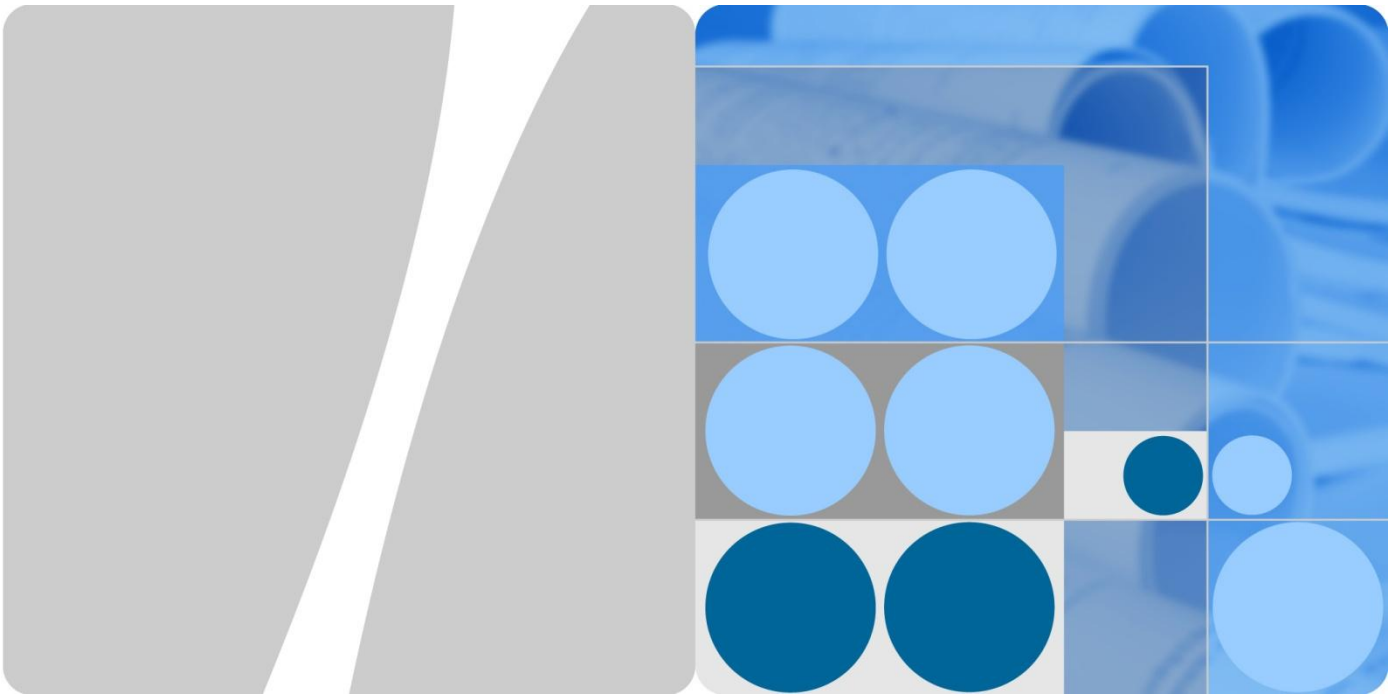


NAC 安全解决方案

技术建议书

文档版本 01

发布日期 2011-06-24

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默示的声明或保证。

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://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

目 录

1 NAC 安全方案概述

1.1 方案背景

1.1.1 企业网络安全概述

随着企业网络的应用和发展，企业生产和经营活动对于网络的依赖性不断增强。但病毒、木马、间谍软件、网络攻击等各种信息安全威胁也在不断增加。统计表明，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点。

在传统的企业网络建设思路中，一般认为企业内网是安全的，而安全威胁主要来自外界。因此各种安全措施基本上都围绕着如何抵御外部的攻击来部署，如部署防火墙、访问控制系统等，并且这些产品和技术在工作上一般都互相独立，不能协同工作。

但是研究证明，许多重大的网络安全问题是在企业内网中引发的。80%的网络安全漏洞都存在于网络内部，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。而内部员工在浏览某些网站时，一些间谍软件、木马程序等恶意软件也会不知不觉地被下载到电脑中，并且在企业内网传播，产生严重的安全隐患。

因此，随着安全挑战的不断升级，仅通过传统的安全措施和独立工作的形式进行边界防御已经远远不够了，安全模型需要由被动模式向主动模式转变，从根源－终端彻底解决网络安全问题，提高整个企业的信息安全水平。

1.1.2 企业内网的主要安全问题

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。另外，大量非法接入和非授权访问的状况，将导致企业业务系统的破坏，以及关键信息资产的泄漏。

从安全角度来分析，目前大部分的企业内部网络中，主要存在如下一些安全问题：

防病毒软件未实现集中管理

对于感染病毒和木马的终端无法进行控制其访问，只能通过管理手段要求员工对终端进行杀毒。并且该工作是事后的工作，当一个未知病毒大面积爆发时有可以造成整个网络无法使用，对网络的安全稳定运行造成非常大的影响。

补丁管理混乱

各终端不打、漏打系统补丁状况严重，而且没有办法强制安装，导致一旦某台终端感染病毒或恶意代码，则很快就会在内网泛滥。

企业安全策略实施困难

员工安全意识薄弱，员工私自安装不合法软件，或者通过调制解调器、ISDN 拨号设备、ADSL 拨号设备、无线网卡等网络设备非法接入互联网，给网络的安全性等带来了极大的隐患。而企业的安全系统无法这些情况进行检测和控制，难以实施有效的安全策略。

缺乏系统的监控审计能力

企业安全系统无法实时监控系统安全状态，无法对员工网络访问行为、非法外联行为、USB 存储设备使用等行为进行审计并上报安全策略服务器，缺乏事后安全审计的手段。

1.2 主要需求

随着企业规模不断扩张，员工及终端数量剧增，网络复杂度也呈几何级增长。如何有效的管理网络，如何更及时的更新系统补丁、升级病毒库，如何让管理员更快捷的查找、隔离及修复不安全的终端，是企业网络安全的主要目标。

企业网络安全方案应能满足身份鉴别、安全性检查、用户授权和安全域划分等需求。

1.2.1 身份鉴别

由于终端问题导致的企业内网问题日益增多，能够对用户进行身份鉴别是对企业网络安全的基本需求。

- 普通的终端（例如 PC 等）用户的身份鉴别应满足如下需求：
  - 符合安全要求的终端提供正确的用户名和密码后，可以正常接入网络。
  - 不符合安全的终端，只能接入到网络隔离区，待终端安全修复后才能接入网络。
  - 不合法的用户不允许接入网络。
- 对于其他终端类型（包括打印机、传真机、IP 电话等），虽然无法通过安装终端软件接入验证合法性，但需要可以通过 MAC 地址进行验证。

1.2.2 安全性检查

由于终端隐患对网络危害极大，因此在企业网络安全方案中，除了对非法用户限制接入外，对合法用户也应进行系统的安全检查。安全性检查应满足如下需求：

- 对入网终端的安全性（杀毒软件安装、补丁更新、密码强度、屏保等）进行扫描，在接入网络前完成终端安全状态的检查。
- 对终端不安全状态能够与控制设备进行联动，当发现不安全终端接入网络的时候，能够对这些终端实现一定程度的阻断，防止这些终端对业务系统的危害，并能够主动帮助这些终端完成安全状态的自修复。

- 对于未能及时修复的不安全终端，能够对其进行权限限制，避免接入网络，引发网络安全问题。

1.2.3 用户授权

目前的企业内网对网络资源的访问控制比较薄弱，只要用户接入网络，就能够自由的访问整个网络。而一般的防火墙隔离只能基于 IP 地址进行控制，不仅配置管理不够灵活，而且还存在 IP 被仿冒等安全风险，无法彻底解决非法接入和越权访问的问题。

因此企业网络安全方案中，需要结合终端用户的身份认证，基于用户角色来对网络访问权限进行管理，不但可以加强内网的网络访问控制，也可以防止非法接入和非授权访问，保证企业内网的安全。

