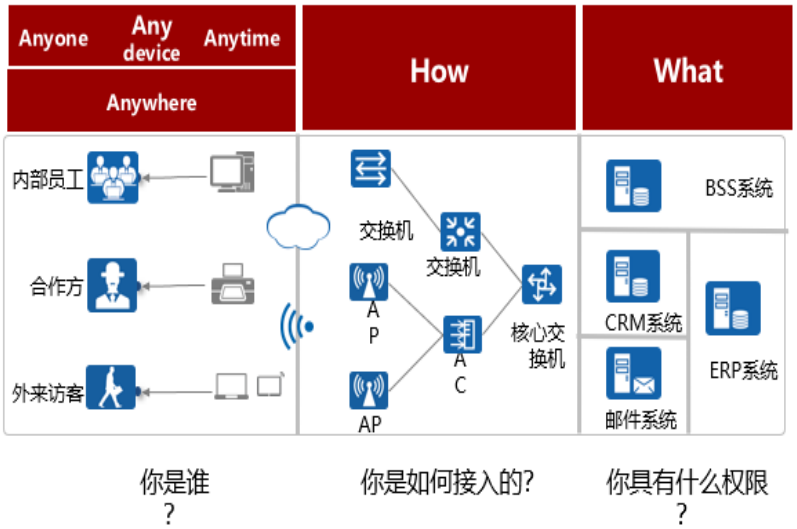
企业访客的定义及接入网络特征

- 什么是访客?
  - 非企业正式员工
  - 到企业来参观、交流的客户，也可能是企业的合作方
  - 在企业消费的客户
  - 普通生活中的大众
- 访客接入有哪些特征?
  - 访客自带设备接入网络
  - 访客言论、行为不受控
  - 访客访问企业网络范围不受控

访客接入的几种典型场景

- 大型企业
  - 典型企业：华为、联想等
  - 典型场景：客户沟通、交流、参观等，接入企业网络，访问企业公共资源或Internet
- 公共事业
  - 典型机构：地铁、机场等
  - 典型场景：普通民众通过这些公共事业单位提供的网络，访问Internet
- 消费型企业
  - 典型企业：高档酒店、咖啡馆等
  - 典型场景：客户在企业消费，同时有访问Internet的需求

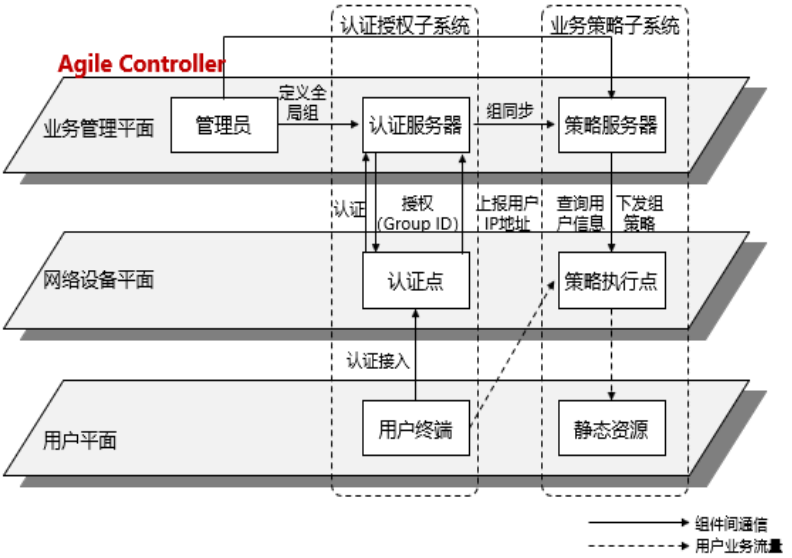
访客认证系统全景图



全生命周期访客管理

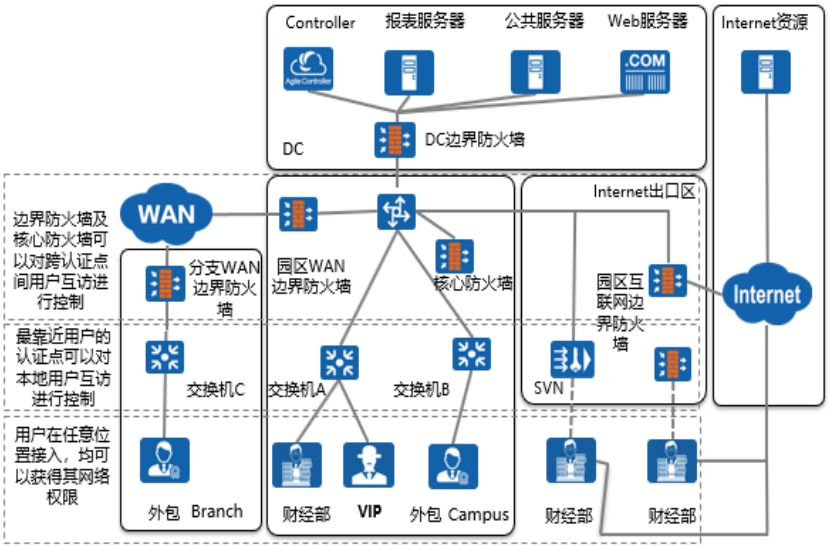
- Agile Controller 系统为企业提供访客管理功能，支持对访客的生命周期管理，实现访客申请、审批、分发、认证、注销的全流程管理。Agile Controller 的访客管理具有如下特点：
- 访客 BYOD 接入，支持 PC、Pad、iPhone、Android 等多种终端接入；
- 支持访客账号注册、审批、分发、注销的全生命周期管理；
- 个性定制，基于 IP，位置等推送定制认证页面，灵活展示广告信息；
- 基于 5W1H 情景感知访客接入授权，严格控制访客访问权限；
- 访客上下线及上网行为审计。

