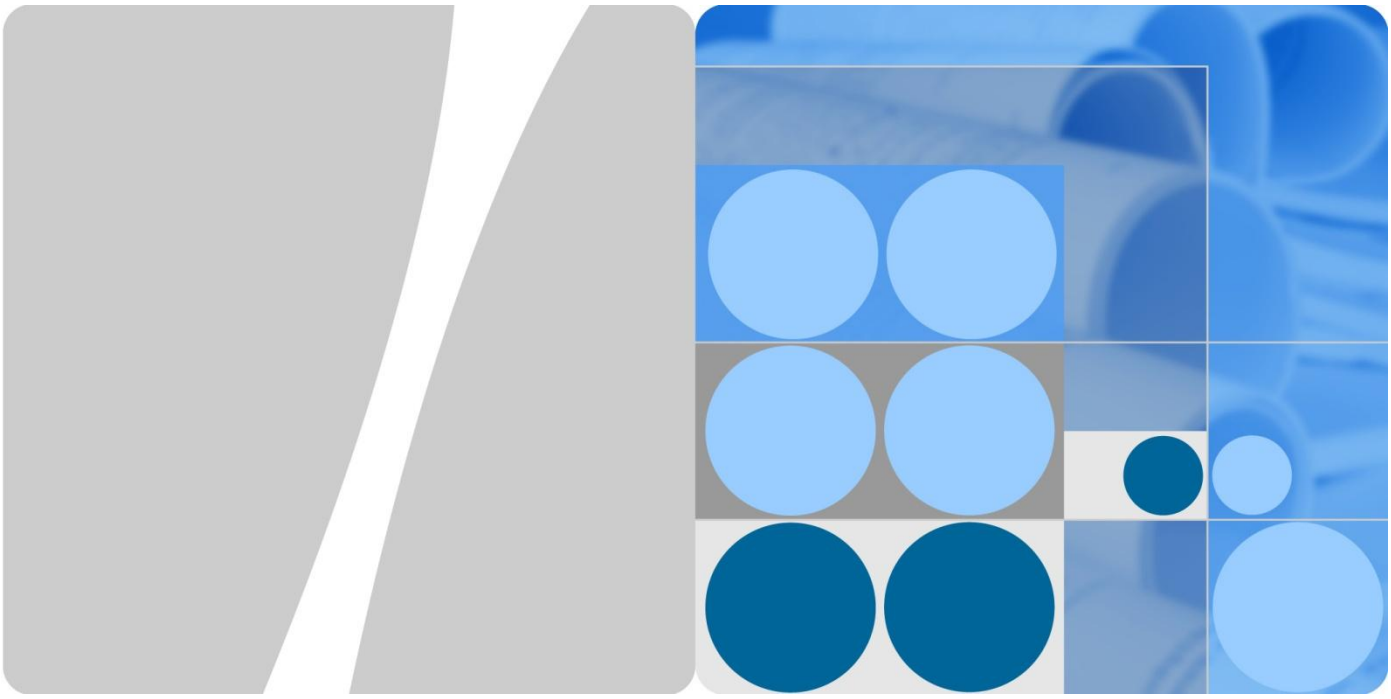
资料编码



ONE NET Campus NAC 安全方案 V100R001C02

技术白皮书

文档版本 01

发布日期 2012-07-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com

客户服务邮箱： ChinaEnterprise_TAC@huawei.com

客户服务电话： 4008302118

目 录

1 前言

随着网络技术的应用与发展，人们对信息网络的应用需求不断提升，对网络的依赖性也越强，伴随而来的信息安全威胁也在不断增加。网络安全已经超过对网络可靠性、交换能力和服务质量的需求，成为企业用户最关心的问题，网络安全基础设施也日渐成为企业网建设的重中之重。

在企业网中，新的安全威胁不断涌现，病毒日益肆虐。它们对网络的破坏程度和范围持续扩大，经常引起系统崩溃、网络瘫痪，使企业蒙受严重损失。在企业网络中，任何一台终端的安全状态（主要是指终端的防病毒能力、补丁级别和系统安全设置）都将直接影响到整个网络的安全。

目前，针对病毒的防御体系还是以孤立的单点防御为主，如在个人计算机上安装防病毒软件、防火墙软件等。当发现新的病毒或新的网络攻击时，一般是由网络管理员发布病毒告警或补丁升级公告，要求网络中的所有计算机安装相关防御软件。从企业病毒泛滥、损失严重的结果来看，当前的防御方式并不能有效应对病毒的威胁，存在严重不足，主要表现在以下几个方面：

