联软科技
LEAGSOFT

技术白皮书

LeagView®联软 UniNAC 网络准入控制系统

深圳市联软科技股份有限公司

2023 年 9 月

版权声明

免责条款

由于产品版本升级或其他原因，本白皮书内容有可能变更。联软科技保留在没有任何通知或者提示的情况下对本白皮书的内容进行修改的权利。本白皮书仅作为使用指导，联软科技全力在本白皮书中提供准确的信息，但是不确保本白皮书内容完全没有错误，本白皮书中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

联系方式

用户支持邮箱：support@leagsoft.com

技术支持热线电话：400-6288-116

网址：http://www.leagsoft.com

目录

一 产品背景

计算机高速发展过程中，网络内出现越来越多的 0day 攻击，此时迫切需要一种技术可以对非法的电脑做网络隔离，并能在网络中自动定位出有问题的电脑，进一步对这些电脑做安全修复，最早的网络准入控制技术应景而生。

在 2003 年，当时全世界最大的网络厂商 Cisco 提出 NAC 技术与 SDN(自防御网络)概念，并形成了网络准入控制技术框架，随后，Microsoft、Juniper 等网络大厂也分别发布相应的产品与解决方案，到了 2006 年，网络准入控制市场发展迅猛，当年 NAC 被国内外媒体称为继防火墙之后最大的网络安全市场热点。

Cisco NAC 网络准入控制技术的演进过程如下所示：

- Cisco NAC 1.0：解决网络隔离问题；
- Cisco NAC 2.0：实现更细粒度的准入控制；
- Cisco NAC 3.0：提出硬件的解决方案，主要解决部署困难的问题；
- Cisco NAC 4.0：思科又放弃了网关的方案，重点解决集中管理的问题，在第二代技术基础上增加了实名制网络资源访问控制等技术，即 Role-based 802.1x 技术。

经过这么多年的发展，NAC 的解决焦点从网络的访问控制演进为对资源的访问控制。在新的技术发展背景下，如何在不同的网络环境、应用环境以及业务环境的基础上营造信息系统的可信环境空间，是每一个信息安全从业者亟待考虑的问题。

二 产品概述

联软网络接入控制系统（以下简称 UniNAC），是解决安全管理问题的基础设施，可以对接入网络的客户机设备进行控制，杜绝非法外来电脑接入内部网络，同时将有问题的客户机隔离或限制其访问，直到这些有问题的客户机修复为止。一方面可以防止这些客户机成为蠕虫和病毒攻击的目标，还可以防止这些主机成为传播病毒的源头。为大型机构的网络安全、终端管理、信息安全管理提供直接支撑。

UniNAC 是中国最早支持 802.1x 协议、业内最早直接支持 Cisco NAC 架构的网络准入控制系统。UniNAC 提倡直接与网络设备联动实现网络准入控制，以实现最佳的网络安全性、可靠性和组网灵活性，目前能直接联动的网络设备型号达数百种。通过与网络设备联动及联软 NACC 准入控制器配合，UniNAC 能解决各种复杂环境下的网络准入控制问题，包括：LAN（Switch/HUB）、WiFi、WAN、VPN，甚至 NAT 环境。

联软在准入控制的演进

联软在 2012 年发布资源访问控制技术 RAC(Resource Access Control)，支持 Role-based 网络资源访问控制，也支持用户终端、哑终端的资源访问控制。

该技术通常用 ACL 控制网络资源访问权限，支持在各种型号的 802.1X 网络交换机、无线控制器、支持 EoU 的路由器、联软的 NACC 网关和客户端上下发 ACL，这样就可以实现对不同的终端、不同的用户角色、不同的应用程序、不同的访问时间下发指定的访问权限，从而对网络的接入实现细粒度的管理。

网络使用中新的安全性和移动性要求，让 NAC 演进为全新的 EVAS（Endpoint、Visibility、Access、Security）端点可视化与访问控制安全。EVAS 定义：一种网络安全技术，提供基于策略的情报、 执行、 弱化风险，并实时监控所有网络设备访问、配置和连接到 IP 网络的任何节点的活动。但是 EVAS 本身不直接实现数据信息的保护，而只能作为“安全基础设施”为数据安全保护提供支撑基础。联软科技率先将 EVAS 概念引入到终端安全管理平台产品中，形成了一套以 EVAS 为基础，集合终端数据信息安全防护的 DEVAS 解决方案。

- 在网络安全方面

有 EAVS，基于设备、用户、网络位置、时间、数据的敏感性等颗粒化的网络访问控制，防止问题电脑接入、问题人员对网络的访问，与安全信息和事件管理间广泛的集成。

- 在应用安全方面

有资源访问控制 RAC，防止不正确的时间、地点、接入方式的异常访问，防范缓冲区溢出攻击、规避审计手段等黑客工具攻击。

- 在信息安全方面

有终端数据信息安全防护，防止被用黑客工具非法盗取信息，防止内部人员将其接触到的信息，转给外部人员泄密。

联软在准入控制的演进

2004 年，全球首创设备快速发现与定位技术，设备接入网络，几分钟内即可发现、定位(无需 Agent)，同类产品需要数小时乃至数天，持续 12 年保持领先；

2005 年，中国第一家基于 802.1x/EoU 网络准入控制产品，EoU 准入这个名词首先在联软的技术文档中被使用；

2006 年，全球第一家，一个 Agent 支持多网络设备厂商，联软成为首家基于 Cicso NAC 框架的产品供应商；

2008 年，中国第一家推出基于硬件网关的准入控制器(NACC)，解决复杂的环境的网络接入管理问题，支持准旁路部署、全旁路部署；

2010 年，中国第一家发布 Linux 客户端的厂商，支持准入控制；

2012 年，在网络准入控制基础上，发布新一代 NAC 技术 RAC，引领第四代网络准入控制技术向前发展；

2014 年，系统支持对移动终端的接入管理；

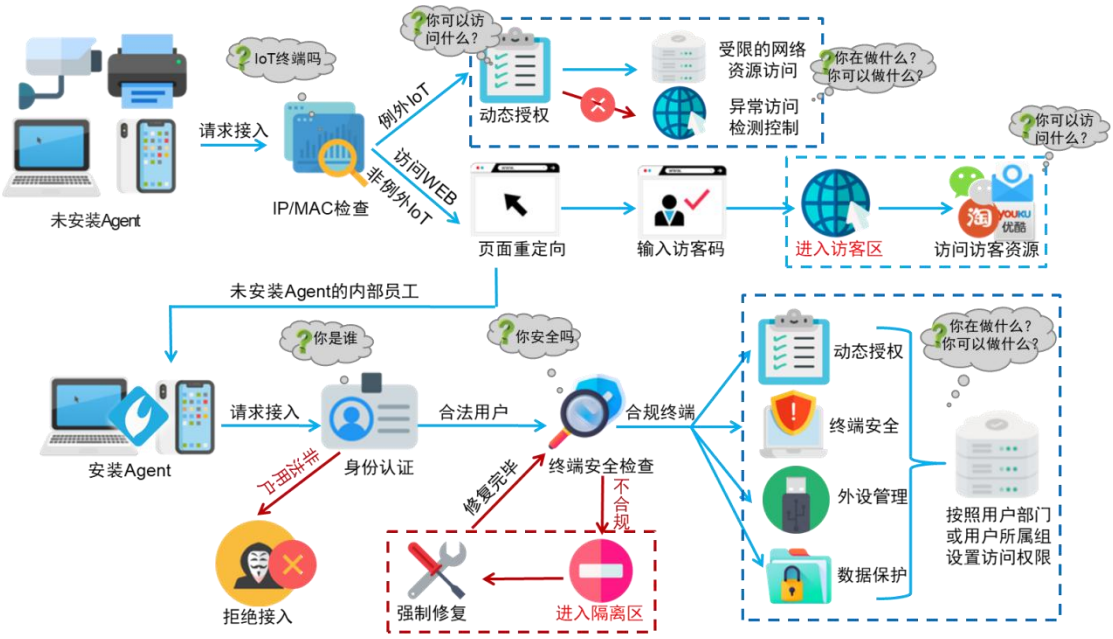
2015 年，系统支持对哑终端设备自动识别和接入管理；集合终端数据信息安全防护的 DEVAS 解决方案。

