什么是 NAC

文档版本 02
发布日期 2020-11-16

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： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 什么是 NAC

定义

NAC（Network Admission Control）称为网络接入控制，是一种“端到端”的安全结构，包括802.1X认证、MAC认证与Portal认证。

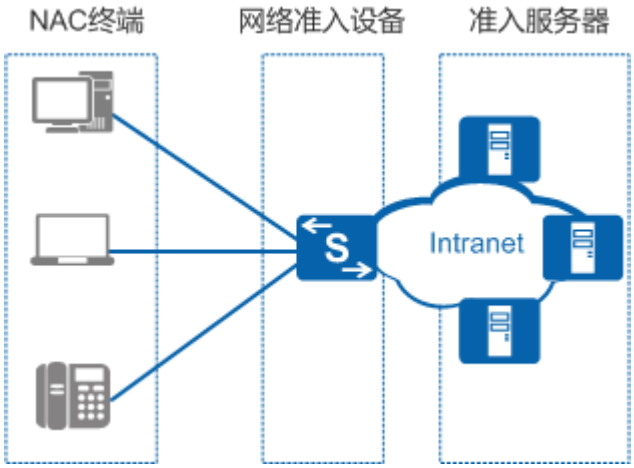
随着企业网络的应用和发展，病毒、木马、间谍软件、网络攻击等各种信息安全威胁也在不断增加。在传统的企业网络建设思路中，一般认为企业内网是安全的，安全威胁主要来自外界。但是研究证明，80%的网络安全漏洞都存在于网络内部，它们对网络的破坏程度和范围持续扩大，经常引起系统崩溃、网络瘫痪。另外，内部员工在浏览某些网站时，一些间谍软件、木马程序等恶意软件也会不知不觉地被下载到电脑中，并且在企业内网传播，产生严重的安全隐患。

因此，随着安全挑战的不断升级，仅通过传统的安全措施已经远远不够，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。

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，进而保护企业整网的安全性。

如图所示，NAC安全构架包括三个关键组件：NAC终端、网络准入设备和准入服务器。

1. NAC典型组网图



- NAC终端：作为NAC客户端的各种终端设备，与网络接入设备交互完成用户的接入认证功能。如果采用802.1X认证，用户还需要安装客户端软件。
- 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）。
- 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，主要进行用户身份认证、终端安全检查、系统修复升级，终端行为监控审计等工作。

目的

传统的网络安全技术只考虑了外部计算机对网络的威胁，而没有考虑到内部计算机对网络的威胁，而且现有的网络设备难以有效防止内部设备对网络的威胁。

为了保证网络通信业务的安全性，可引入NAC安全构架。NAC安全构架从用户终端角度考虑内部网络安全，实现对接入用户进行安全控制，提供了“端到端”的安全保证。

三种认证方式比较

NAC包括三种认证方式：802.1X认证、MAC认证和Portal认证。由于三种认证方式认证原理不同，各自适合的场景也有所差异，实际应用中，可以根据场景部署某一种合适的认证方式，也可以部署几种认证方式组成的混合认证，混合认证的组合方式以设备实际支持为准。三种认证方式比较如下表所示。

表 1-1 认证方式对比

对比项	802.1X认证	MAC认证	Portal认证
适合场景	新建网络、用户集中、信息安全要求严格的场景	打印机、传真机等哑终端接入认证的场景	用户分散、用户流动性大的场景
客户端需求	需要	不需要	不需要
优点	安全性高	无需安装客户端	部署灵活
缺点	部署不灵活	需登记MAC地址，管理复杂	安全性不高

NAC 与 AAA

NAC与AAA互相配合，共同完成接入认证功能。

- NAC：用于用户和接入设备之间的交互。NAC负责控制用户的接入方式，即用户采用802.1X，MAC或Portal中的哪一种方式接入，接入过程中的各类参数和定时器。确保合法用户和接入设备建立安全稳定的连接。
- AAA：用于接入设备与认证服务器之间的交互。AAA服务器通过对接入用户进行认证、授权和计费实现对接入用户访问权限的控制。