业务随行逻辑架构



- 图中的认证服务器包括 Agile Controller 服务器的 RADIUS、Portal、AuthServer 组件，策略服务器包括 NetworkServer 组件。

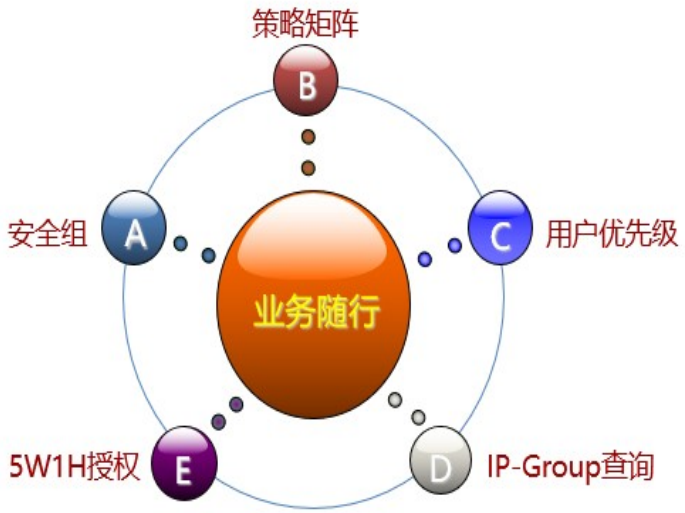
业务随行应用场景



- Agile Controller 业务随行的场景应用：
- 用户访问数据中心权限控制：

- 策略自动部署：如图所示，各部门办公人员访问 DC 的服务器资源，权限策略由 Agile Controller 统一自动部署，管理员只需关注组间互访关系设计，并选取园区中关键位置设备作为策略执行点（通常为认证点交换机、核心防火墙、边界防火墙/SVN）。初始化部署完成之后，无论用户在何位置，以何种方式接入，都可以获得其访问权限。
- 用户间互访控制：
- 跨团队协作办公：如图所示，外包人员与财经人员协作办公，基于策略与 IP，结合“策略自动部署”功能，管理员不需要修改任何配置，就可以快速实现多团队在一起办公，同时保证每个用户都能够拥有正确的网络访问权限。还可根据需要控制团队成员间的数据直接共享行为，保障企业数据的安全。
- VIP 体验保证：
- 出口选路：在广域网与公网出口处，可以根据源和目的组选择不同质量保证的出口。
- SSL VPN 优先上线：SVN 网关资源有限，结合自动优选网关和 VIP 优先上线，可以保证 VIP 用户一定可以接入离其最近的 SVN 网关，享有优质网络体验。

业务随行主要概念



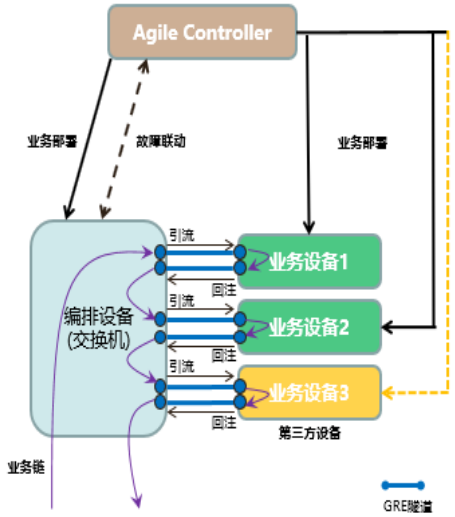
- 安全组：敏捷网络中，用安全组来标识一条流量的源和目的：
- 一类是用户类安全组，这部分安全组中的成员主要指接入网络的用户、哑终端设备，它们的 IP 与安全组的绑定关系在认证中决定；
- 一类是资源类安全组，这部分安全组中的成员主要指网络的一个静态网段或者服务器资源，它们的 IP 需要手动与安全组建立绑定。
- 策略矩阵：业务随行中，通过矩阵关系来描述一个安全组（比如用户）到另一个安全组（比如服务器）的访问权限关系；
- 用户优先级：业务随行中，通过指定某些 VIP 用户所属的安全组的转发优先级，来保障这部分人员的网络使用体验；
- 5W1H 授权：业务随行中，用户类安全组，并不直接与平常使用的用户部门、角色等同，而是通过接入网络中的几个要素：谁（Who）、时间（When）、地点（Where）、终端(What)、终端归属(Whose)、如何接入(How)，来动态决定用

户所归属的安全组；

- IP-Group 查询：因为业务随行中，策略都是基于安全组来定义，而非认证点设备，并不能够识别某一 IP（用户）所归属的安全组，所以需要通过 IP-Group 查询技术，获取 IP 对应的组关系，从而执行基于安全组的策略。