当然，还有业内独创 HTTPS 重定向访问技术，独创 MAC 地址自动获取，接入认证故障诊断辅助工具等等。

经过多年的发展，联软科技已经成为中国网络准入控制市场的技术领导者，而且还将持续创新，为客户更有价值的技术及解决方案。

三 功能说明

3.1 UniNAC 准入流程



联软 UniNAC 整体控制流程。

1）未安装 Agent 的终端入网流程

当未安装 Agent 的终端，请求接入网络时，系统会通过 IP/Mac 来检查是否 IoT 终端，如果是白名单里面的例外 IoT，将允许接入网络并进行动态授权，只允许其访问受限的网络资源，同时也会开启异常访问检测控制防止设备仿冒。

2）非例外 IoT 终端入网流程

如果是白名单以外的非例外 IoT 终端，访问网页时，会跳转重定向页面进行准入控制，外部访客可以输入其获取到的访客码进行登记入网，进入访客区，并且只赋予互联网的访问权限，严禁接入到企业内网。

3）内部员工入网流程

对于未安装 Agent 的内部员工，系统会通过重定向页面引导安装 Agent。当 Agent 安装完成后，才会进行网络准入控制流程。首先进行用户身份认证，认证失败的非法用户拒绝接入。然后进行终端合规检查，用户身份认证合法后，我们会对用户的接入终端进行安全合规检查，安全检查不合规的话安置到隔离区内强制修复，直至修复合规后才能继续接入；最后，在用户身份合法和终端检查合规

后，我们才允许员工接入网络，这时系统会根据用户角色下发基于角色的动态访问控制授权，同时也可以通过 Agent 下发终端安全、外设管理、数据保护等策略。

部署 UniNAC 后，改变了终端接入网络的行为模式。一般来说，只有合法身份和满足安全要求的客户机才允许接入网络，确保接入网络的电脑终端符合安全要求。

3.1.1 接入检查

终端在接入网络时，准入控制系统会检查其用户账户、安全设置状态、终端硬件合法性等。只有合法身份和满足安全要求的客户机才允许接入网络，确保接入网络的电脑终端符合如下要求：

1）必须安装联软客户端，如果是未安装联软客户端的电脑终端接入网络，其打开 WEB 浏览器访问任何 Web site 时，将被重定向到管理员指定的一个页面，提醒其安装联软客户端。不安装联软客户端的电脑将无法访问内部网络（特殊电脑和访客电脑可以例外）。

2）必须符合网络接入安全管理规定，例如：拥有合法的访问账号、安装了指定的防病毒软件、安装了指定的操作系统补丁等。如果不符合管理规定，将拒绝其接入，或者通过网络对该电脑进行自动隔离，并且指引其进行安全修复。

UniNAC 通过网络准入控制技术，对接入网络的电脑终端进行实时安全检查，检查的内容包括：

1）支持的准入控制技术

- 联软 802.1X 准入控制技术
- Cisco Eou 准入控制技术
- 联软 NACC 准入控制技术

2）账户检查：用户名和密码

- 手机动态码验证
- 与企业微信、钉钉实现扫码认证；
- 系统内置账号认证；
- AD/LDAP 账号认证；

- 邮件服务器账号认证；
- 证书认证；
- 第三方 radius 认证；
- 第三方扩展动态库认证；
- 访客及外协账号验证；
- 双因素认证；
- 与竹云 IAM 账号进行认证；
- 与 UOS 域进行认证；
- 助手端扫码和动态码方式的快捷认证。

3）安全设置规范检查：终端的安全设置

- 检查系统账户，包括 Guest 账户和弱口令检查；
- Windows 域检查，检查终端是否加入指定的 Windows 域；
- 检查可写共享设置，检查终端是否设置了可写或者没有权限限制的可写共享；
- 检查终端操作系统补丁安装情况；
- 检查终端的防病毒安装情况及其病毒特征库是否及时升级；
- 检查终端是否有可疑的注册表项；
- 检查终端是否有可疑的文件存在；
- 检查终端是否安装了非法软件。
- 屏保检查；
- 终端系统版本检查；
- 终端服务安装检查；
- 终端防火墙检查；
- 终端端口开启状态检查；
- 主机名检查。

4）终端绑定规则检查

- 对接入终端、接入用户或部门以及接入控制点设备制定相应的绑定规则，根据接入终端或用户是否符合接入规则来决定允许还是拒绝其接入；

- 用户与 mac 地址绑定；
- 用户与交换机端口绑定；
- 用户与接入控制点设备绑定；
- 用户与安全助手生成的主机码和随机码绑定；
- 设备组、部门，以及指定无线 ssid 参数的绑定；
- 终端的 ip 与 mac 地址绑定，防止 ip 地址被占用（功能迁移至设备指纹管理）；
- 对免检设备进行仿冒检查，将仿冒设备隔离；
- 基于终端准入技术/方式和身份验证方式控制其接入规则。

3.1.2 安全隔离

如果在接入检查时，发现终端不符合安全规定，需要对终端进行隔离或拒绝其访问网络资源，例如：发现是外来终端则拒绝接入或进入“访客区”网段，或者是内部不符合安全规定的终端，则让其进入“修复区”。

3.1.3 安全通知

对被隔离的终端进行通知，告知其被隔离的原因。

3.1.4 安全修复

自动引导被隔离的终端，让其修复安全设置或者进行注册登记，使得其可以正常访问网络资源。

一个完整的网络准入控制系统，应该包括以上几个方面的内容，缺少其中一个或者两个方面的内容，就不是完善的解决方案，会给准入控制系统的部署和推广带来问题。

3.2 UniNAC 准入技术

3.2.1 802.1x

IEEE 802.1x 是 IEEE 制定关于用户接入网络的认证标准，全称是“基于端口的网络接入控制”，属于 IEEE 802.1x 网络协议的一部分。它为想要连接到 LAN 或 WLAN 的设备提供了一种认证机制。IEEE802.1x 一般部署在 LAN 网络的接入层

交换机上或者 WLAN 网络的无线控制器上。其准入控制流程如下：

- 每一个 802.1x 交换机端口，交换机都为其创建两个虚拟接口；
- Controlled Port：只有通过 802.1x 认证后才被导通；
- Uncontrolled port：仅仅用于传输 802.1x 认证流程，即 EAP 包(EAPOL)。

初始状态下，交换机上的所有端口处于关闭状态，仅允许 802.1x 协议数据流通过，当用户通过 802.1x 协议登录交换机时，交换机将用户名/口令传送到 Radius 服务器进行认证。如用户名及口令通过验证，则相应的交换机端口打开以允许用户访问相应的网络资源。

UniNAC 准入控制器结合 802.1x 来解决终端电脑身份认证的问题，通过动态切换 VLAN 或者下载 ACL 列表的方式来控制网络资源访问，具有以下优点：

- 支持多厂商网络设备：包括 Cisco、华为、H3C、Juniper 等；
- 控制点是网络的接入层交换机，最接近终端电脑，对不符合策略的电脑可以完全禁止其访问任何网络，使其对网络的危害最小。

3.2.2 Cisco EoU

EoU（EAP over UDP）是 Cisco 的专有协议。EoU 是 Cisco NAC 技术的第一个实现版本，2003 年最早在 Cisco 的路由器上实现，后来在 Cisco 的 3 层交换机上也实现了 EoU。EoU 和 802.1x 相比，最大的区别是 802.1x 在网络接入层进行准入控制，而 EoU 则是在网络的汇聚层或核心层进行准入控制。

EoU 的工作原理是当支持 EoU 的汇聚层设备接收到终端设备发来的数据包时，汇聚层 EoU 设备将要求终端设备进行 EAP 认证。EAP 认证包封装在 UDP 包内，在 EAP 认证的内容中，如果安全状态不符合企业安全策略，汇聚层 EoU 设备将从策略服务器上下载 ACL，限制不安全的客户端的网络访问，并对其进行修复。

EoU 技术的优点是它对网络接入设备要求不高，因而覆盖面较高，且由于网络环境中汇聚层设备数量一般会大大少于接入层设备数量，因此部署相对较为容易。

3.2.3 硬件网关型准入

联软 NACC 准入控制器是一种基于 Cisco EoU 协议的硬件网关型网络准入控制设备，专为解决非 802.1x 网络环境下（接入层交换机或者 AP 不支持 802.1x 协议且汇聚层/核心层不支持 Cisco EoU 协议）的网络准入控制问题而设计。联