1.2.4 安全域划分

管理员根据业务和安全等级将现网的网络资源划分为不同的逻辑安全域，系统根据终端用户身份认证和安全检查的结果开放不同安全域的访问权限，实现对违规终端的隔离，保证企业内网的整体安全性。安全域的划分如表 1-1 所示。

表1-1 安全域的划分

类型	描述
认证前域	终端在身份认证和安全检查通过前能够访问的网络资源，包括DHCP服务器、系统服务器等。
隔离域	终端在通过身份认证但没有通过安全检查时处于被隔离状态，此时仅能够进行安全修复操作，包括防病毒软件病毒库升级服务器、补丁服务器等。
认证后域	终端在通过身份认证和安全检查后能够访问的网络资源，管理员可根据工作相关性和最小授权原则，将不同的终端用户授权访问相应的网络资源，有效防止非法访问和越权访问

企业网络安全方案中，对于安全域的划分应满足如下需求：

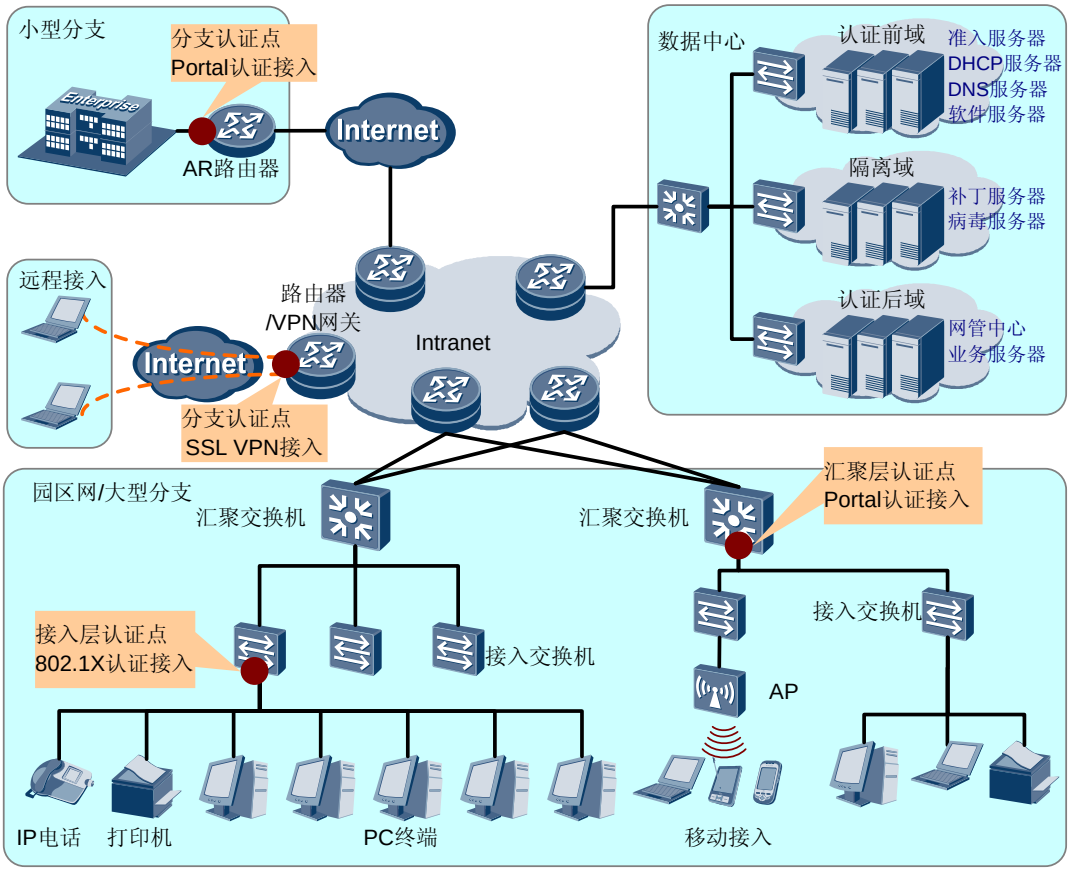
- 普通终端正确接入网络后，能获取有效的公共区域权限及部门权限。并且用户位置迁移后，则需仍能获取自身的网络权限。
- 无线用户正确接入网络后，能够像有线用户一样拥有合法的网络权限。非法的无线用户在本区域将被拒绝接入网络。
- 新用户接入需要有默认权限，出差员工接入网络，都应能进行相应权限限制。
- 对于网络中的打印机、传真机、门禁以及语音视频终端，需按照业务类别给予相应的权限，防止信息口盗用给网络带来的安全问题。
- 能够对终端和终端之间的互相访问进行控制。在终端认证前，限制各终端直接的访问，只能访问策略配置的服务器资源；在终端认证后，采用可信互访的方式，只有认证通过的代理终端才能互相访问。

1.3 华为的 NAC 安全解决方案

华为的 NAC（Network Access Control）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，提供以“用户认证、安全检查、修复升级”为基础的一体化终端安全防护功能。可帮助企业构建一个安全网络，保证企业业务的正常开展和进行。

华为的 NAC 安全解决方案，从接入网络的终端安全控制入手，将终端安全状况和网络准入控制结合在一起，通过检查、隔离、加固和审计等手段，加强网络用户终端的主动防御能力，保证企业中每个终端的安全性，保护企业网络的安全性。如图 1-1 所示。

图1-1 NAC 解决方案示意图



华为的 NAC 安全解决方案包括如下内容：

- 通过多种身份认证方式确认终端用户的合法性。
- 绑定检查终端的安全漏洞、终端杀毒软件的安装和病毒库更新情况。
- 通过统一接入策略和安全策略管理，控制终端用户的网络访问权限。
- 通过桌面运维，完成进行桌面资产注册和监控、外设管理和软件分发。

2 NAC 安全方案规划建议

2.1 概述

2.1.1 NAC 安全方案简介

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。

身份认证和访问控制

NAC 方案可以对接入网络的用户身份进行合法性进行认证,只有合法用户才允许接入，并且不同的角色，不同的用户所能够访问的资源是不同。

管理员可以为用户分组，或者定义不同的角色，配置不同的资源，使得特定的用户只能访问授权的特定资源，禁止访问未授权的网络资源。

接入安全检查和控制

NAC 方案可以对用户终端的安全性进行检查，只有“健康的、安全的”用户终端方可接入网络。企业网络管理人员可以自定义企业网络安全规则和策略，比如终端必须安装启动防病毒软件、病毒库必须是最新的，终端系统不得安装违规软件，必须安装系统补丁等等。

系统修复与升级

如果系统存在安全隐患，华为 NAC 方案提供了系统自动和手动的修复升级功能。支持与 WSUS（Windows Server Update Services）的联动，可自动下载和升级系统补丁；提供与商业防病毒软件的强联动，触发病毒谱的更新；可自动杀死非法/违规进程等强制安全措施。