业务随行部署三步曲

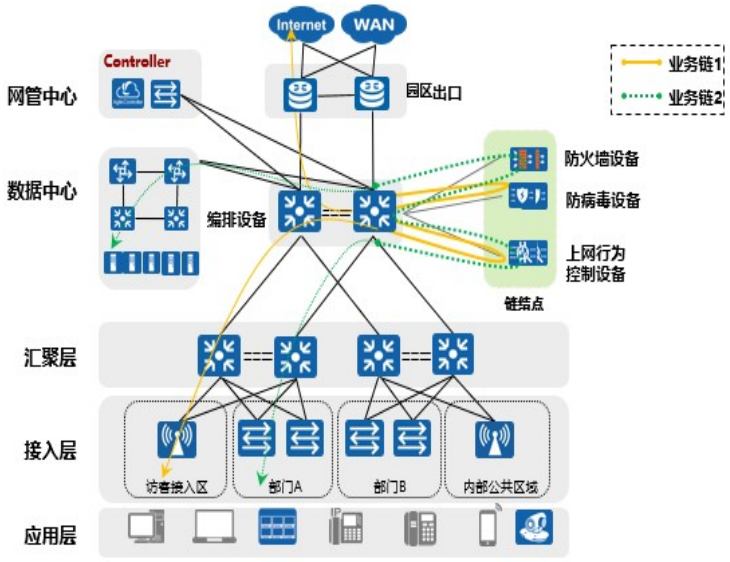
业务编排技术架构



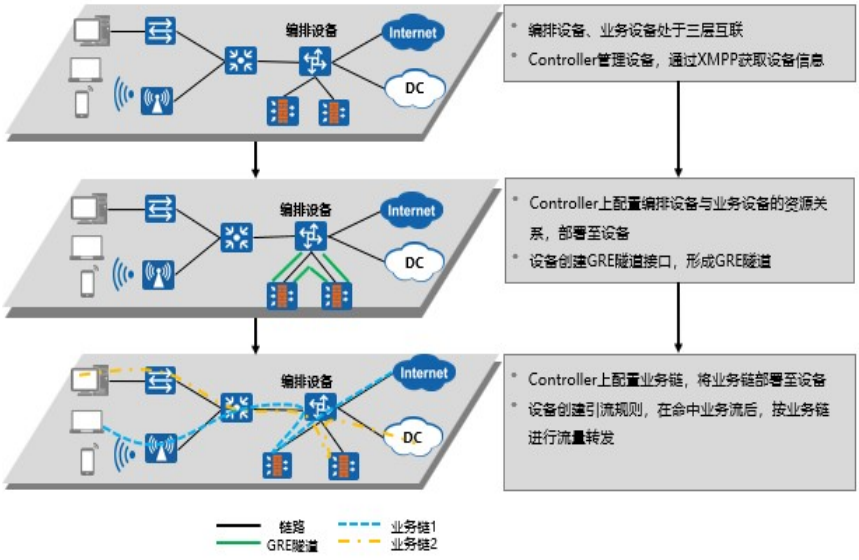
- **Agile Controller**：负责业务链的业务逻辑配置、故障联动。
- **编排设备**：负责业务流量的识别和分流重定向。
- **业务设备**：负责将引导过来的流量进行业务处理。
- **主要技术：**
  - 业务部署基于XMPP协议（华为设备）、TELNET和SNMP协议（第三方）；
  - 设备间的引流，基于两条GRE隧道，通过策略路由方式实现。

- 业务编排基本概念：
- ACL：访问控制列表（Access Control List），是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。
- UCL：用户控制列表（User Control List），是针对用户级别的 ACL 控制，使用数据包的源安全组、目的安全组、端口号等内容定义规则。
- 业务流：符合指定特征（ACL 或者 UCL 规则）的网络流量。
- 编排设备：对业务流进行有序引导的设备，一般指交换机。
- 业务设备：对编排设备引入的业务流进行安全业务处理的设备，主要包括防火墙设备、防病毒设备和上网行为控制设备。
- GRE 隧道：GRE（Generic Routing Encapsulation）隧道是一个虚拟的点对点的连接，提供了一条通路使封装的数据报文能够在这个通路上传输，并且在一个 GRE 隧道的两端分别对数据报进行封装及解封装，用于在编排设备和业务设备之间构建数据的传输通道。
- 业务链资源：业务链资源是指编排设备、业务设备和两种类型设备间的 GRE 隧道信息。
- 业务链：业务链是指由编排设备和业务设备组成的处理业务流的有序链路。
- XMPP（Extensible Messaging and Presence Protocol，前称 Jabber）是一种以 XML 为基础的开放式实时通信协议，是经由互联网工程工作小组（IETF）通过的互联网标准（RFC 3920、 RFC 3921、RFC3922、RFC3923）：

业务编排应用场景

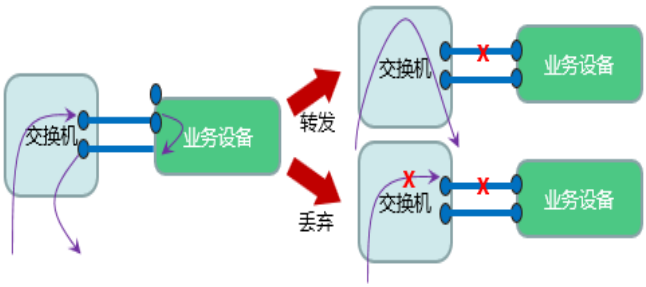


业务编排流程



GRE隧道故障处理 (1)

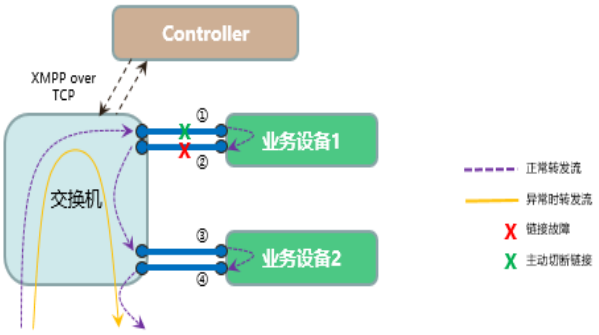
1.出交换机方向GRE隧道故障处理



- **故障处理：**
  - **GRE隧道保活机制**：GRE隧道默认开启Keepalive保活机制；
  - **GRE隧道故障处理**：为了增加业务编排场景的可靠性，可以通过配置当GRE隧道故障时丢弃或直接转发报文。

GRE隧道故障处理 (2)