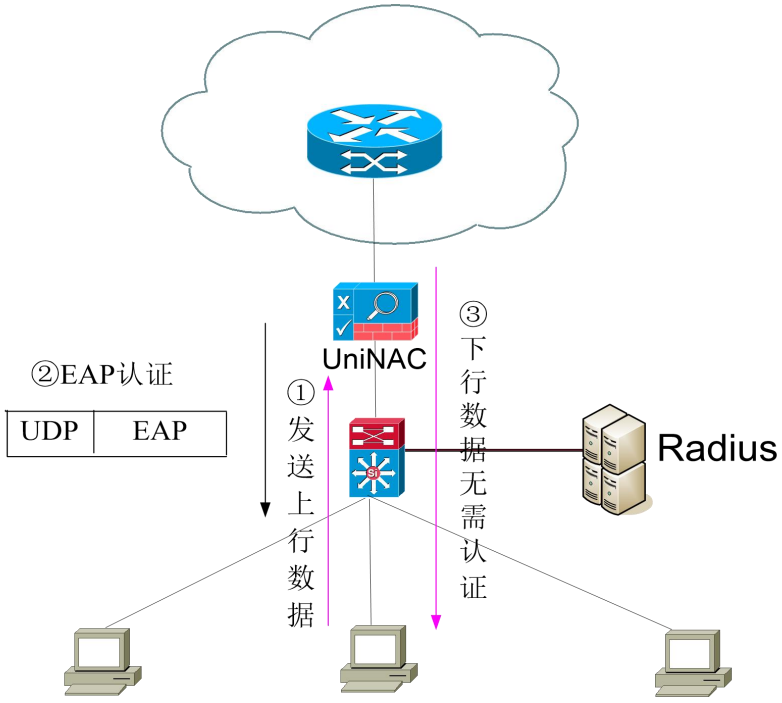
软 NACC 准入控制器通常部署在网络核心交换机或指定服务器前，来判断接入设备是否符合接入安全要求。与 802.1x/EOU 相比，采用 NACC 硬件网关实现准入控制，业务实现流程清晰可靠、环节少，用户只需要购买少量网关设备，并通过网关方式或者旁路方式部署至网络关键节点处，即可实现全面的准入控制。

联软 NACC 准入控制器支持 3 种部署模式：网关部署模式（即串联模式）、策略路由模式（上行控制、下行不控制）和端口镜像模式。

1. 网关部署模式：

将 NACC 设置为网关，并将 NACC 上行端口（与终端相连的端口）设置为要求通过 EAP 认证，将其下行端口（与外网相连的端口）设置为不要求通过 EAP 认证。终端设备发送的数据包全部通过 NACC，并由 NACC 要求终端进行 EAP 认证。NACC 根据源 IP 地址对应的设备的网络准入控制状态来决定是允许、拒绝还是重定向。对于经验证后允许接入的数据包，其下行数据包则可以不需要通过验证直接接入。

网关接入模式的优点是成本较低、设置简单，其部署示意图如下图所示：



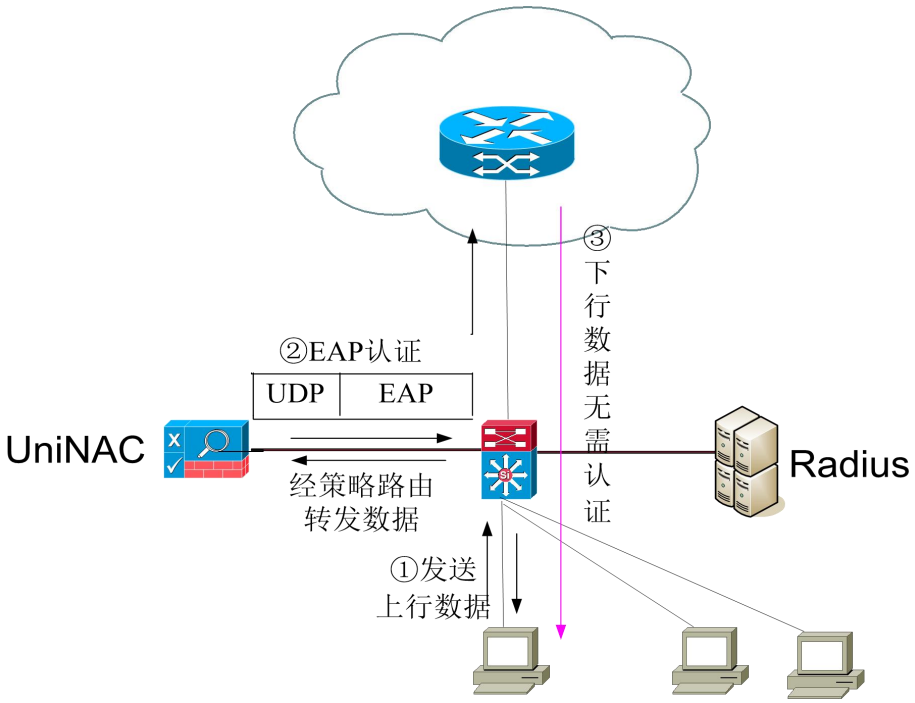
2. 策略路由模式—准旁路模式：

将 NACC 部署在网络中的汇聚层或核心层，并与汇聚层或核心层的交换路由设备连接。在交换路由设备上启用策略路由，将上行数据包（终端设备发送的数据包）路由到 NACC 中，由 NACC 要求终端设备进行 EAP 认证。NACC 根据源 IP 地

址对应的设备的网络准入控制状态来决定是允许、拒绝还是重定向。对于经过验证之后允许接入的数据包，其下行的数据包则从正常的路由汇聚层或核心层设备走，不经过 NACC。

策略路由模式的优点是仅有上行数据包通过 NACC 而避免出现链路拥塞、网络可扩容性好、冗余性强。

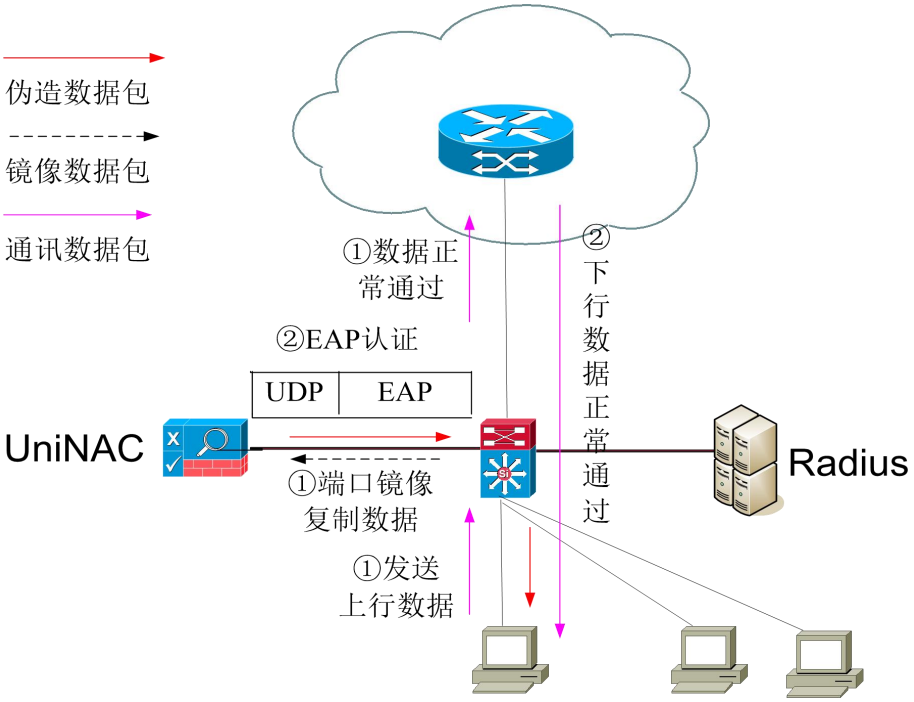
其部署示意图如下图所示：



3. 端口镜像模式－全旁路模式：

将 NACC 部署在网络中的汇聚层或核心层，并与汇聚层或核心层的交换路由设备连接。将终端设备上行经过的交换机端口或 VLAN 镜像到 NACC，通过 http 流量触发 NACC 对客户端发起 EOU 认证，根据认证结果决定是否对 http 请求包发送重定向页面。根据认证结果可选择对 TCP 包发送 Reset 信息强制断开链接。