丰富的扩展特性

华为 NAC 解决方案，还提供行为管理、软件分发、资产管理等等扩展功能。

- 行为管理

TSM 提供基于终端的员工行为管理功能，目的在于提醒终端用户在使用终端主机时遵守企业制定的行为规范，通过规范员工的行为来提高内网安全管理的能力。

- 软件分发

  TSM 提供软件分发功能，将软件手工或按计划自动分发到相应的终端主机上，并支持按部门、按操作系统进行分发。

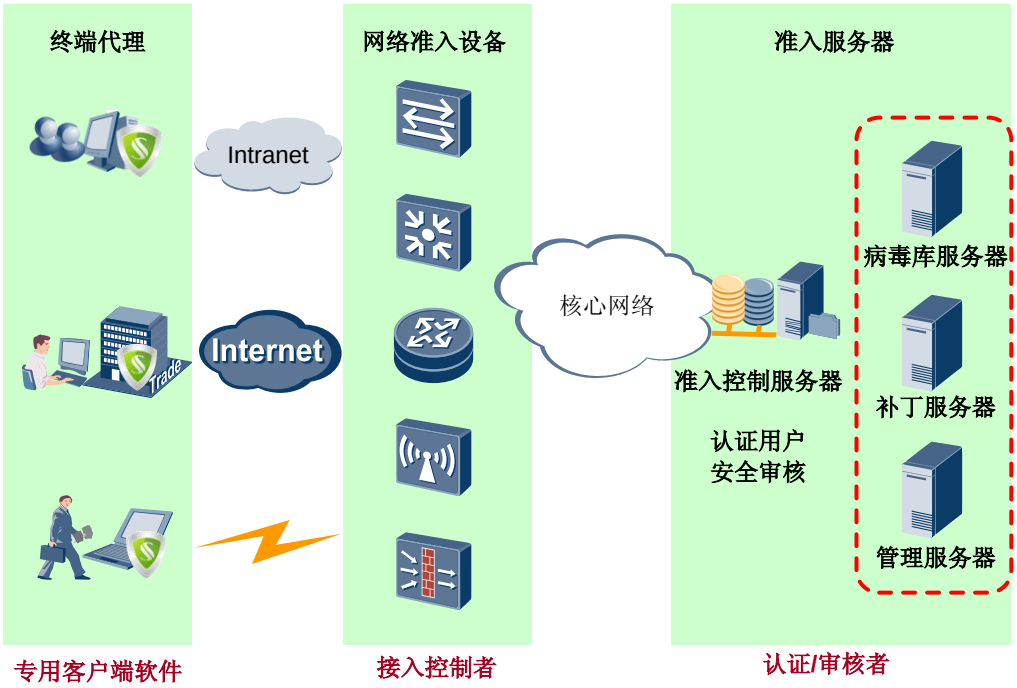
- 资产管理

  TSM 提供资产管理功能，统一管理企业资产，提高效率，降低维护成本，避免员工私自更改企业终端主机的配置，降低资产遗失的风险。

2.1.2 NAC 系统组成

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 2-1 所示。

图2-1 NAC 系统组成部件示意图



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。

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。

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。

2.1.3 NAC 系统业务能力

NAC 安全方案可提供接入认证、权限控制、终端管理、攻击防御、资产管理等功能，并具有高可靠性、执行灵活、融合开放等特点。

提供多种认证方式

- 提供基于接入层、汇聚层不同的认证方案，适合大型园区网使用。
- 提供 802.1x 认证，Portal 认证，MAC 认证，强推 web 认证，AD/LDAP 联动认证等多种认证方式，与域认证联合，只需一次认证。
- 支持多种终端部署，包括 PC 终端、非 PC 终端、无线终端及 IP 电话等。
- 提供 Agent 客户端，无 Agent 的 ActiveX 插件。

丰富的安全控制

- 支持基于用户及端口下发 ACL，基于限定用户的访问权限。
- 能够根据用户安全状态进行权限限制。
- 提供完善的一键智能修复功能。

完善的终端管理方案

- 提供组织人员管理，策略管理，行为监控，补丁管理等功能。
- 提供业界最丰富的安全策略，可根据用户需要定制。
- 提供丰富的用户行为审计功能，包括 USB 设备监控，非法外联管理，进程与服务监控等。

攻击防御

- 支持阻止从终端主机发出 ARP 欺骗报文。
- 支持阻止从终端主机发出 ARP 泛洪报文。
- 提供 ARP 地址静态绑定功能。

高效的资产管理功能

- 提供资产注册、资产生命周期管理、资产统计、变更告警等丰富的资产管理功能。
- 提供服务器平台监控，公告及远程协助功能便于用户管理。

高可靠性

- 提供 RADIUS 服务器备份及 Portal 服务器备份，可靠性高。
- 提供双机热备、双机冷备、单点逃生等功能。

灵活方便的执行界面

- 提供功能完备，简单易用的操作界面。
- 便捷的安装模式，一次安装，按需购买 License。

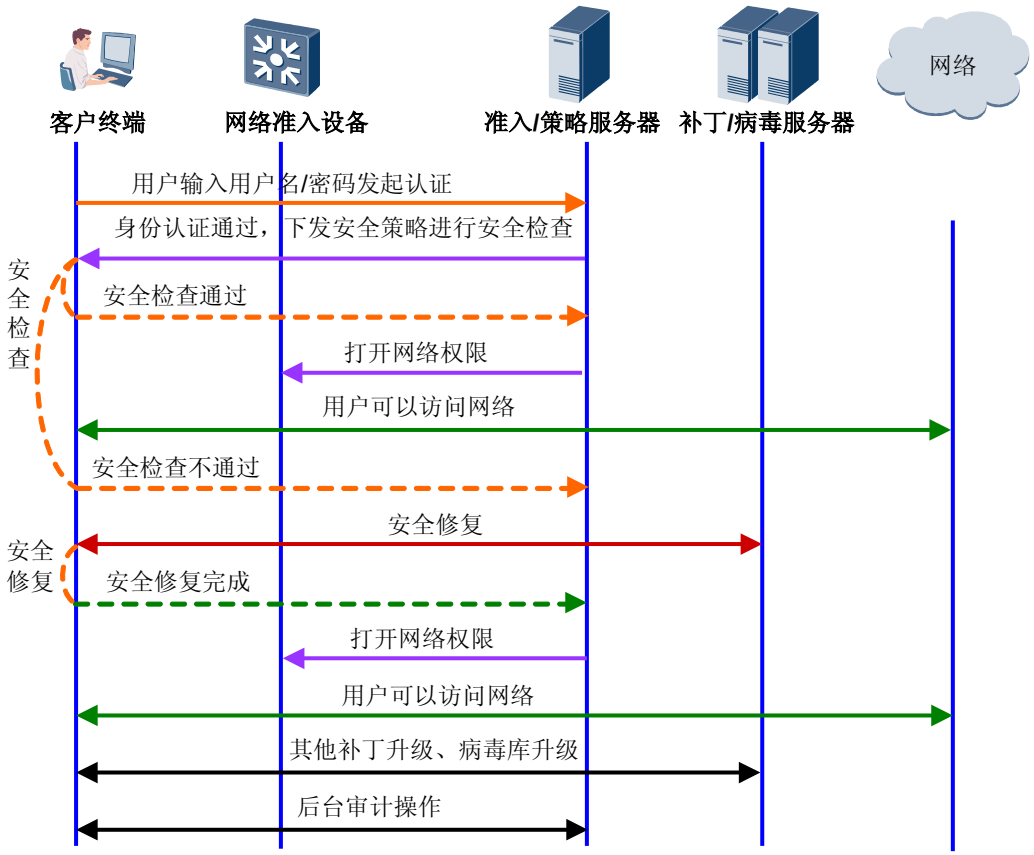
丰富灵活、融合开放的解决方案

- 实现了集中统一的认证、授权管理。
- 充分利用已有的网络安全建设，将各个孤立的解决方案实现最佳的融合。
- 灵活丰富的安全检查，包含了业界最多的终端安全检查策略，并且在用户访问的整个过程当中都可以进行检查。
- 业界一流的高安全性，在系统管理方面，采用基于管理角色的操作权限控制，并记录管理员的操作日志保证提高操作安全性和可追溯性。
- 优异的高可靠性，重要组件均提供主备和负载均衡，提供独有的逃生通道功能。
- 支持 Windows 系统的软件安装，并提供认证配合 Windows 域联合进行认证。