2.进交换机方向GRE隧道故障处理



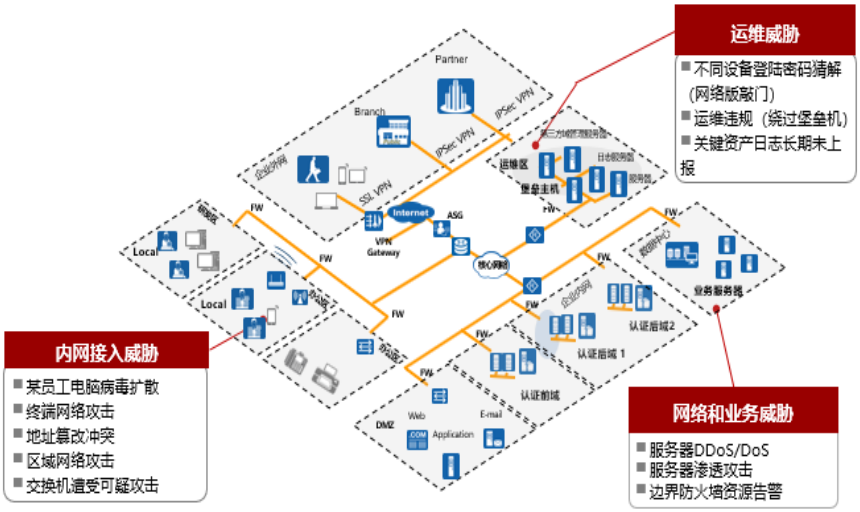
- 隧道②发生故障时，流量会经过隧道①到达业务设备1后，被丢弃，无法得到正确处理。
- Controller解决上述问题的过程：
  - 当交换机的GRE隧道发生故障时，通过XMPP接口向Controller上报故障；
  - Controller判断并主动Down掉其成对的另一个GRE隧道口，取消GRE隧道③和GRE隧道④的配置。从而使交换机接收的流量按照指定的策略选择丢弃或者直接查找路由表进行转发。

- 正常处理过程：
- GRE 隧道未发生故障时，如图所示，流量转发到交换机之后，交换机按照匹配规则将流量重定向到指定 Tunnel 接口，经 GRE 隧道 ①转发给应用安全网关；
- 业务设备 1 处理此流量后再将其重定向到指定 Tunnel 接

口，经 GRE 隧道②返回给交换机；

- 交换机将从 GRE 隧道②接收的业务流量又重定向到 GRE 隧道③所在的 Tunnel 接口，转发给业务设备 2。就这样，业务流量又经过业务设备 2 处理后再次返回给交换机；
- 交换机在从 GRE 隧道④接收业务流量后，由于后续不在需要其他业务设备处理，所以交换机就通过查找路由表将此业务流量转发到外部网络。

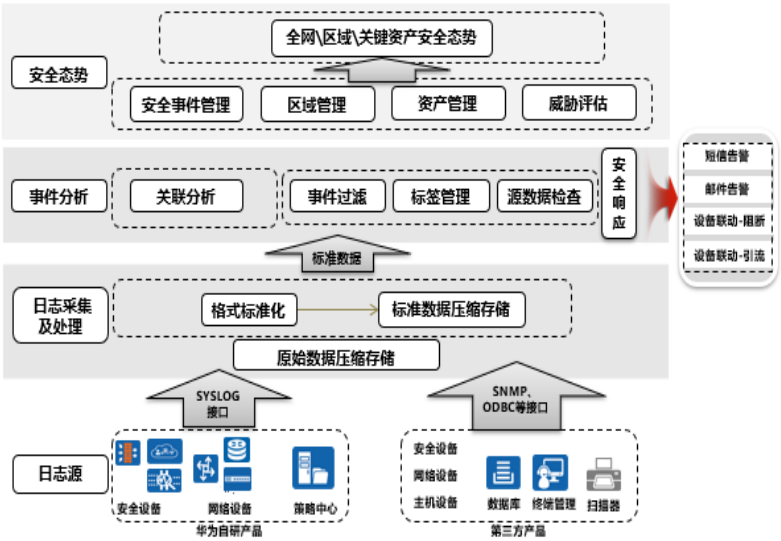
安全协防应用场景



- 安全协防通过关联分析网络中的日志，识别网络中潜在的安全问题，并将发现的网络安全问题直观的展现给网络管理员。

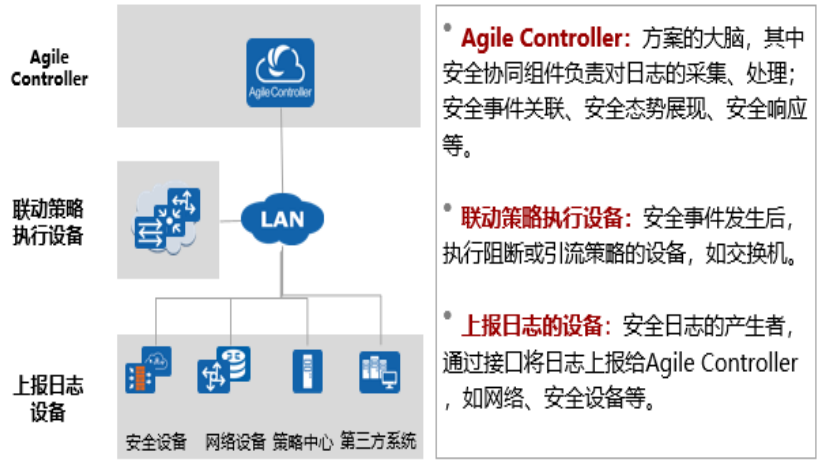
- 有了安全协防后，管理员可以将资产添加到安全协防进行统一的管控，安全协防通过对资产上报的日志进行关联分析，识别网络中潜在的安全问题，最后通过拓扑和列表等多种方式，将安全态势直观的展现给管理员，帮助管理员轻松方便的掌握所有资产的安全情况，构筑安全网络。
- 堡垒机是在一个特定的网络环境下，为了保障网络和数据不受来自外部和内部用户的入侵和破坏，而运用各种技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动，以便集中报警、记录、分析、处理的一种技术手段。