- 被动防御，缺乏主动抵抗能力

  在多数情况下，当一个终端受到感染时，病毒已经散布于整个网络。亡羊补牢的方法固然有效，但企业用户更多需要的是：在安全威胁尚未发生时就对网络进行监控和修补，使其能够自己抵御来自外部的侵害。而对网络管理员来说，目前的解决方式无法有效监控每一个终端安全状态，也没有隔离、修复不合格终端的手段，造成主动防御能力低下。

- 单点防御，对病毒的重复、交叉感染缺乏控制

  目前的解决方式，更多的是在单点防范，当网络中有某台或某几台机器始终没有解决病毒问题而又能够顺利上网时，网络就会始终处于被感染、被攻击状态。

- 分散管理，安全策略不统一，缺乏全局防御能力

  只有从用户的接入终端进行安全控制，才能够从源头上防御威胁，但是，分散管理的终端难以保证其安全状态符合企业安全策略，无法有效地从网络接入点进行安全防范。在分散管理的安全体系中，新的补丁发布了却无人理会、新的病毒出现了却不及时升级病毒库的现象普遍存在。分散管理的安全体系无法彻底解决病毒和操作系统漏洞带来的网络安全威胁。

2 NAC 技术介绍

华为的 NAC 安全解决方案以“只有合法的用户、安全的终端才可以接入网络”为主导思想。以全系列的企业网络和安全产品，结合 TSM（Terminal Security Management）系统，提供以“用户认证、安全检查、修复升级”为基础的全面安全 NAC 解决方案，并提供了丰富扩展特性，为企业网络提供了整体终端安全防护能力。

2.1 802.1X 认证

标准的 802.1X 协议是一种基于端口的网络接入控制协议，用于在局域网接入设备的端口一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

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。在客户端与设备端之间，EAP 协议报文使用 EAPoL（EAP over LAN）封装格式，直接承载于 LAN 环境中。

2.2 Portal 认证

Portal 认证是一种三层认证方式。用户可以通过访问 Portal 服务器（Web 服务器）上的 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。采用 Portal 认证，用户可以无需安装客户端软件，用户访问 Portal 页面时，通过自动提示下载的 ActiveX 控件实现基本安全检查功能。

Portal 认证支持 Web 认证且可以无需安装客户端软件，这两个特性使得 Portal 认证对于访客和出差用户具有很好的支持。

说明

Portal 认证方式下，仍旧可以通过下载客户端的方式实现完整的终端准入控制功能特性。

2.3 MAC 认证

对某些特殊情况，终端用户不想或不能通过输入用户帐号信息的方式完成认证。例如某些特权终端希望能“免认证”直接访问网络；对于某些特殊的 PC 终端，如打印机、IP

电话等设备，无法安装客户端软件，也无法通过输入用户帐号信息的方式进行认证授权。此时可以采用 MAC 认证的方式实现对终端的网络访问控制。

MAC 认证就是以终端的 MAC 地址作为身份凭据到系统进行认证。启用 MAC 认证后，当终端接入网络时，网络准入设备提取终端 MAC 地址，并将该 MAC 地址作为用户名和密码进行认证。如果认证失败使用户下线，并保持一段时间内不再发起认证和探测，超时后重新开始探测过程。如果认证成功，交换机将增加该 MAC 地址进入 MAC 表，用户将可以正常访问网络。