2.1.4 NAC 安全方案基本流程

结合终端代理、网络准入设备、准入服务器各个组件，NAC 方案的基本流程如图 2-2 所示。

图2-2 NAC 方案基本流程



详细流程说明如下：

1. 客户端接入网络，认证前都具有认证前域网络权限，可以根据需要进行认证前的访问等操作。

2. PC 客户端安装终端代理软件或 Web Agent 插件，用户输入用户帐号和密码发起身份认证，身份认证通过后，终端代理软件或 Web Agent 插件与准入服务器联动检查终端安全状态。
3. 对合法并安全的用户，身份认证后，准入服务器下发网络权限到网络准入设备，允许该用户访问认证后域网络。
4. 对合法但存在较低安全风险的用户，身份认证后，准入服务器下发网络权限到网络准入设备，允许该用户访问认证后域网络，同时提示终端安全风险。
5. 对合法但严重不安全的用户，身份认证后，准入服务器下发隔离域网络权限到网络准入设备，仅允许该用户访问隔离域网络，用户此时可访问隔离域内的补丁病毒服务器，用户安全修复后，重新下发网络认证后域的网络权限。
6. 支持用户在线实时安全状态检查，上线用户使用过程中出现严重安全问题，仍会被隔离。
7. 用户认证后可以根据需要打补丁，病毒库升级可以访问相关服务器进行升级。
8. 后台策略服务器可以对用户进行后台审计操作。
9. 非法用户及未认证用户仅允许访问认证前域网络资源。

2.2 认证方案规划建议

2.2.1 认证协议简介

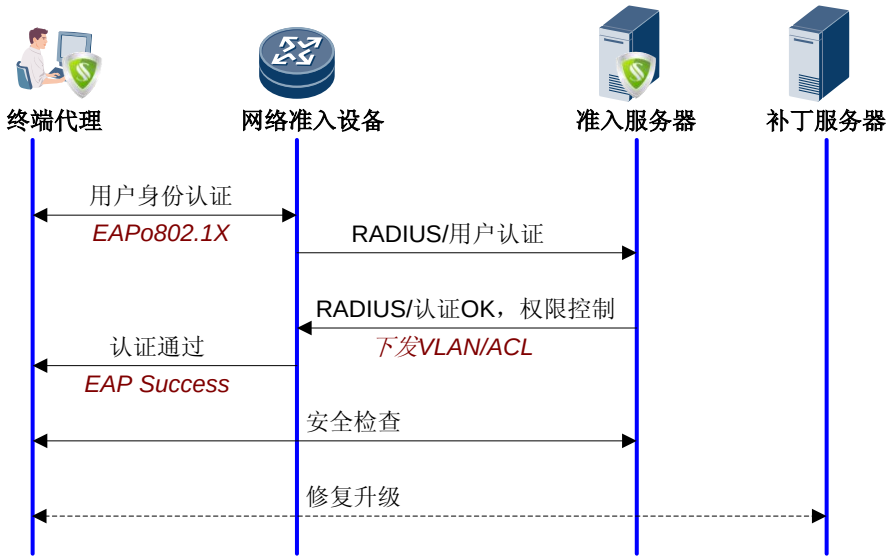
华为公司 NAC 方案，支持 802.1X、MAC 认证、Portal 认证多种网络访问控制方式，并可灵活部署在用户网络的接入交换机、汇聚交换机、无线控制器、AR 等多种网络设备上，配合 NAC 的代理客户端和服务器共同完成 NAC 控制，为企业网、园区网、城域网提供安全可靠的访问控制。

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。

图2-3 802.1X 认证流程图



详细的流程说明如下：

1. 用户终端接入网络，终端代理与网络准入设备通过 EAP 交互帐号和密码信息。
2. 网络准入设备与准入服务器通过 RADIUS 协议，对终端用户身份合法性进行认证。
3. 用户认证通过后，准入服务器通过 RADIUS 协议告知网络准入设备，同时下发用户接入的 VLAN ID 或对应的 ACL，实现对认证后合法终端用户的访问控制。
4. 网络准入设备通过 EAP Success 消息通知用户终端。
5. 终端代理与准入服务器交互终端系统安全状态信息，对用户终端的进行安全检查。
6. 如果用户终端不安全，终端代理启动系统修复升级工作，与相关服务器（补丁、病毒库等）交互，完成系统的安全修复。

当客户网络由于特殊的情况，不能在底层接入交换机上部署 802.1X 协议时，或者接入交换机下挂 HUB 接入多个用户终端的情况下，标准的基于端口的 802.1X 协议就无法实现对各个终端的单独访问控制。

华为针对上述问题，在交换机、路由器上对标准 802.1X 协议进行了功能增强，实现了基于 MAC 的 802.1X 访问控制，可实现当单端口接入多用户终端时，针对具体单个终端的访问控制。华为的 NAC 方案中同时支持基于端口和基于 MAC 的 802.1X 访问控制，用户网络可以有针对性的选用。

- 基于端口模式：当采用基于端口方式时，只要该端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源。但是当第一个用户下线后，其他用户也会被拒绝使用网络。
- 基于 MAC 模式：当采用基于 MAC 地址方式时，该端口下的所有接入用户均需要单独认证。

在用户终端的访问控制方面，可以通过下发 VLAN 或下发 ACL 方式（也可以两者同时使用）。根据控制方式的不同，802.1X 认证可进一步细分为基于 Guest VLAN 的 802.1X 认证和基于 ACL 的 802.1X 认证。

- 基于 Guest VLAN 的 802.1X 认证

这是业界最常用的 802.1X 认证方式，用户认证前缺省归属 Guest VLAN，认证通过后准入服务器下发用户认证后的相应角色 VLAN 号，将用户终端从 Guest VLAN 切入到相应角色 VLAN。

- 基于 ACL 的 802.1X 认证

  该方式下，用户终端认证通过后，准入服务器仅下发用户 ACL 实现针对该用户的访问控制。该方式在大用户量情况下，对设备 ACL 规格要求较高。

另外，准入设备首先触发用户采用 802.1x 认证方式，如果用户长时间内没有进行 802.1X 认证，则以用户的 MAC 地址为认证信息，把 MAC 地址作为用户名和密码上送服务器进行认证。此种认证方式被称为 MAC 旁路认证。

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。

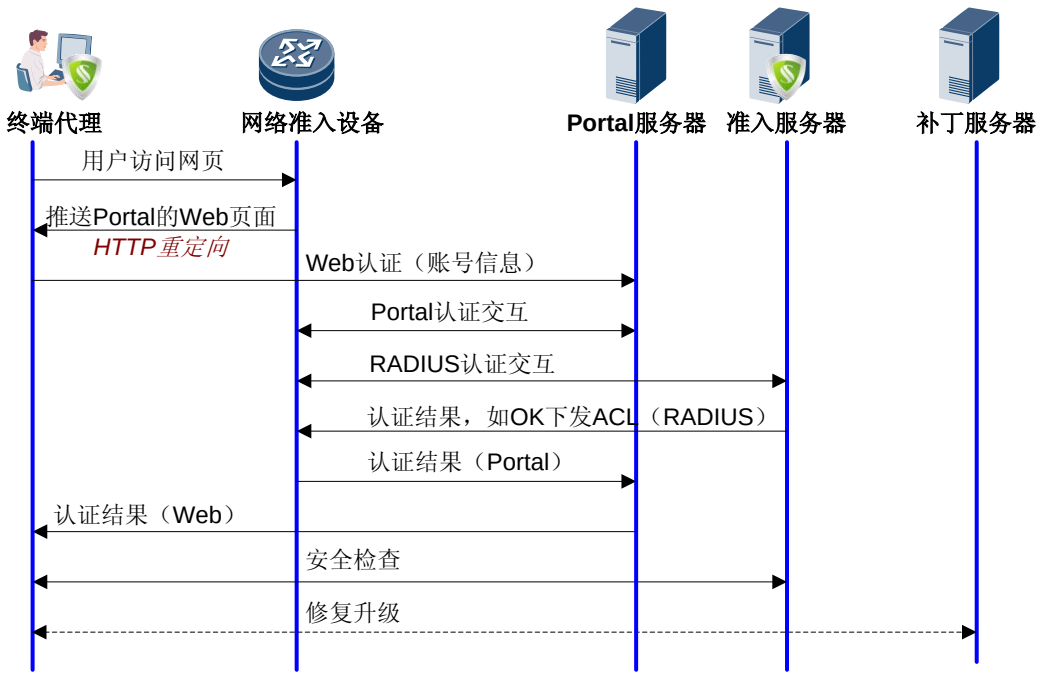
Portal 认证支持 Web 认证且可以无需安装客户端软件，这两个特性使得 Portal 认证对于访客和出差用户具有很好的支持。