方案整体架构



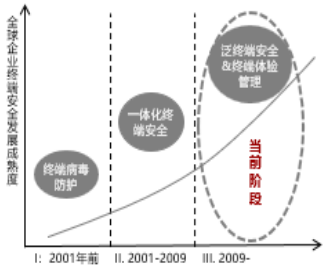
- 方案架构由以下几个层次构成：
- 日志源：能够提供日志信息的设备或服务器，本方案中重点针对华为自研产品进行日志采集和处理。当然也可以对第三方产品进行采集，请参见产品支持规格列表；
- 日志采集及处理：日志源将日志信息通过相应接口提供给日志采集及处理层后，该层对原始日志进行压缩存储，并对原始日志进行标准化处理和存储，标准化处理的目的是为了提高数据在后续处理中的速度；
- 事件分析：将标准化的数据以及配置的关联规则，通过关联分析引擎的计算得出有价值的安全威胁事件。对安全事件提供几种安全响应手段，其中包含告警（短信告警和邮件告警）和设备联动（阻断和引流）；
- 安全态势：根据分析得出全网发生的安全事件，通过区域管理、资产管理、威胁评估等手段，得到基于关键资产、区域乃至全网的安全态势。

方案组件与用途



- 安全联动解决方案中主要用到三个组件，从下到上依次为：
- 上报日志设备：由网络中部署的设备（网络设备、安全设备、策略服务器、第三方系统等）来承担，主要负责提供网络、安全日志；
- 联动策略执行设备：由交换机来承担，主要负责安全事件发生后的设备联动部分的安全响应，是执行阻断或引流策略的设备；
- Agile Controller：方案的大脑，本方案用到的是 Agile Controller 的安全协同组件，这部分负责对日志的采集、处理、事件关联、安全态势展现、安全响应。

终端安全管理现状和发展趋势

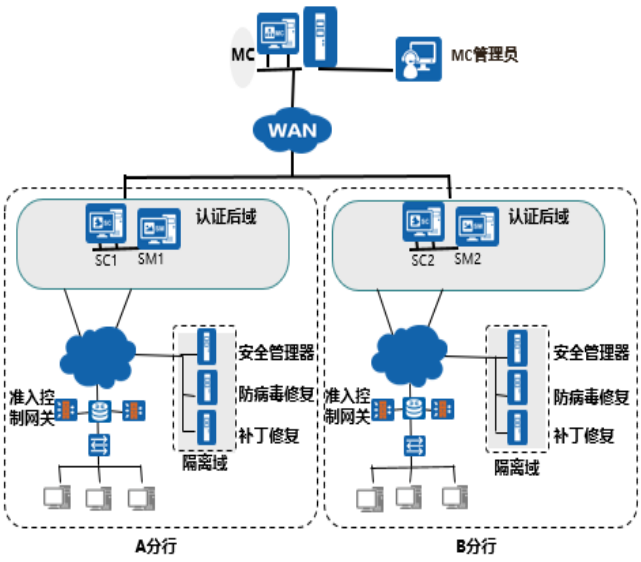


- 2001年以前，终端安全主要依赖于防病毒、反间谍软件技术，随着技术变化和安全威胁的花样翻新，终端安全事件屡屡发生，导致了用户对防病毒软件的不信任，以至于引发了防病毒软件是否卖“过期药”的激烈讨论；
- 2001年到2009年，终端安全由简单的病毒防护，发展到以准入控制、终端安全、行为管控的**一体化解决方案**；
- 2009年以后，随着移动办公用户的快速增长，终端安全管理的范畴由传统PC机的管理扩展到智能终端以及各种IP设备的**泛终端统一管理**，终端安全的管理方针由以前的事件驱动发展为**主动防御、综合防范、强化体验。**

终端安全管理4大发展趋势

泛终端	全功能	平台化	个性化
□各种类型终端统一管理 □物理+虚拟统一管理	□准入控制+安全管理 □被动防御+主动控制	□全网联动协同 □开放集成能力	□桌面管家应用 □桌面用户服务

终端安全技术架构



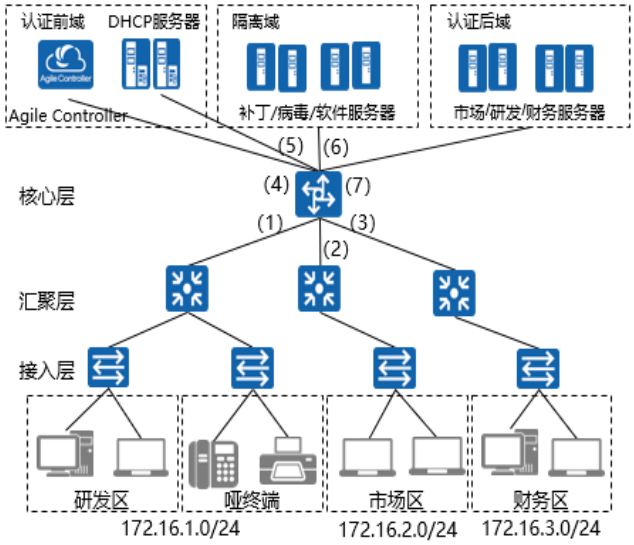
多级管理模型

- 通过MC管理中心可以集中配置和分发策略到下级终端安全管理服务器。
- 终端安全客户端按照分配的安全策略对终端进行检查，检查通过后服务器可以通知准入控制设备给终端开放网络权限，如果检查不通过，可以对终端进行隔离修复。