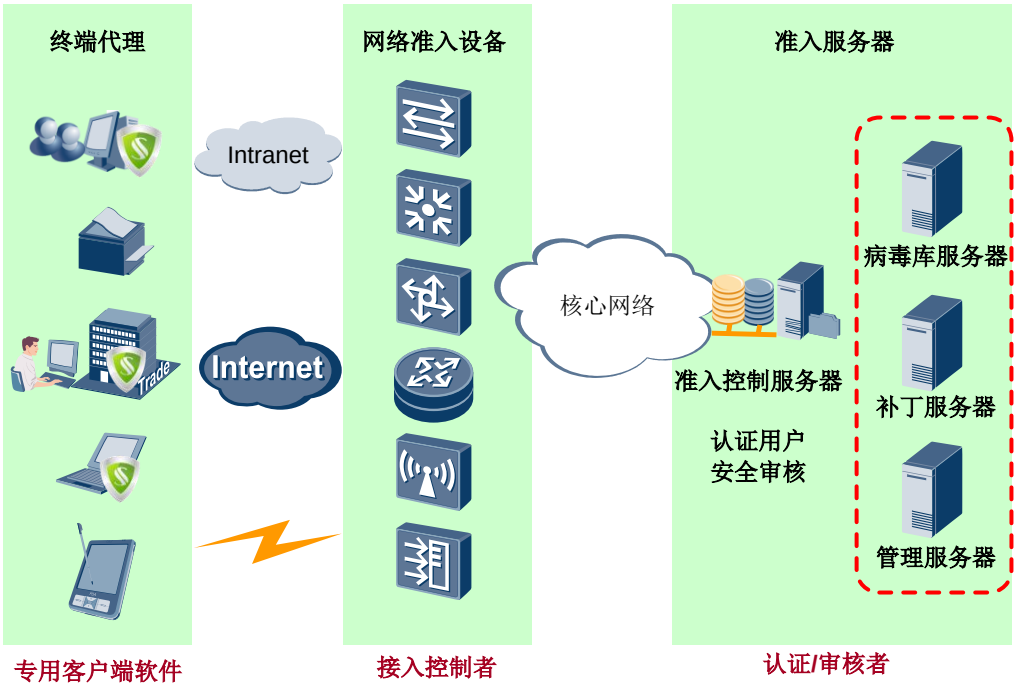
对于用户的 MAC 认证，即可以是本地认证，也可以是远端 RADIUS 服务器认证。如果采用 RADIUS 认证，用户的访问权限由 RADIUS 服务器下发的 ACL 或 VLAN 来控制。

3 NAC 解决方案

3.1 概述

NAC 安全系统（以下简称 NAC 系统）框架中包括三个关键组件：终端代理、网络准入设备和准入服务器，如图 3-1 所示。

图3-1 NAC 系统组成部件示意图



3.2 终端代理

终端代理是安装在用户终端系统上的专用客户端软件，与准入服务器联动进行用户身份认证、终端安全检查、系统修复升级，终端行为监控审计等工作。

- 用户身份认证

  终端安装客户端软件后，可以进行用户名及密码输入，送到准入服务器。

- 终端安全检查

  终端安全检查也称终端健康检查。客户端软件负责根据准入服务器下发的安全策略检查用户终端的安全状态，包括操作系统版本、系统补丁状况、防病毒软件安装情况、病毒库日期、应用进程黑白名单等信息，并将安全检查结果上报准入服务器，用于判断终端是否“安全/健康”。

- 系统修复升级

  客户端软件接受准入服务器的指示，对未达到安全标准的用户终端，自动或强制其进行修复升级工作，修复完成后可以向准入服务器上报结果。

- 监控审计

  实时监控终端主机安全状态和用户行为是否符合安全策略，并将安全事件定时上报到准入服务器，用于事后进行安全审计。终端主机安全检查包括终端代理执行补丁、防病毒软件、屏幕保护、共享目录等检查。用户行为监控包括终端代理执行文件操作、网络连接、访问站点、USB 存储设备等监控。

3.3 网络准入设备

网络准入设备是终端访问网络的网络控制点，是企业安全策略的实施者，负责按照客户网络制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）。

华为 NAC 方案中，网络准入设备可以是交换机、路由器、无线接入点、VPN 网关或其它安全设备，通过这些网络准入设备，实现强制用户准入认证、拒绝非法用户的网络访问、隔离不健康终端、为“合法用户、健康终端”提供网络服务的目的。

网络准入设备具备如下功能特性：

- 用户身份认证

  网络准入设备可协助终端代理完成认证。华为 NAC 方案支持 802.1X、MAC 认证和 Portal 多种认证方式。在各种认证方式下，网络准入设备辅助客户端软件与准入服务器进行认证。

- 实现用户权限控制

  网络准入设备科监控用户认证过程，根据准入服务器给出的结果，给用户授予相应权限：

  - 终端认证前具有认证前域的访问权限，可以访问准入服务器、公用软件服务器进行终端代理安装等操作。
  - 安全隔离的终端具有隔离域的权限，可以访问病毒服务器、补丁服务器等。
  - 终端认证通过后具有认证后域的网络权限，不同的用户角色可以授予不同的网络权限。