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。

在 Portal 的 Web 认证前，用户首先要访问认证页面，在认证页面输入帐号和密码，然后提交。用户访问认证页面的过程，可以采用主动访问页面和被动访问页面即强推的方式来实现。

图2-4 Portal 认证流程图



详细的流程说明如下：

1. 用户终端访问任意 Web 服务器。
2. 网络准入设备截获用户 HTTP 请求，如果非 Portal 服务器，通过 HTTP 重定向命令推送 Portal 的 Web 认证页面。
3. 用户终端访问 Portal 服务器 Web 认证页面，输入帐号/密码，提交认证。
4. Portal 服务器与网络准入设备通过 Portal 协议交换用户帐号信息。
5. 网络准入设备通过 RADIUS 协议，向准入服务器（RADIUS 服务器）进行用户认证。
6. 准入服务器进行用户身份认证，并反馈认证结果。如果认证通过，一并下发用户 ACL。
7. 网络准入设备收到 RADIUS 认证结果，通过 Portal 协议告知 Portal 服务器。如果认证成功，放开用户上网权限，并启动 ACL 实现该用户的网络访问控制。
8. Portal 服务器向用户终端通过 HTTP 通知认证结果。
9. 用户终端下载安装 ActiveX 控件（或安装了客户端代理软件），认证通过后，终端代理将与准入服务器进行安全状态信息交互，实现对终端用户的安全性检查。
10. 如果用户终端不安全，终端代理启动系统修复升级工作，与相关服务器（补丁、病毒库等）交互，完成系统的安全修复。

说明

华为 NAC 方案中，Portal 服务器与准入服务器已经集成，可以是部署在同一个物理服务器上的不同功能模块。

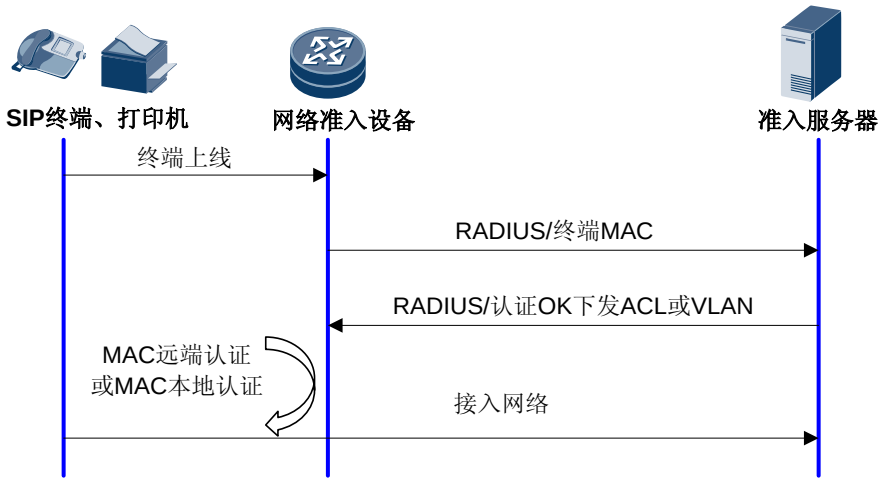
MAC 认证

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。

图2-5 MAC 认证流程图



MAC 认证的详细流程如下：

1. 终端设备上线，网络准入设备自动提取终端 MAC 地址。
2. 网络准入设备对终端设备 MAC 地址进行认证：
   - 如果采用 RADIUS 认证，网络准入设备将终端设备 MAC 地址作为帐号和密码，通过 RADIUS 协议送准入服务器认证。
   - 如果采用本地认证，网络准入设备在本地配置的 MAC 认证表中对终端设备 MAC 地址进行认证。
3. 认证通过后，打开该终端设备的上网权限。如果 RADIUS 认证，采用 RADIUS 下发的 ACL 或 VLAN 对终端设备进行权限控制。

三种认证方式比较

802.1X 认证、Portal 认证和 MAC 认证的优劣势比较如表 2-1 所示。

表2-1 认证方式对比

对比项	802.1X 认证	Portal 认证	MAC 认证
客户端需求	必须	Portal 需要，web 强推不需要	不需要
优点	部署在接入层时，直接控制网络接入信息口的通断，安全性高	部署灵活	无需安装客户端
缺点	部署不灵活	安全性不高	管理复杂，需登记 MAC 地址
适合场景	新建网络，用户集中，信息安全要求严格的场景	认证方式灵活，适用于用户分散，无线场景	适用于 SIP 终端，打印机，传真机等终端接入认证的场景

2.2.2 认证方式和认证控制点选择

如“2.2.1 认证协议简介”所述，目前可选用的认证方式包括 802.1X 认证、Portal 认证和 MAC 认证。

而从认证控制点的部署选择来看，有接入层部署认证控制点、汇聚层部署认证控制点、以及路由器/VPN 网关上部署认证控制点。

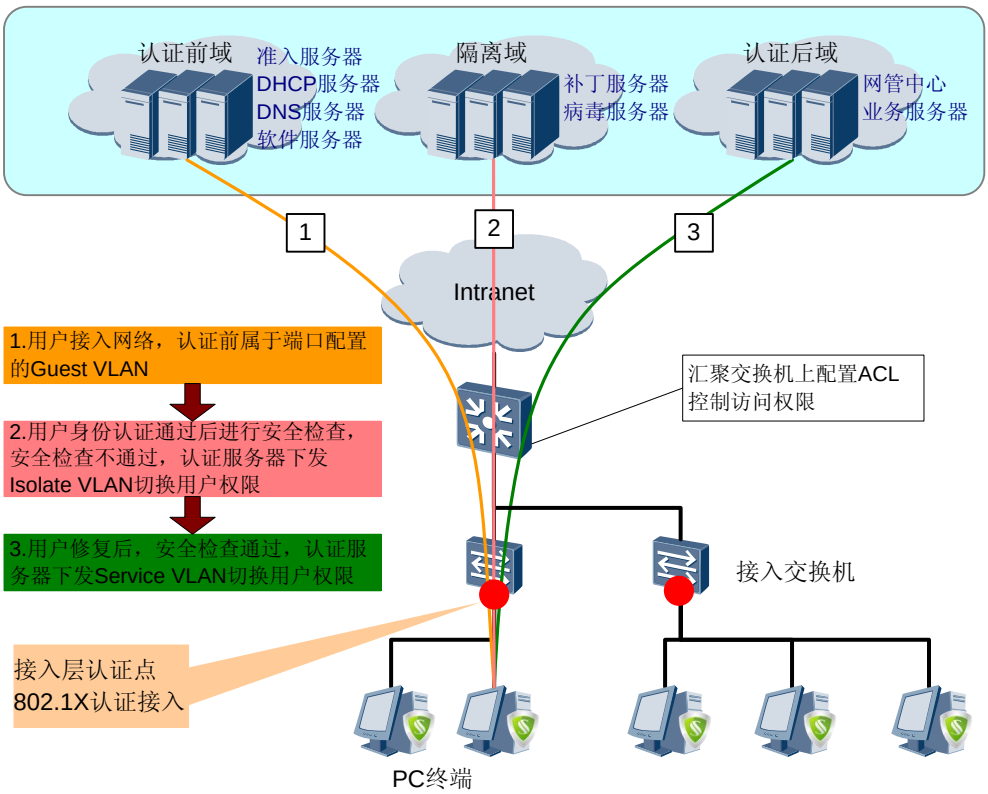
接入层部署认证控制点

在接入层部署认证控制点，建议使用 802.1X 认证，如图 2-6 所示。

- 认证前所有用户在 Guest VLAN 中。
- 认证通过后由认证服务器下发 Service VLAN，切换用户域。
- 不安全用户下发 Isolate VLAN 隔离。
- 用户权限控制在汇聚交换机上针对不同的 VLAN/网段配置实现。