端口镜像模式的优点：无网络瓶颈、无网络故障风险、零网络改造其部署示意图如下图所示：



3.3 准入认证方式

3.3.1 Web Auth

Web Auth 认证方式 （部分网络厂商将其命名为 Portal 认证）指未认证接入设备通过 HTTP 访问网络资源时，网络设备强制用户登录到指定站点并提交用户准入认证信息，准入认证前，用户只能访问 DHCP、DNS 等有限网络资源。准入认证成功后，通过动态下发 ACL 的方式控制接入设备访问的网络资源。

Web Auth 适用于用户 PC/笔记本终端和各类移动智能设备办公的场景。依据网络设备对 Web Auth 支持的特性，准入控制接入点可在网络接入层或网络汇聚层实现。

3.3.2 MAB/IAB 认证

MAB（MACAuthentication Bypass）属于 802.1x 协议，可依据接入设备的 MAC 地址做身份认证。

基于 MAC 地址的认证是一种基于端口和 MAC 地址对接入设备访问网络资源进行权限控制的一种认证方式，无须安装任何客户端软件。网络设备在首次检测到接入设备的 MAC 地址后，即启动对该接入设备的身份认证。网络设备通过 Radius 服务来支持 MAC 地址认证，在这种认证方式下，网络设备与 Radius 服务配合完

成 MAC 地址身份认证：Radius 服务完成对该接入设备的认证后，认证通过的接入设备可以访问网络。Radius 可以通过 VLAN 切换或下发 ACL 的方式来限制认证接入设备访问指定的网络资源。

MAB 认证一般适用于无人值守设备（如网络打印机、演示机、叫号机等），也可用于一般位置不会移动的用户终端设备。根据 MAB 认证的控制点位置和网络设备的支持性，MAB 认证可以在接入层和汇聚层实现，并且支持有 HUB 的网络结构。IAB（IP Address Bypass）属于联软 NACC 准入控制技术里的特有功能，可依据 IP 地址做认证。其认证流程与 MAB 认证相似。

在部署了联软 NACC 准入控制器后，可通过 IAB 认证，对无人值守设备（如网络打印机、演示机、叫号机等）以及位于一般不会移动的用户终端设备放行。使得此终端无需做认证即可访问网络。

3.3.3 系统自带 802.1x 客户端认证

诸如 Windows、IOS、Andriod 等终端操作系统均自带 802.1x 客户端，对于此类设备可以通过对客户端进行配置，包括网络身份验证信息、身份验证方法等，实现接入设备的 802.1x 准入控制认证。

3.3.4 联软客户端认证

联软客户端准入控制认证，主要用于杜绝非法外来电脑接入内部网络；同时将有问题的客户机隔离或限制其访问，直到这些有问题的客户机修复为止，这样，一方面可以防止这些客户机成为蠕虫和病毒攻击的目标，还可以防止这些主机成为传播病毒的源头。其准入控制流程如下：

首先，终端接入网络前必须符合安全管理规定，例如：

- 拥有合法的访问账号；
- 安装了指定的防病毒软件、安装了指定的操作系统补丁等；

对于不符合安全管理规定的终端，拒绝其接入网络，或者通过网络对该电脑进行自动隔离，并且指引其进行安全修复。

然后，对接入网络终端可进一步的做如下管控，包括：

- 安全设置检查、加固，非法操作的管理、限制；
- 防止文件非法外传（U 盘/软盘/共享/E-mail/QQ/MSN 等）；

- 电脑终端的集中式管理，例如：资产管理、软件分发、远程控制、补丁管理、分组策略分发及集中审计。

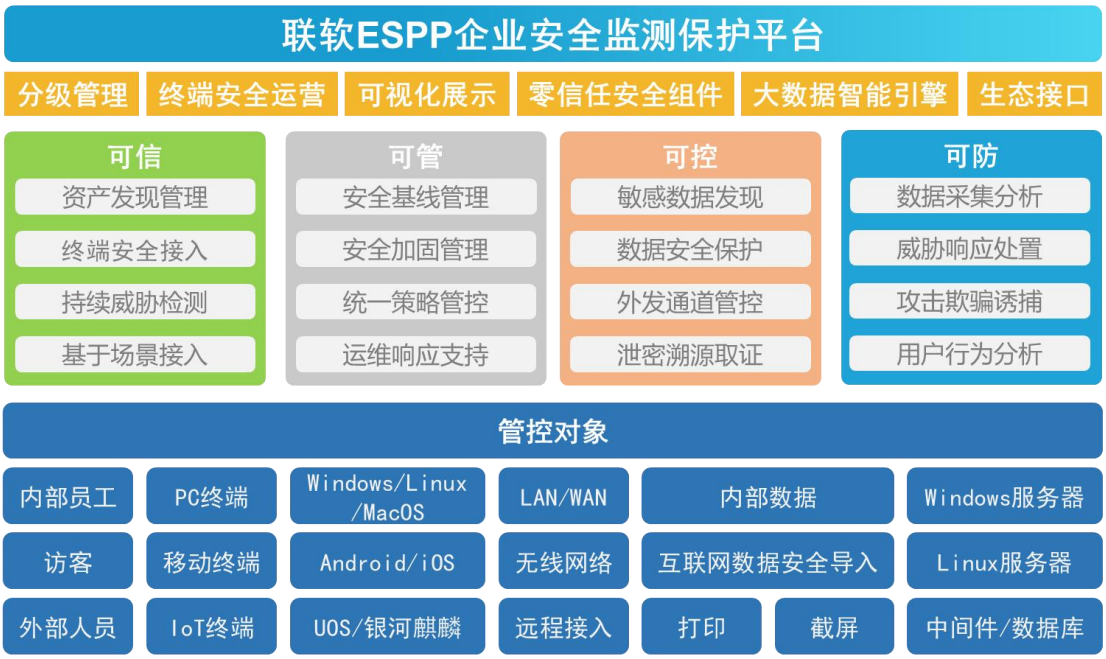
联软客户端认证适用于用户 PC/笔记本终端在各个场景的接入控制，包括 WAN、LAN、WLAN、VPN 等。

3.4 集成扩展

3.4.1 UniNAC 与企业信息体系集成方案

根据 ISO27001 信息安全管理体系模型，组织应通过 PDCA 持续改进自身的信息安全风险管理，建立动态的“计划、设计和部署、监控评估、改进提高”管理方式，以持续不断地改进组织整体信息安全。

UniNAC 从系统设计初始即将 PDCA 持续改进模型融入系统架构中，以 PDCA 为线索，设计各个功能模块，通过各项安全功能支持企业在网络和终端安全持续发现，以及改进终端桌面和网络接入的相关风险，如下图所示：



- P(Plan)：组织可通过 UniNAC 制定终端安全的相关策略；
- D(Do)：组织可通过 UniNAC 准入控制模块实现 Plan 阶段指定的相关安全策略；
- C(Check)：组织可通过安全评估模块检查终端安全策略执行的有效性；
- A(Act)：组织可通过安全审计模块发现终端安全管理中存在的问题，以

便进行总结，并进入 PDCA 的下一个循环进行改进。

通过基于 PDCA 的模块化设计，UniNAC 可以有效地支持组织信息安全风险管理，以一种科学、高效的方式帮助组织开展网络接入和终端安全的风险管理。

同时，企业信息安全体系中的一个重要核心就是信息安全技术架构，企业通过设计、构建整体信息安全技术架构来从整体控制如何减轻企业信息资产面临的各项信息安全风险，架构中的各技术组件专门负责特定领域的安全控制。但是企业在建设整体信息安全技术架构时，往往会出现“单独建设，单独管理”，虽然建设了大量安全系统，彼此之间却无法有效集成，从而形成了安全领域中的“信息孤岛”，无法发挥信息安全技术架构的整体效力，也给运维人员带来繁杂的运维压力。

UniNAC 从设计起就充分参考了 ISO27001 等国际信息安全标准，设计了各类预留接口，并提供相关功能以便于企业实现与其他安全组件的集成，从而方便企业整合相关各类安全，真正的实现企业信息安全架构。