通过终端安全检查确保终端安全合规

- 终端安全管理特点：
- 一键修复，降低终端管理维护成本：
- 如果终端不符合企业安全策略，用户往往希望提供自动修复功能，现在已经完全能实现不合规状态的自动修复，用户只需要点击鼠标,即可在最短的时间内实现一键修复。
- 桌面安全标准化、降低病毒感染风险：
- 只允许安装标准软件，实现桌面办公标准化；
- 控制非法的 web 访问，提高工作效率；
- 禁止非标软件的安装，降低病毒感染风险。
- 终端外设管理和行为监控：
- 控制终端外泄途径，通过准入控制确保入网终端强制安装客户端且符合安全要求，监控通过使用外设和网络进行泄密的行为，同时提供全面审计，满足事后审计需求。

Agile Controller配置案例



- 业部署 Agile Controller-Campus，希望控制终端设备的接入，实现如下需求：
- 以核心交换机作为与 Agile Controller 联动的网络接入设备；
- 在未进行认证的情况下，只允许用户访问 Agile Controller 与 DHCP 服务器，禁止访问隔离域与认证后域；
- 通过认证，但没有通过安全检查的用户，需要在隔离域内进行修复；
- 认证通过后，市场部员工能够访问市场部的服务器，研发部员工能够研发部的服务器，财务部能够访问财务部的服务器；
- 园区接入场景主要用于实现基于帐号、终端类型和接入方式的权限控制，与用户在何处登录无关，权限随行；
- 对于哑终端设备采用 MAC 旁路认证。

园区IP地址规划

- 园区IP地址规划表如下：

项目	数据
(1)	交换机接口GigbitEthernet 0/0/1，IP地址为172.16.1.254，属于VLAN 10。
(2)	交换机接口GigbitEthernet 0/0/2，IP地址为172.16.2.254，属于VLAN 20。
(3)	交换机接口GigbitEthernet 0/0/3，IP地址为172.16.3.254，属于VLAN 30。
(4)	交换机接口GigbitEthernet 0/0/4，IP地址为172.16.4.254，属于VLAN 40。
	业务管理器和业务控制器的IP地址为172.16.4.253。
(5)	交换机接口GigbitEthernet 0/0/5，IP地址为172.16.5.254，属于VLAN 50。
	DHCP服务器的IP地址为172.16.5.253。
(6)	交换机接口GigbitEthernet 0/0/6，IP地址为172.16.6.254，属于VLAN 60。
	补丁服务器和防病毒服务器的IP地址为172.16.6.253。
(7)	交换机接口GigbitEthernet 0/0/6，IP地址为172.16.7.254，属于VLAN 70。
	研发部的服务器IP地址为172.16.7.253。
	市场部的服务器IP地址为172.16.7.252。
	财务部的服务器IP地址为172.16.7.251。

组织结构规划

- 组织结构规划表如下：

项目	子项	数据
组织规划	部门	研发部
		市场部
		财务部
	接入控制方式	802.1X交换机
域规划	认证前域	Guest VLAN中的网络资源
	隔离域	隔离域：切换至VLAN 60
	认证后域	认证后域： 研发部访问研发部服务器 市场部访问市场部服务器 财务部访问财务部服务器
帐号规划	帐号	Kelly（研发部）；Larry（市场部）；Tony（财务部）
	初始帐号密码	Admin@123
	接入控制方式	继承所属部的接入控制方式
免认证规划	打印机	哑终端设备
	认证方式	免认证
	MAC地址	00-0c-29-69-9c-40

配置思路分析 (1)

- 交换机侧的配置思路：
  - 配置RADIUS服务器模板
  - 配置认证方案和计费方案
  - 配置default域
  - 开启DHCP中继：动态切换VLAN需要DHCP服务器的支持。当端口切换到另一个VLAN时，DHCP服务器为端口分配不同网段的IP地址，以便接入新的VLAN
  - 开启802.1X
  - 创建VLAN并配置IP地址
  - 开启接口的802.1X，并把接口加入VLAN
  - 在二层交换机上开启802.1X认证报文二层报文透明传输功能
  - 保存配置信息

配置思路分析 (2)

- 业务管理器侧的配置思路：
  - 增加交换机组：在实际的应用环境中，实施802.1X接入控制的交换机很可能不止一台。需要对实施802.1X认证的所有交换机进行集中管理，称之为交换机组，成员是实施802.1X认证的交换机
  - 增加隔离域
  - 增加认证后域
  - 应用隔离域和认证后域到各部门：在终端用户在安全检查不通过或安全检查通过时业务控制器将终端用户切换至隔离域和认证后域，以便实现网络隔离和网络访问授权
  - 增加MAC旁路设备：为无法安装AnyOffice或者不适合实施802.1X网络接入控制的设备开启免认证功能

交换机配置 (1)

- 配置RADIUS服务器模板：

```
<Quidway> system-view
[Quidway] radius-server template template1
#以业务控制器的IP地址作为认证服务器的地址，认证端口是1812。
[Quidway-radius-template1] radius-server authentication 172.16.4.253 1812
#以业务控制器的IP地址作为计费服务器的地址，认证端口是1813。
[Quidway-radius-template1] radius-server accounting 172.16.4.253 1813
#将RADIUS认证的共享密钥设置为Admin@123。
#在业务管理器配置802.1X交换机时，配置界面上的认证密钥、计费密钥必须与此密钥保持一致。
[Quidway-radius-template1] radius-server shared-key cipher Admin@123
[Quidway-radius-template1] quit
#创建RADIUS服务器模板后，查看RADIUS服务器模板的配置信息。确认RADIUS服务器的IP地址、端口、密钥正确无误。
[Quidway] display radius-server configuration template template1
```

交换机配置 (2)

- 创建认证方案auth和计费方案acco，然后将认证模式设为RADIUS，计费模式设为RADIUS。

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme auth
#将认证与计费模式设为RADIUS，配置完成后检查认证方案的参数配置。
[Quidway-aaa-authen-auth] authentication-mode radius
[Quidway-aaa-authen-auth] quit
[Quidway-aaa] display authentication-scheme
[Quidway-aaa] accounting-scheme acco
[Quidway-aaa-accounting-acco] accounting-mode radius
[Quidway-aaa-accounting-acco] quit
[Quidway-aaa] display accounting-scheme
```

交换机配置 (3)

- 引用RADIUS服务器模板template1、认证方案auth和计费方案acco。