此种认证方式部署简洁，控制点离用户最近，内网得到最大的安全保障，适合大部分新建或网络设备比较新的园区网络，但认证点较多，给管理维护带来困难。

图2-6 接入层部署认证控制点



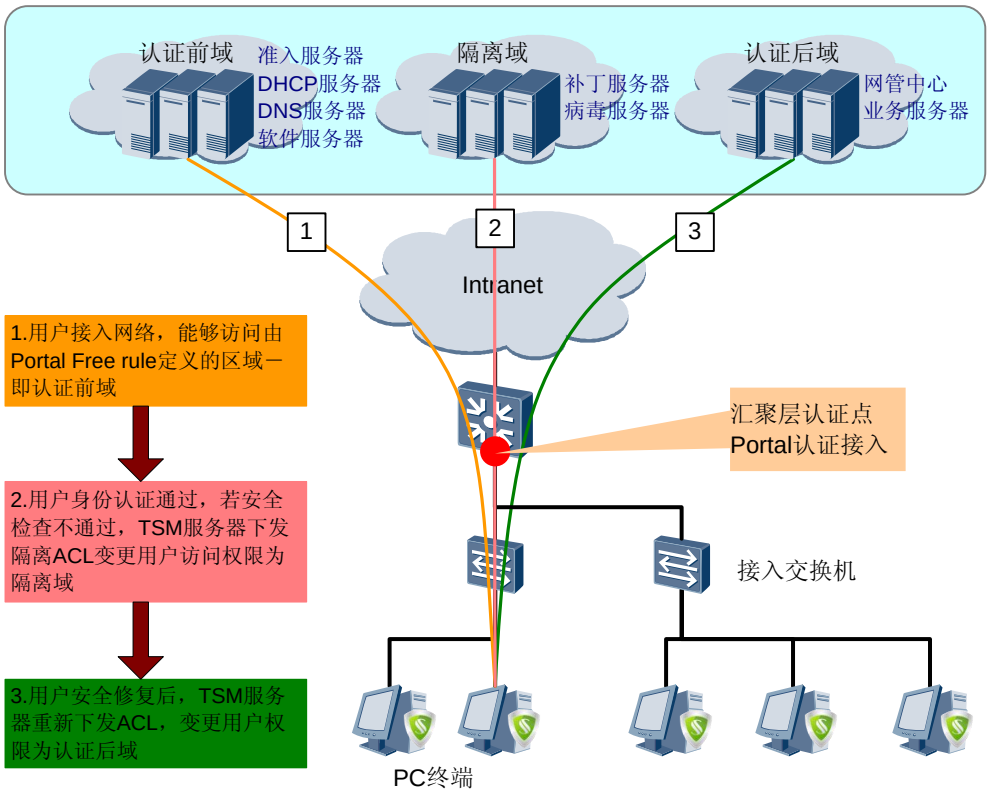
汇聚层部署认证控制点

在汇聚层部署认证控制点，建议使用 Portal 认证，如图 2-7 所示。

- 用户认证前域由 Portal Free Rule 限定。
- 认证通过后认证服务器下发 ACL 切换用户权限。
- 不安全用户也是由服务器下发 ACL 隔离。

此种方式认证点少，适应各种用户接入，方便灵活，管理维护方便，适合用户分散，无线有线混合接入的场合，还适用于旧网改造中增加网络安全接入控制，而又不改变原来网络结构的场景。为解决用户接入层互访带来的网络安全问题，可在接入交换机上配置端口隔离，DHCP Snooping 等安全功能。

图2-7 汇聚层部署认证控制点



路由器/VPN 网关部署认证控制点

路由器/VPN 网关部署认证控制点一般用于远程移动办公人员的接入认证控制。通常采用 Portal 认证，具体的部署方式与汇聚层的认证控制点部署类似，此处不再详述。

2.3 接入层认证方案规划建议

2.3.1 应用场景

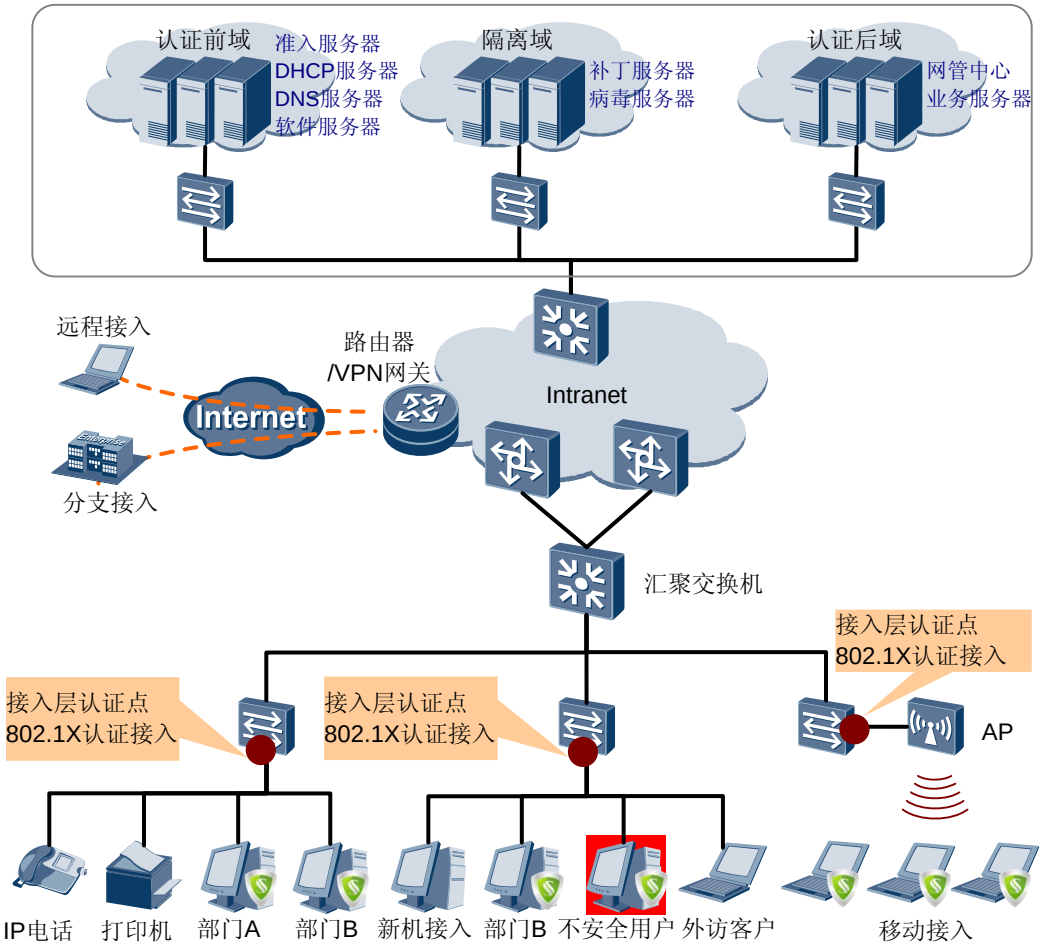
目前的安全解决方案专注于保护网络的第三层及以上。然而，危及第二层安全的任何行为都将会危害到整个网络，因此接入层是部署网络安全控制的最佳点。使用 802.1X 身份认证可以直接将非法用户在接入层隔离，确保接入用户的合法性。

在接入层部署 NAC 方案需要接入层交换机支持 802.1X 认证方式。这种认证方案部署简洁，控制点离用户最近，内网得到最大的安全保障，这种部署方式适用于新建网络，或现网改造中需要增加身份认证而又不希望改变当前网络中已有的安全部署。

2.3.2 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。汇聚交换机上配置 ACL 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 2-8 所示。