3.4 准入服务器

准入服务器包括准入控制服务器、管理服务器、病毒库服务器和补丁服务器。

- 准入控制服务器主要进行用户认证和安全审核，实施安全策略，并且与网络准入设备联动，下发用户权限。
- 管理服务器主要进行用户管理，包括增加、删除、修改用户权限及用户部门配置，及安全策略的定制和管理等。
- 病毒库服务器主要用于控制各种终端上的防病毒软件的病毒库的自动更新。
- 补丁服务器主要用于控制各种终端上的操作系统和应用软件的补丁安装和更新。

4 典型应用组网

4.1.1 接入层认证方案规划建议

4.1.2 应用场景

认证控制点越贴近终端，权限的控制粒度便越细，安全性也越高。因此接入层是部署网络安全控制的最佳点，可以直接将非法用户在接入层隔离，阻止其危害整网安全。

在接入层认证方案中：

- 对于有线用户，可以在接入层交换机上部署 802.1X+MAC 混合认证。这种认证方案需要接入层交换机支持 802.1X 认证协议，适用于新建网络或现网改造中需要增加身份认证又不希望改变当前网络中已有安全部署的场景。
- 对于无线用户，可在 AC 上部署 802.1X 认证，无线用户通过 802.1X 认证接入网络。

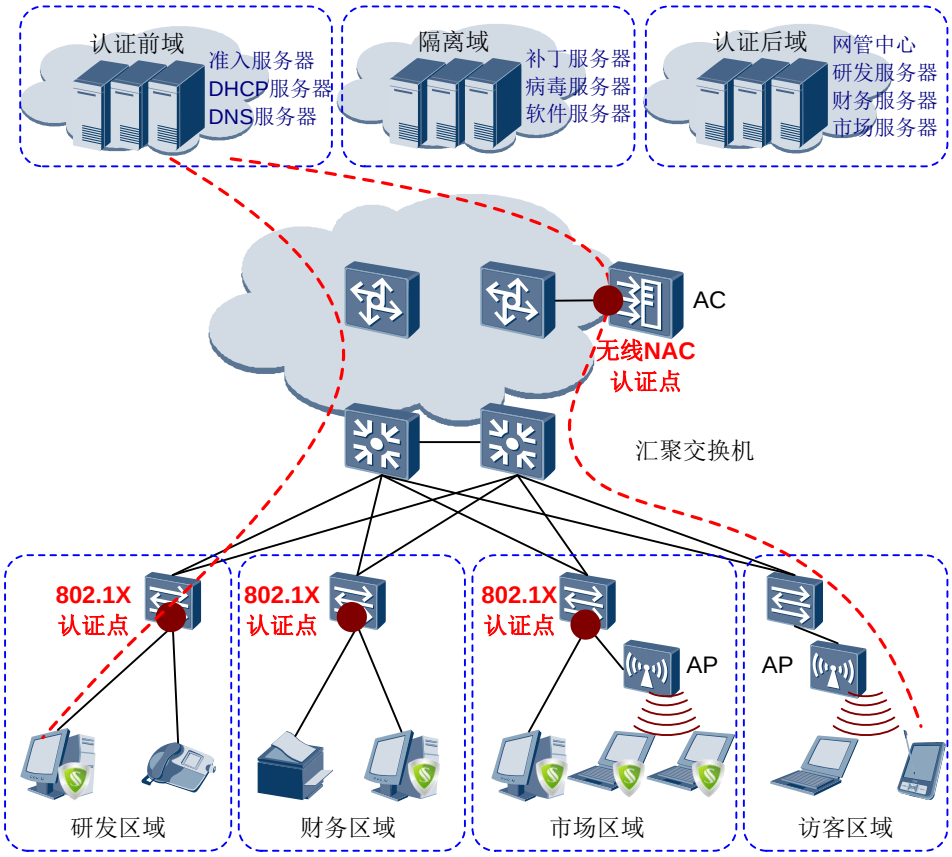
本方案适用于大、中、小型园区，特别是用户对安全控制要求较高的场景。

4.1.3 组网规划

接入层认证方案采用传统的三层网络结构，接入层交换机部署 802.1X 认证或 MAC 认证，对接入用户进行身份认证，隔离非法用户和不安全用户。

服务器区域一般分为认证前域、隔离域和认证后域三部分，除了部署传统的业务服务器、网络管理服务器、DHCP/DNS 服务器外，还需要部署准入服务器以及补丁、病毒服务器。如图 4-1 所示。