UniNAC 预留的开发接口包括：

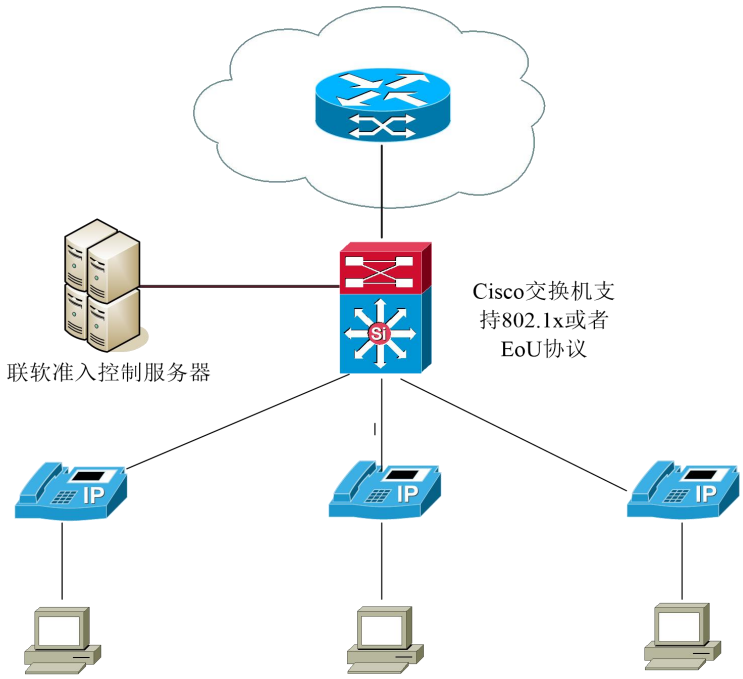
安全组件	预留接口设计
Windows AD 域	准入平台支持 AD 域作为系统认证的第三方认证源； 准入平台可以定期自动跟 AD 服务器进行组织架构的同步； 准入客户端程序可以自动获取当前登录的 AD 账号名称。
LDAP、电子邮件服务器	准入平台支持 LDAP、电子邮件服务器作为系统认证第三方认证源。
PKI/CA	定期自动跟 PKI 服务器进行 CRL（证书吊销列表）的同步； 准入平台可以同时支持 AD 账号和 PKI 证书的混合认证； 准入客户端程序可以自动获取当前插入的USB-KEY 的证书名称，并在客户端界面上支持中文显示； 客户端支持拔出 USB-KEY 自动锁定屏幕和立刻清除当前 KEY 的缓存信息。
SOC	可通过接口实现安全日志交换到 SOC 平台。
ITIL	服务台可通过接口快速调阅终端软硬件变更、网络接入位置等

	信息，方便进行事件处理。
ERP/财务管理系统	可通过接口实现终端软硬件资产信息数据交换。

通过各类预留接口设计，UniNAC 可与企业已有安全组件进行集成，充分利用已有投资，并通过系统集成实现单个系统无法实现的安全功能和安全保障，避免了信息孤岛，从而真正发挥组织信息安全技术架构和信息安全体系的威力。

3.4.2 UniNAC 与 VoIP 的准入集成管理方案

很多企业内部部署了 VoIP 电话，VoIP 和终端设备往往共用一个网络接口，部署方案如下图所示：



由于 IP 电话一般无法安装准入控制的客户端，如何保证在启用了准入后，不影响 IP 电话的正常网络接入和运行将成为一个必须解决的问题。此时准入控制系统在支持终端设备接入的同时也必须支持 VoIP，联软 UniNAC 有以下几种解决方案用于支持各类品牌 VoIP（Cisco、Avaya 等）VoIP 的网络接入：

解决方案	接入场景	说明
联软 802.1x 与 VoIP 的准入控制方案	Cisco 交换机 + Cisco IP 电话	Cisco 交换机可以通过 CDP 识别出 Cisco ip 电话，并通过 802.1x 中主机模式为

		multi-domain，实现 IP 电话的自动放行。
	Cisco 交换机 + avaya IP 电话	Cisco 交换机的 multi-host 的主机模式下，可以设置 native vlan 和 auxiliary VLAN，802.1x 认证只会在 native vlan 生效，在 auxiliary VLAN 不生效。可通过配置 avaya ip 电话采用 supplicant mode 以支持 802.1x 接入。
	Cisco 交换机 + 任意 IP 电话	在较新的 IOS 版本中，Cisco 推出了 802.1x 的 MAB（mac-auth-bypass）的特性，该特性可以让无法安装安全助手或者无须安装安全助手的设备，通过 MAC 地址完成认证。相关 IP 电话上也需要进行配置以支持 802.1x 协议。
	h3c 交换机+ H3C IP 电话	在纯 H3C 的环境下，可以直接在启用了 802.1x 的准入控制的交换机上，增加 voice vlan 的配置以支持 H3C IP 地址网络接入。
	802.1x 的交换机+任意 IP 电话	在启用了 802.1x 的端口，可以在每个端口上直接绑定 IP 电话的 MAC 地址，将 IP 电话直接放行，而接在 IP 电话上的 PC 则必须进行身份验证。
Cisco EoU 与 VoIP 的准入控制方案	Cisco 交换机 + Cisco ip phone	EoU 支持交换机上配置来实现 Cisco IP 电话的例外放行。
	Cisco 交换机+ avaya ip phone	EoU 支持 IP 电话的准入控制例外。

3.5 UniNAC 高可用性

由于网络准入控制服务一旦发生故障，会导致电脑终端无法接入网络，因此

方案必须提供保障以实现网络准入控制的高度可靠性。联软科技提供的 UniNAC 方案具有如下特征：

1） 和认证过程相关的设备和系统，不存在单点故障。即单台服务器或者设备的暂时性故障，不会导致整个网络接入服务不可用；

2） 和准入控制系统相关的网络设备、服务器、数据库和软件故障，系统能够实现自动报警，向相关管理员发送手机短信息等；

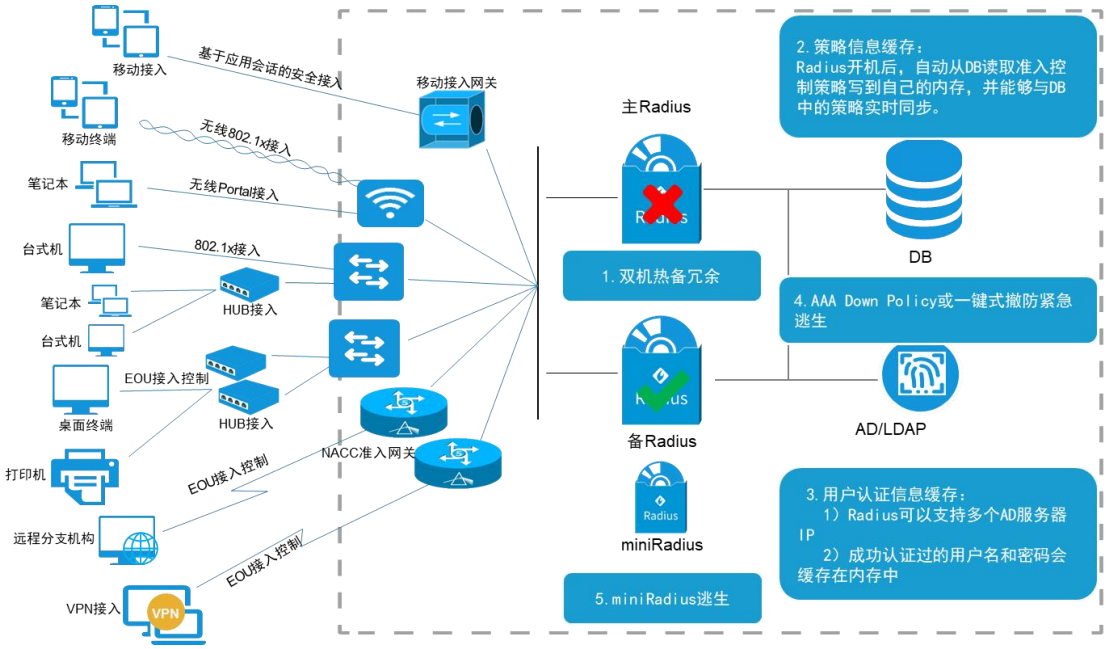
3） 在特殊紧急情况下（例如：双机故障，或分支机构到总部的广域网线路中断）

- 网络管理员可以通过执行脚本的方式，快速将网络接入设置为“不设防”状态（临时撤销所有准入控制措施），使得所有电脑终端能够正常接入网络。
- 如果执行网络准入控制的网络设备是 Cisco 的交换机或者路由器，可以在网络设备上配置紧急模式。在紧急模式下，可以指定电脑终端可以访问哪些资源。

通过以上手段，UniNAC 可以保障网络接入服务的高度可靠性。

3.5.1 冗余保障

准入控制服务器控制着终端接入网络，如服务器发生故障，可能导致终端无法接入网络，直接影响员工办公。（备注：已经接入网络的终端，在准入控制服务器发生故障的情况下，不会断网。）为保障网络准入控制服务高可靠性，建议采取如下措施（如下图所示）：