图2-8 接入层认证方案组网图



2.3.3 NAC 系统规划

软件系统规划

- 客户端

  PC 安装代理客户端软件，并将软件中的认证模式设置为 802.1x。
- 服务器端

- 认证前域部署准入服务器、DHCP 服务器、DNS 服务器，以及公用软件服务器。
- 隔离域部署补丁服务器、病毒服务器。
- 网络管理服务器及业务系统部署在认证后域。
- 根据网络可靠性级别要求，可部署准入服务器备份。

网络设备规划

- IP 地址

  客户端 IP 地址使用 DHCP 动态获取，用户的静态地址可以通过动态分配不变地址的方法解决。有以下两种方法：
  - 用户申请一次 IP 地址后，在 DHCP Server 上将 IP 与 MAC 绑定，以后此 MAC 的终端上线都分配同样的 IP 地址。
  - 采用 option82 将 IP 地址与用户上线的交换机、交换机端口绑定，以后此端口上线的用户都分配同样的 IP 地址。
- VLAN 规划

  VLAN 可划分为认证前域 Guest VLAN、隔离域 Isolate VLAN、认证后域 VLAN 三类。实际部署时可以按职能部门分配 VLAN，同时预留 Guest VLAN 和隔离 VLAN。
- 域规划

  认证前域、隔离域、认证后域通过 VLAN 规划来区分，各个 VLAN 的访问权限在汇聚交换机上配置 ACL 实现控制。部署中根据实际情况，认证前域和隔离域可以合并为一个域。
- 认证配置
  - 接入层设备作为接入控制点，配置 802.1X 认证，指定 EAP 模式。
  - PC 代理客户端配置 802.1X 认证。
  - 打印机、IP Phone 等终端配置 MAC 认证。
  - 如果即有打印机又有 PC 从端口接入，则可在接入设备上配置 MAC 旁路认证。

2.3.4 安全策略规划

- 准入服务器上可以统一配置安全模板，模板内确定安全检查项目，并制定安全级别，安全级别分为一般及严重。
- 终端 PC 如有一般违规，认证后进入认证后域，准入服务器会下发认证后域的 VLAN 给接入交换机进行权限控制。虽然没有进行权限限制但是终端 PC 会收到违规告警，提示用户尽快进行违规修复。
- 用户的终端 PC 如有严重违规，认证后进入隔离域，终端 PC 的权限会受到控制，并且会收到严重违规告警，提示用户尽快进行违规修复。用户可以通过自动修复按钮进行自动修复。修复成功后用户才能够获取认证后域的权限。
- NAC 系统提供实时进行安全检查，如果终端 PC 重新违规，会触发重新认证进入隔离域，并告警提示。

2.3.5 用户权限规划

- 合法用户权限控制

接入层使用 802.1x 认证，通过认证前后 VLAN 的切换变更用户权限。VLAN 或网段访问权限控制在汇聚层交换机上配置 ACL 实现。

- 不合法用户权限控制

  不合法用户及未认证用户都在接入交换机上被限制访问权限，只能接入到 Guest VLAN 限定的网络。

- 不安全的用户权限控制

  802.1X 认证必须安装代理客户端，准入服务器与终端代理联动对客户端进行安全检查，对于存在不同级别安全风险的终端将会分别对待。

  - 普通的安全违规，如用户未设屏保，共享文件等小风险违规，终端软件将会进行风险提示，但是不会对用户权限进行变更。
  - 如果终端有重大安全违规，如补丁未升级，病毒库未更新等，此类安全隐患如不控制将会对内网造成极大危害，所以此类用户将会被直接划入隔离域，并告警提示用户违规并修复。终端代理软件提供了一键自动修复功能，方便用户进行违规修复，待终端修复后再次进行安全检查，如符合安全策略，代理终端自动进行重认证，获取到认证后域的网络权限。

2.3.6 可靠性规划

- 可以在接入交换机上部署 DHCP snooping，IP Source Guard 等安全特性防止用户间地址盗用、欺骗。
- 还可以绑定用户或客户端到交换机端口，有效限制接入终端和防止终端盗用。

2.4 汇聚层认证方案规划建议

2.4.1 应用场景

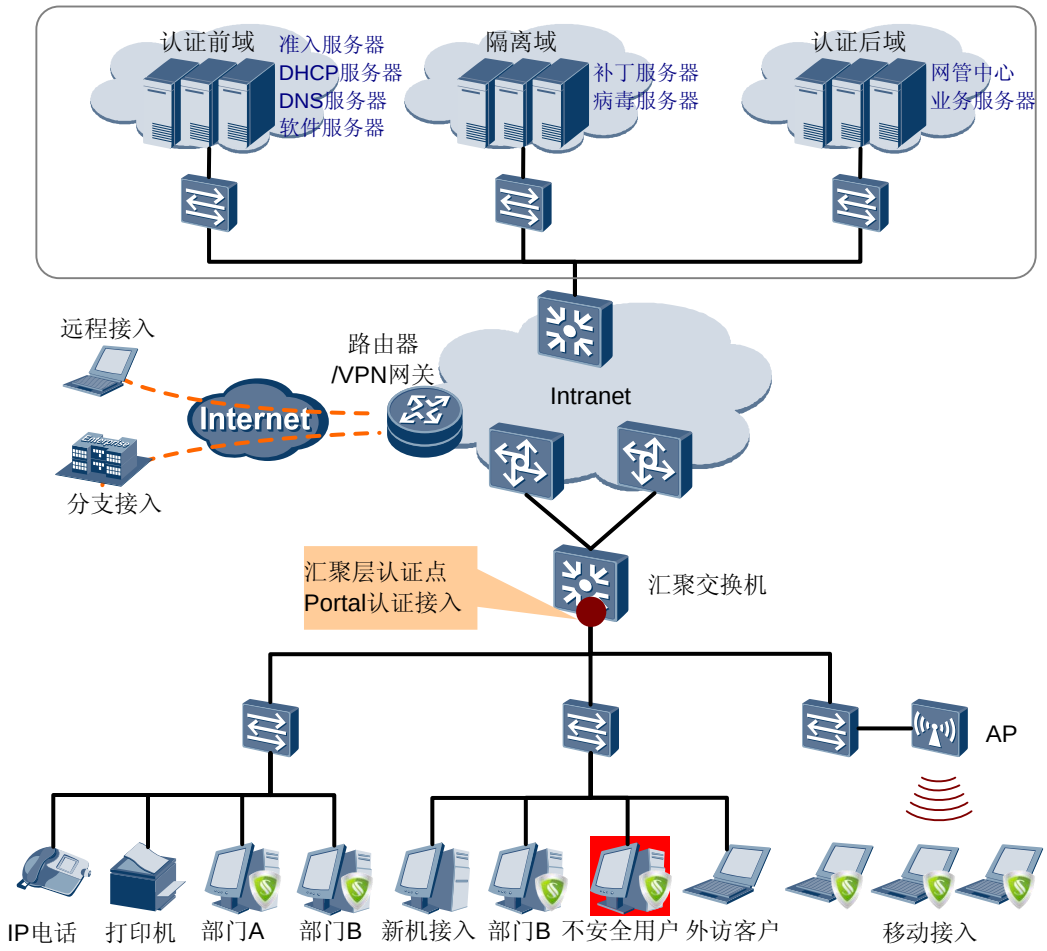
汇聚层部署认证控制点适用于接入用户分散，接入终端类型较多，无线有线混合接入的场景，认证协议建议采用基于网关的 Portal 认证。

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。

2.4.2 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 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 2-9 所示。

图2-9 汇聚层认证方案组网图



2.4.3 NAC 系统规划

软件系统规划

- 客户端

  PC 可以安装代理客户端软件，其认证模式默认为 Portal，也可以不安装。

- 服务器端
  - 认证前域部署准入服务器、DHCP 服务器、DNS 服务器，以及公用软件服务器。
  - 隔离域部署补丁服务器、病毒服务器。
  - 网络管理服务器及业务系统部署在认证后域。
  - 根据网络可靠性级别要求，可部署准入服务器控制器备份。