图4-1 接入层认证方案组网图



4.2 汇聚层认证方案规划建议

4.2.1 应用场景

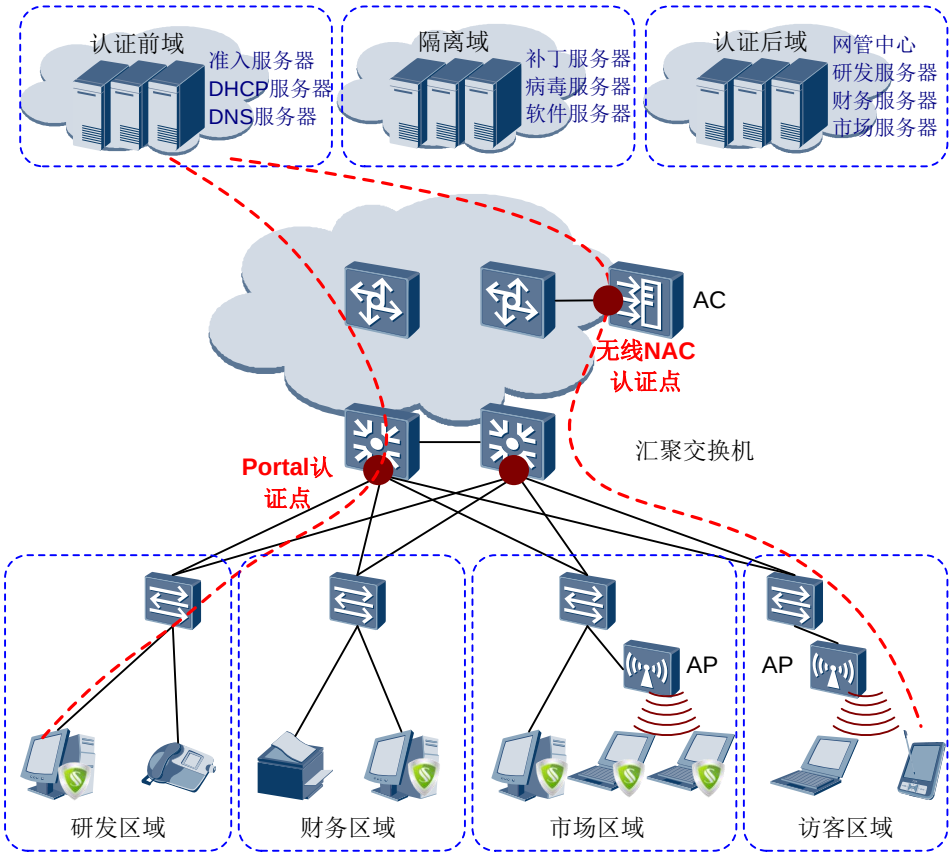
汇聚层部署认证控制点适用于接入用户分散，接入终端类型较多，无线有线混合接入的场景，认证协议建议采用基于网关的 Portal 认证。

这种认证方式与接入层设备无关，终端设备既可以安装代理客户端，也可以不安装（Web 强推方式），适应各种终端接入（PC、手持设备等），方便灵活，管理维护方便。旧网改造中若需要增加安全接入控制功能，而又不希望改变原来网络结构，可以直接在汇聚层部署 Portal 认证。

4.2.2 组网规划

汇聚层认证方案采用传统的三层网络结构，在汇聚层交换机基于网关部署 Portal 认证，对接入的用户进行身份认证，隔离非法用户和不安全用户。汇聚交换机上配置 ACL 或 ACL 组，准入服务器下发 ACL 号或 ACL 组名来控制访问权限。服务器区除了部署传统的业务服务器、网络管理服务器、DHCP/DNS 服务器外，还需要部署准入服务器以及补丁、病毒服务器。如图 4-2 所示。

图4-2 汇聚层认证方案组网图



4.3 无线用户 AC 集中认证方案规划建议

4.3.1 应用场景

WLAN 网络的部署可以分为自治式架构（FAT AP 架构）和集中式架构（FIT AP 架构）。企业级用户的管理由于用户较多且分散，一般采用集中式架构。

华为集中式 WLAN 部署方案可以提供将 AP 及无线用户统一管理，能为无线用户提供认证和授权，保障无线用户接入的安全。同时，同一 AC 下的用户能漫游，为移动中的用户提供良好的体验。