- Radius 采用双机，通过在网络设备上设置多个 Radius IP 地址，网络设备会在第一台 Radius 服务器发生故障的情况下，自动切换到第二台 Radius 服务器。
- 主 Radius 服务器采用独立的硬件服务器，避免在其上面安装数据库或者其他应用软件，保障 Radius 服务器能够稳定、高效运行。
- User Cache 技术保证 AD/LDAP（用户名、密码验证）服务器故障情况下，不会导致准入控制服务立刻停止。所有曾经接入网络的用户账户，Radius 服务器会将其账户 Cache 在内存中，只要用户的账户不改变密码，下次接入时，就不需要重新到 AD/LDAP 服务器上认证。
- Policy Cache 技术保证数据库服务器故障情况下，不会导致准入控制服务停止。Radius 在完成准入控制认证过程中，需要访问管理员预先定义的准入控制策略，这些策略 Radius 会在启动时，自动到数据库中读取并缓存在内存中（Policy Cache 技术），并且在准入控制策略发生变化时，Radius 会收到后台程序的变更通知，自动更新 Cache。通过 Policy Cache 技术，即使数据库服务器发生故障也不会影响准入控制服务；通过采用 Policy Cache 和 User Cache 两种技术，既解决了准入控制中的数据库和 AD/LDAP 服务器的单点故障问题，同时通过内存 Cache 这种方式，大大提高了终端接入认证的速度。

- 3A down policy 或一键式撤防紧急逃生，优先保障网络的连通性。
- 也可以通过部署额外的 MiniRadius 服务器逃生，当系统出现物理故障时，可以迅速切换到 MiniRadius 服务器紧急恢复网络，直接放行所有网络接入请求。

3.5.2 灾难恢复

考虑到准入控制系统作为一个特殊的关键生产系统，必须考虑特殊灾难情况的发生。

本方案采取两种措施应对灾难情况：

- 单个准入控制服务组件发生故障，如：Radius、DB、AD/LDAP 服务器

UniNAC 可以自动监测这些服务器的运行状态，一旦这些服务器发生故障，系统可以通过手机短信、电子邮件、电话、语音等方式予以及时的告警。这样系统管理维护人员可以及时采取修复措施，保障系统的冗余度。

- 多个准入控制服务组件发生故障，如两台 Radius 服务器同时发生故障

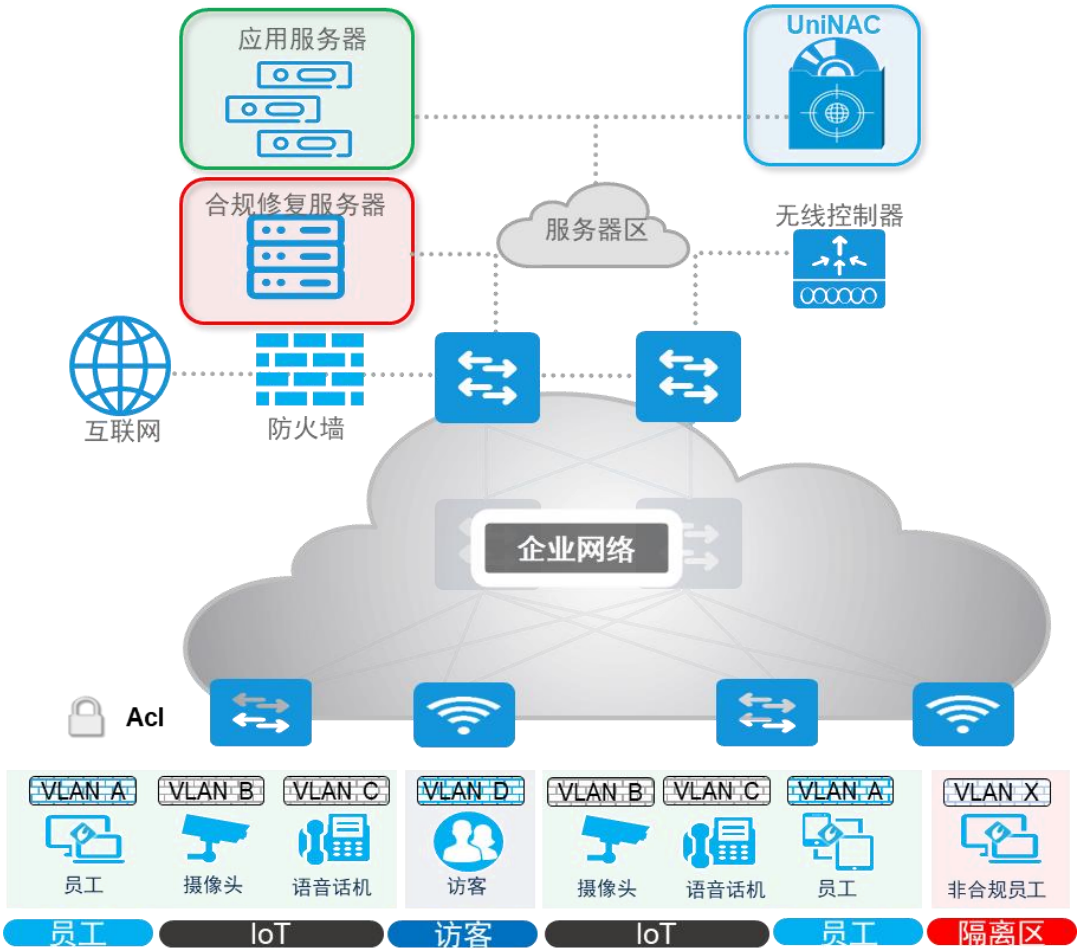
在部署准入控制系统时，提供“一键式”复原脚本，系统管理维护人员只需要在灾难发生时，鼠标点击执行复原脚步（在 3—5 分钟内执行完毕），即可临时撤销准入控制，保障用户可以继续接入网络。

四 部署方案

4.1 802.1x 组网方案

1）组网示意图

联软 UniNAC 可以配合接入层交换机，通过 802.1x 认证技术实现对接入用户的控制。在这种组网方案中，策略强制执行点在接入层交换机上，具有对不符合安全策略的用户隔离严格的特点，可以有效防止来自网络内部的安全威胁，适用于绝大多数企业网络环境，并且可灵活性选择现有设备可实现的认证方式，802.1x 组网方案如下图所示：



2）权限规划

采用 802.1x 组网方案时，不同类型人员和设备可采用的认证方式如下所示：

准入技术	是否安装客户端	入网终端类型	接入方式	认证方式	访问控制

802.1X	有代理	PC 终端	有线、无线	内置账号、AD 域、邮箱、证书、第三方	身份认证失败：接入失败 VLAN，受限 ACL； 安检失败：修复区 VLAN，受限 ACL； 安全规则校验失败：修复区 VLAN，受限 ACL； 认证成功：工作区 VLAN（绑定用户、部门），允许接入 ACL（绑定用户、部门）。
		外协	有线、无线	内置账号（驻场外协管理）	
		移动终端	无线	内置账号、AD 域、邮箱、第三方	
	无代理	PC 终端	有线、无线	内置账号、AD 域、邮箱、第三方	身份认证失败：接入失败 VLAN，受限 ACL； 安检失败：修复区 VLAN，受限 ACL； 安全规则校验失败：修复区 VLAN，受限 ACL； 认证成功：工作区 VLAN（绑定用户、部门），允许接入 ACL（绑定用户、部门）。
		外协	有线、无线	内置账号（驻场外协管理）	
		移动终端	无线	内置账号、AD 域、邮箱、第三方	
		哑终端、IoT	有线、无线	Mac 地址白名单	身份认证失败：访客区 VLAN，受限 ACL； 安全规则校验失败：修复区 VLAN、受限 ACL； 认证成功：工作区 VLAN，允许接入 ACL。

采用基于 802.1x 的 UniNAC 组网方案，主要通过划分不同权限的 VLAN 或设置不同权限的 ACL 来实施网络访问控制：

- 设立一个单独的 VLAN/ACL 作为访客区，并可以选择性的在访客 VLAN 部署探测器。访客区通常是给外部访客使用，一般只能用来做 internet 访问。当终端未安装 802.1x 代理，将会被切换到访客区。假如在访客区部署了探测器，那么当访客终端上网时将会被重定向到 802.1x 代理的安装页面，强制安装代理。管理员可以在确认访客身份后，停止对其重定向。
- 设立一个单独的 VLAN 做为修复 VLAN。当终端通过身份认证，但健康状况检查不通过的时候，将会被切换到这个 VLAN。这个 VLAN 通常设置一些文件服务器，以便终端对其安全缺陷进行修复。
- 当身份认证失败时，用户将被拒绝接入或切换到一个特定的 VLAN。当