```
[Quidway-aaa] domain default
#通过名称template1引用RADIUS服务器模板。
[Quidway-aaa-domain-default] radius-server template1
#通过名称auth引用认证模式。
[Quidway-aaa-domain-default] authentication-scheme auth
#通过名称acco引用计费模式。
[Quidway-aaa-domain-default] accounting-scheme acco
[Quidway-aaa-domain-default] quit
[Quidway-aaa] quit
#查看AAA的配置信息，确认认证方案、计费方案和RADIUS服务器模板是正确的。
[Quidway] display domain name default
```

- 把RADIUS服务器配置成授权服务器，以便RADIUS服务器根据终端用户的认证状态通知交换机切换接口的VLAN。

```
[Quidway] radius-server authorization 172.16.4.253 shared-key cipher Admin@123
```

交换机配置 (4)

- 开启DHCP功能。

```
[Quidway] dhcp enable
```

- 开启802.1X认证功能。

```
[Quidway] dot1x enable
[Quidway] dot1x authentication-method eap
```

- 创建VLAN 10、20、30、40、50、60、70，并配置各个VLAN接口的IP地址。

```
[Quidway] vlan batch 10 20 30 40 50 60 70
```

- 将VLAN 10接口的IP地址配置为172.16.1.254，并在接口开启DHCP中继功能，确保VLAN 10能够跨网段获取DHCP服务器分配的IP地址。

```
[Quidway] interface Vlanif 10
[Quidway-Vlanif10] ip address 172.16.1.254 255.255.255.0
[Quidway-Vlanif10] dhcp select relay
[Quidway-Vlanif10] dhcp relay server-ip 172.16.5.253
[Quidway-Vlanif10] quit
#VLAN20，VLAN30的配置与VLAN10类似，略。
```

交换机配置 (5)

- 在连接终端主机的接口开启802.1X认证功能，并把接口分别加入相应VLAN。

```
[Quidway] interface GigbitEthernet 0/0/1
#加入VLAN 10。交换机其他的接口加入VLAN过程类似，略。
[Quidway-GigbitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigbitEthernet0/0/1] port hybrid untagged vlan 10
```

- 在接口GigbitEthernet 0/0/1启用802.1X功能，GigbitEthernet 0/0/2和GigbitEthernet 0/0/3配置类似，略 。

```
[Quidway-GigbitEthernet0/0/1] dot1x enable
[Quidway-GigbitEthernet0/0/1] dot1x port-control auto
#启用基于端口的接入模式。
[Quidway-GigbitEthernet0/0/1] dot1x port-method port
#确保AnyOffice在认证前能够访问业务控制器所在的VLAN。
[Quidway-GigbitEthernet0/0/1] authentication guest-vlan 40
[Quidway-GigbitEthernet0/0/1] quit
#连接打印机接口的配置MAC旁路认证，确保打印机在免认证的情况下能够访问网络。
[Quidway-GigbitEthernet0/0/1] dot1x mac-bypass
[Quidway-GigbitEthernet0/0/1] quit
```

交换机配置 (6)

- 使能802.1x认证的接入设备Switch与用户之间存在二层的汇聚与接入交换机，为保证用户的802.1x认证报文能够通过二层交换机，需要在汇聚与接入交换机上进行如下配置（二层交换机以S5700HI为例进行说明）：