此方案的优点在于：

- 无线用户在 AC 上集中认证，可以保证无线用户集中管理。
- AC 将授权信息通过控制隧道下发到 AP 设备，精细化控制用户访问权限。
- 用户漫游、安全策略等由 AC 进行灵活控制。

4.3.2 组网规划

无线用户 AC 集中认证方案可采用二层组网或三层组网方式。一般而言，在大、小型园区都采用三层组网方式。

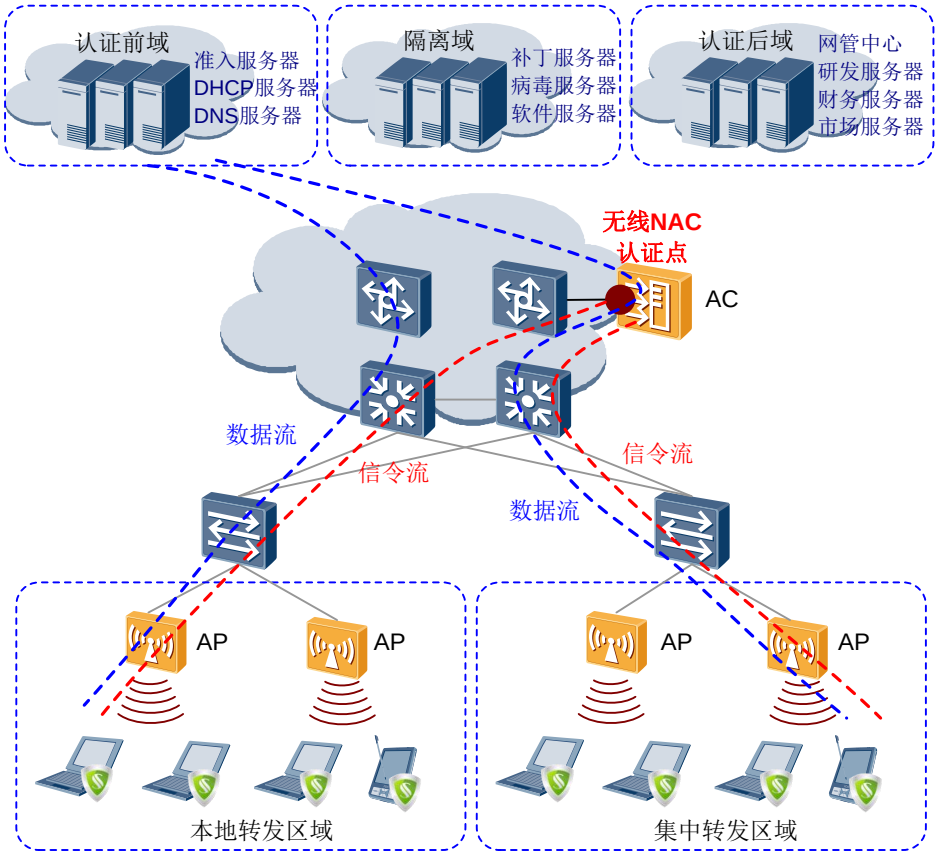
AP 的转发模式可以采用集中转发模式和本地转发模式两种。

- 采用集中转发模式时，WLAN 管理报文与数据报文都通过 CAPWAP 隧道在 AP 与 AC 之间传输。
- 采用本地转发模式时，仅管理报文通过 CAPWAP 隧道在 AP 与 AC 之间传输，数据报文由 AP 直接进行转发。

说明

在 AP 进行本地转发时，可以通过配置使让 EAP、Portal 报文进入 CAPWAP 控制隧道，从而上送到 AC 设备，完成认证过程。

图4-3 无线用户 AC 集中认证方案组网图



5 产品建议

对于 NAC 安全方案所涉及的各节点和网元，华为公司推荐使用的产品如下：

表5-1 部件产品建议表

部件	产品/型号
接入交换机	S1700、S2700、S3700、S5700
汇聚交换机	S5700、S6700、S7700
核心交换机	S7700、S9700
WLAN AC	S7700 AC 插卡、S9700 AC 插卡、AC6605
WLAN AP	AP6010、AP6310、AP6510、AP6610
接入路由器	AR150、AR200、AR1200、AR2200、AR3200
Server 端软件	TSM Server
Client 端软件	TSM Agent
AD服务器	Windows 2008 Server