身份认证和健康状况检查都通过后，终端才会切换到正常的工作 VLAN。

- 设立一个单独的工作区，当合法用户通过认证、检查并成功进入网络后，规定用户可以访问的网络资源，如：文件服务器、邮件服务器、其它应用系统等。

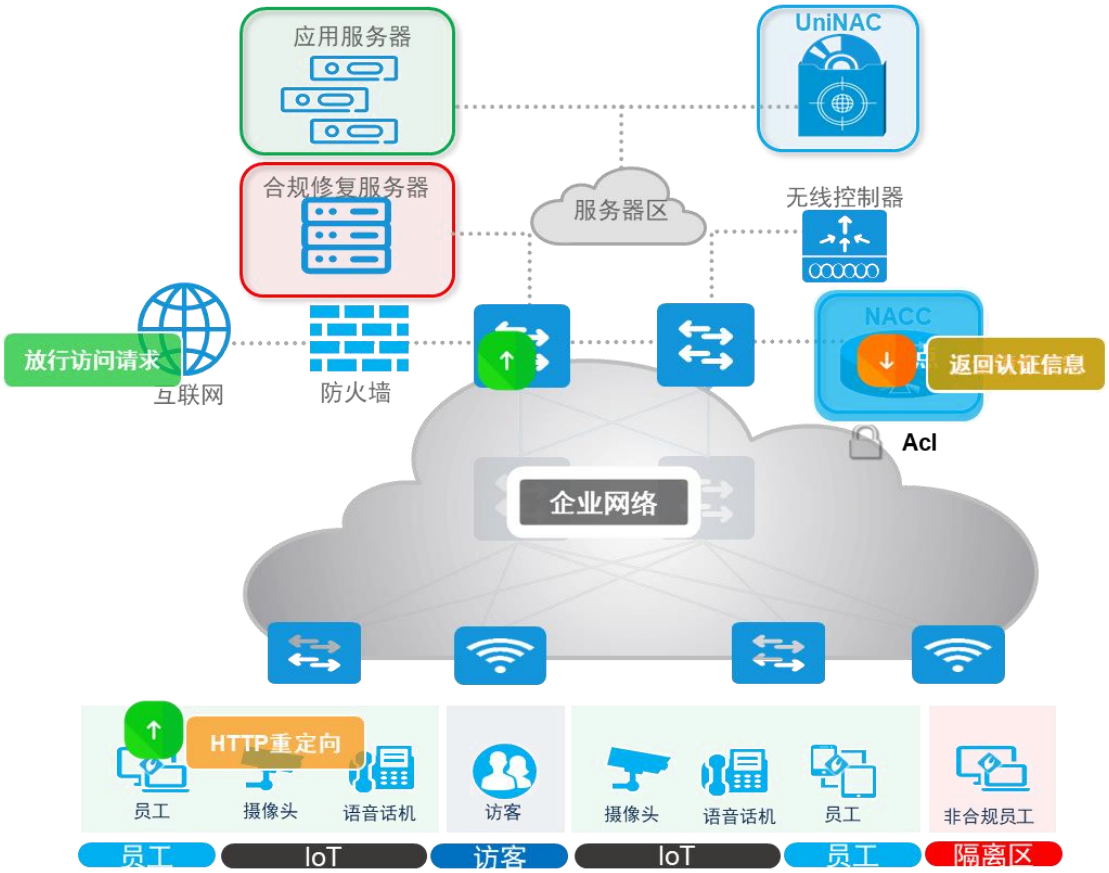
4.2 基于联软 NACC 准入控制器的组网方案

1）组网示意图

当用户网络环境由于接入层和汇聚层/核心层网络设备不支持相关技术，以至于无法采用 802.1x 组网方案或 EoU 组网方案（接入层交换机或者 AP 不支持 802.1x 协议、汇聚层/核心层不支持 Cisco EoU 协议），可采用基于联软 NACC 准入控制器的组网方案。

与 802.1x/EOU 相比，联软 NACC 准入控制器是一种基于 Cisco EoU 协议的硬件网关型网络准入控制设备，采用该方案实现准入控制，业务实现流程清晰可靠、环节少，用户只需要购买少量网关设备，并通过网关方式或者旁路方式部署至网络关键节点处（具体部署方式参见 2.2.3 节），即可实现全面的准入控制。

基于联软 NACC 准入控制器的组网方案如下图所示：



2）权限规划

采用联软 NACC 准入控制器组网方案时，不同类型人员和设备可采用的认证方式如下表所示：

准入技术	是否安装客户端	入网终端类型	接入方式	认证方式	访问控制
NACC	有代理	PC 终端	有线、无线	内置账号、AD 域、邮箱、证书、第三方	身份认证失败、安全检查失败、安全规则校验失败：限制接入 ACL；认证成功：允许接入 ACL（绑定用户、部门）。
		外协	有线、无线	内置账号（驻场外协管理）	
		移动终端	无线	内置账号、AD 域、邮箱、第三方	
	无代理	PC 终端	有线、无线	内置账号、AD 域、邮箱、第三方、指纹	身份认证失败、安全规则校验失败：限制接入 ACL；认证成功：允许接入 ACL（绑定用户、部门）。
		外协	有线、无线	内置账号（驻场外协管理）	
		移动终端	无线	短信、扫码、指纹	

		访客	无线	内置账号、AD 域、邮箱、第三方	身份认证失败：限制接入 ACL； 认证成功：允许接入 ACL（只能访问互联网）。
		哑终端、IoT	有线、无线	IP 地址白名单、指纹	安全规则校验失败：限制接入 ACL； 认证成功：允许接入 ACL（受限访问）。

采用基于 EoU 的 UniNAC 组网方案，主要通过划分、下发不同的 ACL（访问控制列表）来实施网络访问控制，包括：

- 定义一个无需安装助手设备的 ACL 列表，此 ACL 列表主要是针对企业临时访客、客户进行的准入控制，临时访客和客户可以在不安装联软安全助手的情况下就可以接入网络，并访问系统定义的网络资源；
- 定义一个单独的未安装安全助手设备 ACL 列表，此 ACL 列表将被限制访问网络资源。当终端接入网络访问网络资源时，系统就会将终端设备划分到未安装助手设备的 ACL 列表中，同时还会重定向到 Cisco EOU 代理的安装页面，强制安装代理；
- 定义一个单独的身份验证失败 ACL 列表，此 ACL 列表也将被限制访问网络资源，当终端接入网络访问网络资源时，系统就会将终端设备划分到身份验证失败的 ACL 列表中，同时还会重定向到接入失败页面；
- 定义一个单独的安全检查不合规的修复 ACL 列表，此列表将被限制访问网络资源，当终端通过身份认证，但健康状况检查不通过的时候，将会被切换到这个 ACL 列表，这个 ACL 列表通常设置一些文件服务器，以便终端对其安全缺陷进行修复；
- 定义一个单独的身份和安全策略验证成功的工作 ACL 列表，当合法用户通过认证、检查并成功进入网络后，规定用户可以访问的网络资源，如：文件服务器、邮件服务器、其它应用系统等。

3）功能特性

采用联软 NACC 准入控制器的组网方案，还支持以下功能特性：

- 传统防火墙的功能，如针对 IP，协议设置策略，控制对网络内外资源

的访问，NAT；

- 依据应用（BT、Flashget、迅雷、MSN、QQ、网络视频应用）、站点（站点的名称，如新浪；站点的类型，如色情网站；站点的 IP 范围）等方式的访问控制；
- 对流经网关的信息的审计，包括按照用户名、IP 地址等进行流量统计，对访问过的站点的统计，记录往外传输的文件（email、FTP、http upload 等）；
- 对访问局域网的终端进行流量控制。