```
<HUAWEI> system-view
[HUAWEI] sysname LAN Switch
[LAN Switch] l2protocol-tunnel user-defined-protocol dot1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002
#group-mac不能设置为保留的组播MAC地址（0180-C200-0000～0180-C200-002F）以及其他几种特殊MAC地址，其余MAC地址均可。
[LAN Switch] interface gigabitethernet 0/0/1
#需要在二层交换机连接上行网络以及用户的所有接口上进行配置
[LAN Switch-GigabitEthernet0/0/1] l2protocol-tunnel user-defined-protocol dot1x enable
[LAN Switch-GigabitEthernet0/0/1] bpdu enable
[LAN Switch-GigabitEthernet0/0/1] quit
```

业务管理器配置

- 以Admin帐号登录Agile Controller。
- 增加交换机组。
  - #在业务管理器选择“资源 > 设备 > 设备管理”。
  - #在“设备组 > 准入控制设备组”单击 。单击“增加子组”，增加一个交换机组，如下图：

- #单击“确定”。增加交换机组成功后，选择“所有设备”。
- #单击“增加”。

业务管理器配置

- #添加设备后，填写认证设备的IP地址172.16.4.254，使用RADIUS时认证与审计的密码为Admin@123。
- #单击“确定”。单击“准入控制设备组”，选择“Quidway S5300”交换机，然后单击“移动”，把“Quidway S5300”交换机移动到“Switch_Core”交换机组，如下图：

增加授权结果 - 隔离域

- #选择“策略 > 准入控制 > 认证授权 > 授权结果”，单击“增加”，增加VLAN 60作为隔离域。

- #设置完成后如下如图:

增加授权结果 - 认证后域

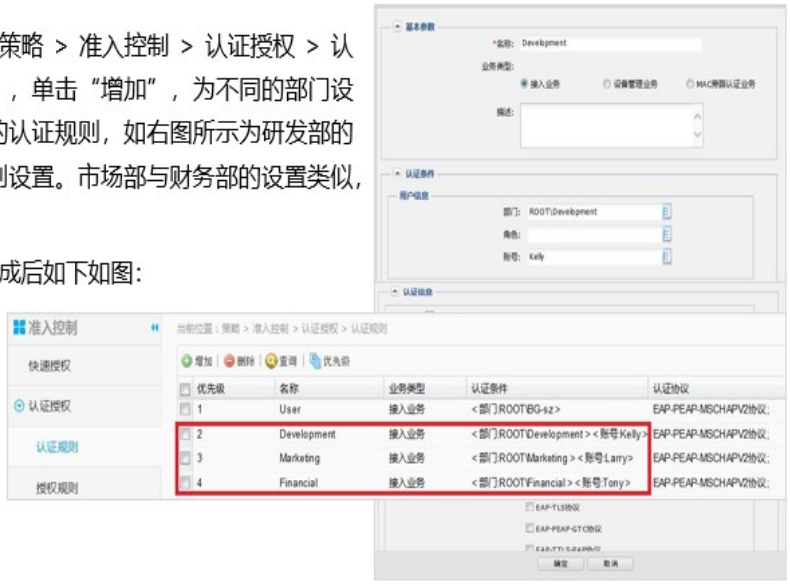
- #由于各部门的服务器设置在同一VLAN中，所以为保证各部门人员只能访问本部门的服务器，需要在Controller上设置动态ACL，控制访问权限。如右图所示，分别设置ACL 3001，ACL 3002与ACL 3003只允许访问研发部服务器，只允许访问市场部服务器与只允许访问财务部服务器。
- #选择“策略 > 准入控制 > 策略元素 > 动态ACL”，单击“增加”，增加ACL 3001。
- #设置完成后如右图:

增加授权结果 - 认证后域

- #选择“策略 > 准入控制 > 认证授权 > 授权结果”，单击“增加”，为不同的部门设置不同的认证后域，如右图所示为研发部的认证后域设置。市场部与财务部的设置类似，只是调用不同的ACL，操作略。
- #设置完成后如下如图：

增加认证规则

- #选择“策略 > 准入控制 > 认证授权 > 认证规则”，单击“增加”，为不同的部门设置不同的认证规则，如右图所示为研发部的认证规则设置。市场部与财务部的设置类似，操作略。
- #设置完成后如下如图：



增加授权规则 - 隔离域

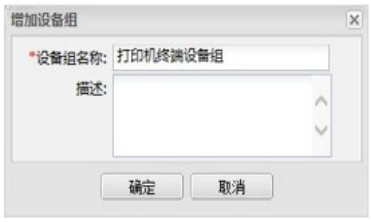
- #选择“策略 > 准入控制 > 认证授权 > 授权规则”，单击“增加”，配置当终端执行策略检查出现严重违规时交换机把接口所属的VLAN切换到为VLAN 60（隔离域）。为不同的部门设置不同的授权规则，如右图所示为研发部的授权规则设置。市场部与财务部的设置类似，操作略。
- #设置完成后如下如图：

增加授权规则 - 认证后域

- #选择“策略 > 准入控制 > 认证授权 > 授权规则”，单击“增加”，配置当终端执行策略检查没有发现严重违规时交换机把接口所属的VLAN切换到为VLAN 70（认证后域）。为不同的部门设置不同的授权规则，如右图所示为研发部的授权规则设置。市场部与财务部的设置类似，操作略。
- #设置完成后如下如图：

增加MAC旁路认证设备 (1)

- #选择“资源 > 终端 > 终端列表”，选择“设备组”，单击“增加”，为打印机创建单独的一个终端设备组。



- #选择“打印机终端设备组”，在“设备组列表”中单击“增加”，增加设备组名称为“Printer”，操作如下图:

- #点击确定后，完成设备组的创建。

增加MAC旁路认证设备 (2)

- #选择“Printer”，在“设备列表”中单击“增加”，操作如下图:

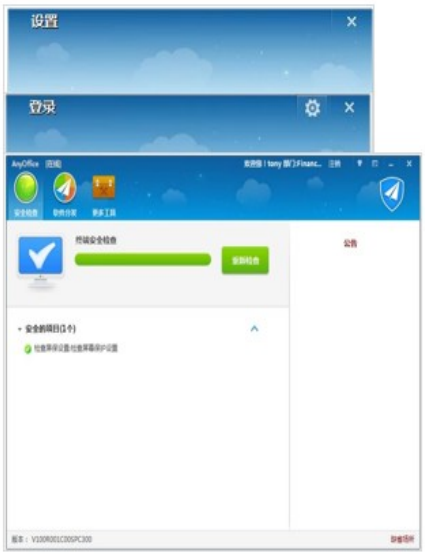
- #根据需求将需要进行MAC旁路认证的打印机MAC地址填入右图所示的列表中并勾选“自定义设备组”，点击确定完成设备添加。

增加MAC旁路认证设备 - 认证与授权

- #选择“策略 > 准入控制 > 认证授权 > 认证规则”，单击“增加”，配置交换机触发MAC旁路认证请求时，Agile Controller-Campus予以放行。如右图所示：
- #选择“授权规则”，单击“增加”，配置交换机触发MAC旁路认证请求时，交换机予以放行。如右图所示：
- #非打印机终端设备组的MAC旁路认证请求则交换机不允许接入网络。同样在“授权规则”页面单击“增加”，增加非打印机终端设备组的设备拒绝接入的授权规则。

验证配置的正确性

- #在AnyOffice使用财务部的Tony帐号进行身份认证，在进行身份认证时选中“启用802.1X协议”。
- #身份认证和安全检查均通过，如右图所示，此时就可以访问财务部的服务器了。



思考题

1. Agile Controller的认证域有哪几种？（ ）

   A. 认证前域

   B. 认证后域

   C. 隔离域

   D. 认证域

2. Agile Controller能够实现准入控制的技术有哪些？（ ）

   A. MAC认证

   B. Portal认证

   C. 802.1X认证

   D. SACG认证

- 1、答案：ABC。
- 2、答案：ABCD。
-