网络设备规划

- IP 地址

  客户端 IP 地址使用 DHCP 动态获取，用户的静态地址可以通过动态分配不变地址的方法解决。有以下两种方法：

- 用户申请一次 IP 地址后，在 DHCP Server 上将 IP 与 MAC 绑定，以后此 MAC 的终端上线都分配同样的 IP 地址。
- 采用 option82 将 IP 地址与用户上线的交换机、交换机端口绑定，以后此端口上线的用户都分配同样的 IP 地址。

- VLAN 规划

  部署时按职能部门分配 VLAN，打印机、IP Phone 等终端设备尽量部署到其他不认证 VLAN。

- 域规划

  认证前域是由 Portal Free Rule 指定的访问区域，隔离域、认证后域通过准入服务器下发 ACL 实现。部署中根据实际情况，认证前域和隔离域可以合并为一个域。

- 认证配置
  - 汇聚层设备作为接入控制点，配置 Portal 认证。
  - PC 代理客户端采用默认配置 Portal 认证。
  - 打印机、IP Phone 等终端若与 PC 部署在同一 VLAN，则配置 Portal Free Rule 打开其访问权限。若与 PC 部署在不同 VLAN，则该 VLAN 无需配置认证。

2.4.4 安全策略规划

- 准入服务器上可以统一配置安全模板，模板内确定安全检查项目，并制定安全级别，安全级别分为一般及严重。
- 终端 PC 如有一般违规，认证后进入认证后域，准入服务器会下发认证后域的 VLAN 给接入交换机进行权限控制。虽然没有进行权限限制但是终端 PC 会收到违规告警，提示用户尽快进行违规修复。
- 用户的终端 PC 如有严重违规，认证后进入隔离域，终端 PC 的权限会受到控制，并且会收到严重违规告警，提示用户尽快进行违规修复。用户可以通过自动修复按钮进行自动修复。修复成功后用户才能够获取认证后域的权限。
- NAC 系统提供实时进行安全检查，如果终端 PC 重新违规，会触发重新认证进入隔离域，并告警提示。

2.4.5 用户权限规划

- 合法用户权限控制

  汇聚层访问控制使用 Portal 认证方式，通过准入服务器下发 ACL 到汇聚交换机实现用户权限控制。

  实际部署时，根据用户的不同部门，不同级别，可以灵活配置 ACL。准入服务器还支持按部门进行统一配置 ACL，极大的方便了实际部署。

- 不合法用户权限控制

  不合法用户及未认证用户都在汇聚交换机上被限定访问权限，仅能访问 Portal Free Rule 限定的区域。

  为避免用户间互访，可在接入层交换机上部署端口隔离或其他安全特性。

- 不安全的用户权限控制

  安装了终端代理的客户端，准入服务器与终端代理联动对其进行安全检查，处理方式与接入层部署认证方案相同，即“小风险提示，大风险隔离”，不同的是汇聚层部署认证方案时，隔离信息是 ACL 控制信息。

未安装终端代理，采用 Web 方式认证的客户端，Web Agent 插件也能够对其进行安全检查，安装终端代理相比，不支持对违规项进行自动修复。

2.4.6 可靠性规划

- 可以在接入交换机上部署 DHCP snooping、IP Source Guard 等安全特性防止用户间地址盗用、欺骗。
- 还可以绑定用户或客户端到交换机端口，有效限制接入终端和防止终端盗用。
- 为防止终端用户互访，还可在接入交换机上部署端口隔离。

2.5 汇聚层旁挂认证方案规划建议

2.5.1 应用场景

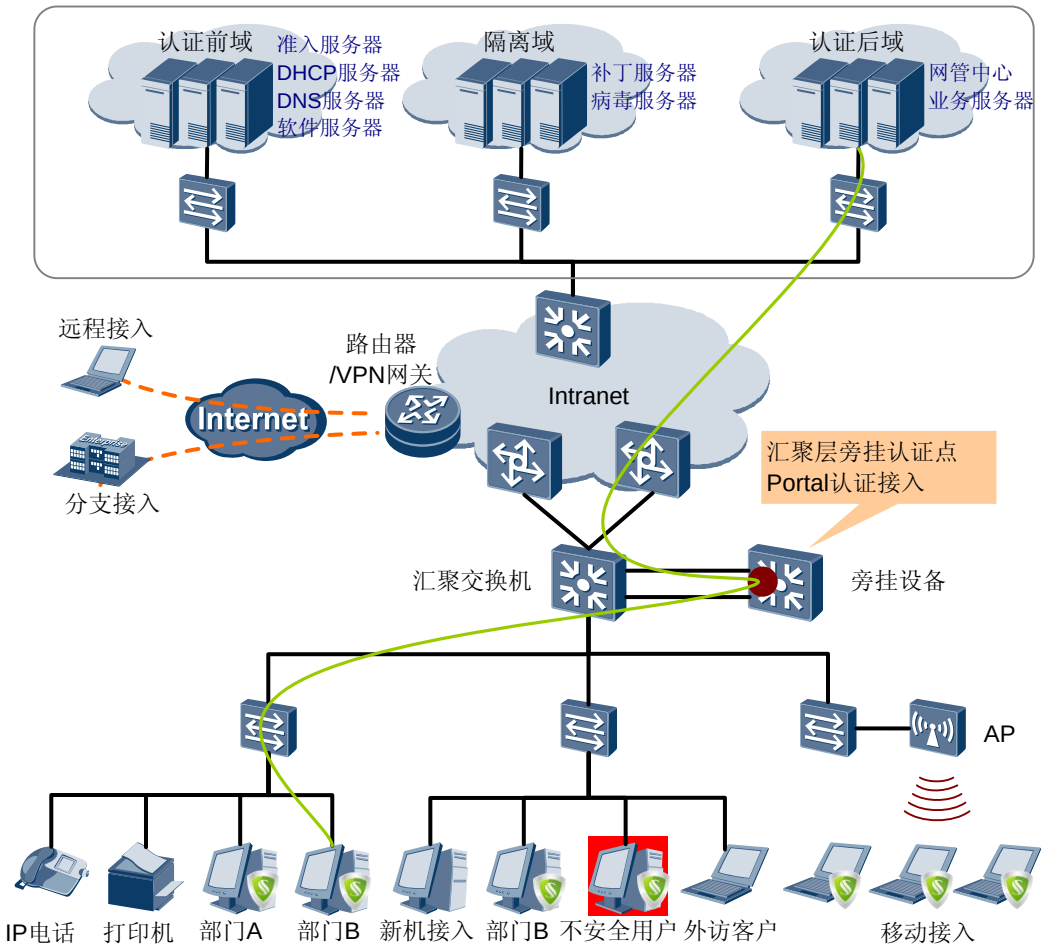
汇聚层旁挂认证方案主要针对那些网络设备较为老旧的网络升级场景，不需要改变原有网络结构，旁挂设备一台设备即可引入一整套的网络安全接入控制方案，能够有效节约用户投资。本方案中，上下行流量都以旁挂设备为网关，对旁挂设备的性能要求较高。

汇聚旁挂方案仍然推荐使用 Portal 认证方式，具体的 NAC 系统规划、安全策略规划、用户权限规划和可靠性规划都和汇聚层认证相同。本节不再详述。

2.5.2 组网规划

网络结构与汇聚点认证控制方案类似，不同的是汇聚交换机旁挂一台具有认证功能的交换机作为网关，在旁挂交换机上基于网关部署 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。如图 2-10 所示。

图2-10 汇聚层旁挂认证方案组网图



3 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3-1 部件产品建议表

部件	产品/型号
接入交换机	S5700、S3700、S2700
汇聚交换机	S7700、S5700
核心交换机	S9300
WLAN AC	S9300 AC 插卡
Server 端软件	TSM Server
Client 端软件	TSM Agent
AD 服务器	Windows 2003 Server