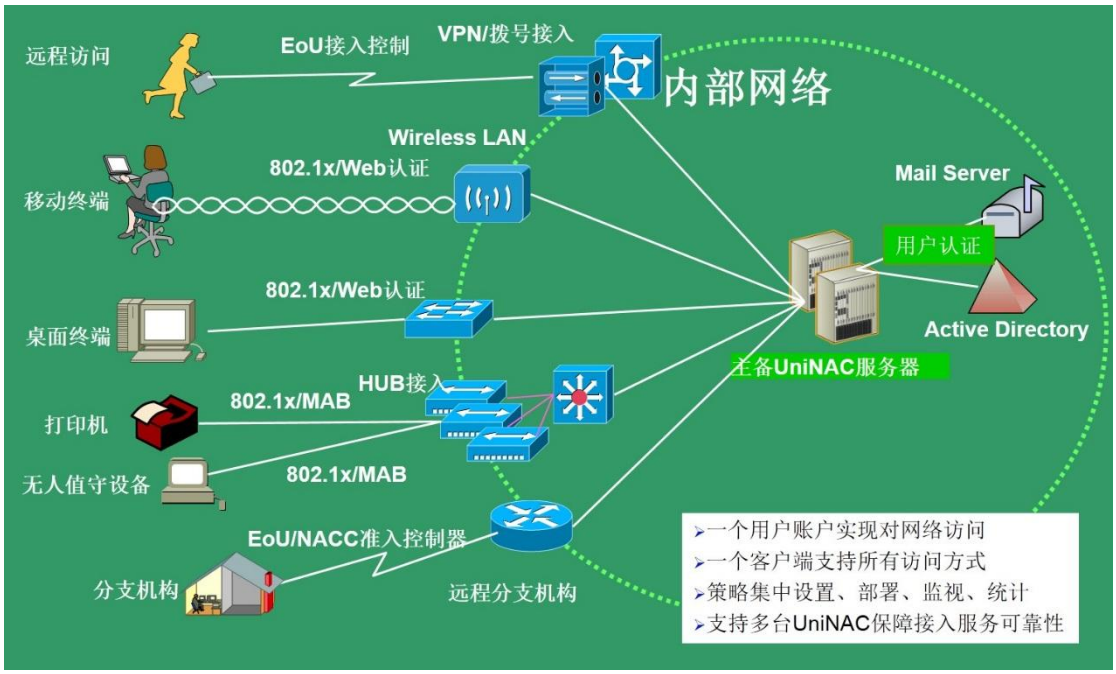
4.3 EoU 组网方案

如果接入层设备不支持 802.1x，联软 UniNAC 可以配合支持 Cisco 三层接入交换机，在这种组网方案中，安全策略的强制执行点在汇聚层交换机上，所以对接入层交换机要求非常低，支持 HUB 接入，且容易部署，不需要对接入层的交换机做任何配置，只需要在汇聚层少数几台交换机上就可以完成配置，并且对现有的网络环境不需要作任何调整。

联软 NACC 准入控制器基于 Cisco EoU 协议，EoU 组网方案同 NACC。

4.4 大型综合性网络解决方案

许多大型集团公司的网络，通常是由园区网、无线 Lan 网络、VPN/拨号接入，以及分支机构广域网等错综复杂的方式构成。针对这种环境，联软科技通过组合自身所支持的各种准入控制技术，来提供一个统一的、完整的解决方案。



采用 UniNAC 准入控制方案，可以帮助企业实现：

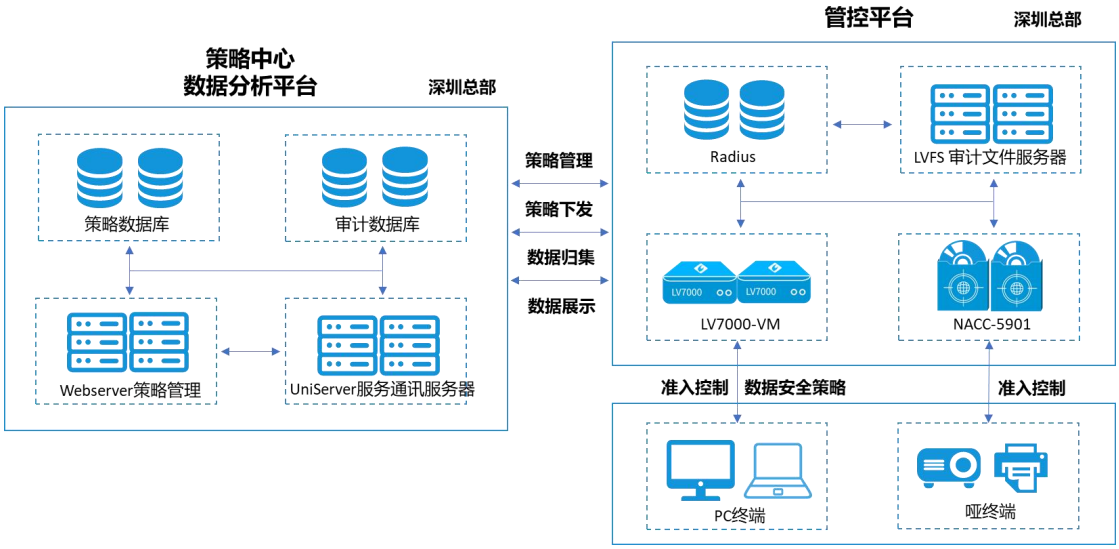
- 全面实施网络准入控制，不留安全死角；
- 各种准入控制机制通过 UniNAC 达到无缝集成，完全不存在不兼容问题，只使用一套产品就能实现各种准入控制；
- 灵活性强，用户可以随意组合和选择准入控制方案，能适应各种网络环境，在各种复杂的网络环境中实现准入控制；
- 统一认证，无论选用了多少种准入控制机制，都只需要一台 UniNAC 服务器来完成身份认证，所有的身份认证都可以集中到一台服务器完成，有利于对账户使用的集中审计。

4.5 部署架构

UniNAC 网络准入控制解决方案支持集中式部署和分级式部署两种部署架构，可充分满足了多种应用场景下的可靠性和可维护性问题。

4.5.1 集中式部署

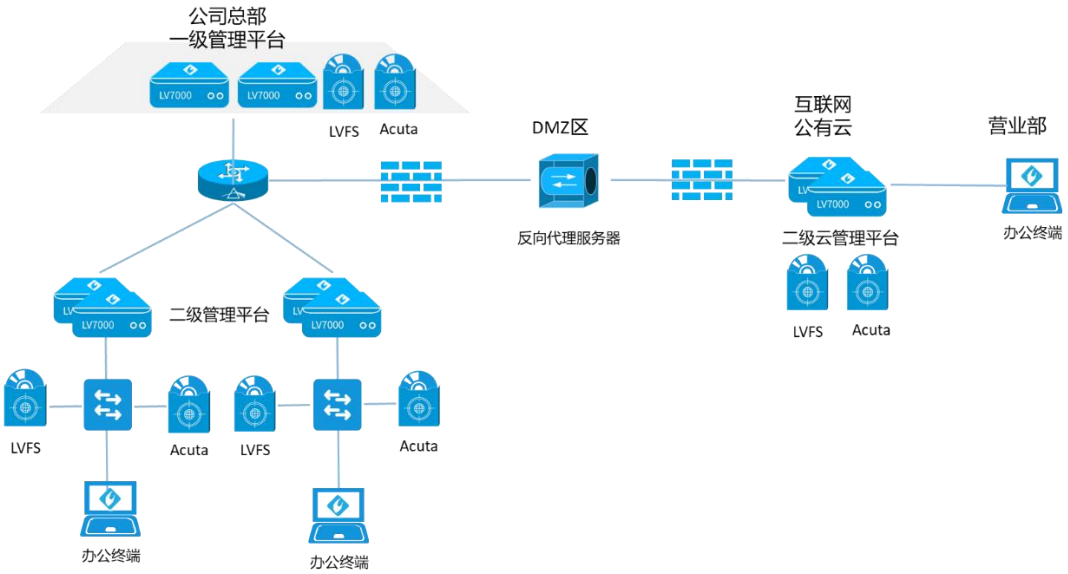
对于分支机构较小，或分支机构缺少专业 IT 管理人员的情况，联软科技建议采用集中式部署方式，由总部管理中心统一对包括总部、分支机构实现准入控制，如下图所示：



在这种模式下，企业实施准入控制总体成本较低，只需维护总部管理中心的 UniNAC 服务器即可，但是，这种部署模式对总部与分支机构之间的广域网连接的稳定性要求非常高，一旦总部与分支机构之间的网络产生拥塞或中断，往往会导致分支结构的终端无法接入网络，从而影响正常的业务操作。

4.5.2 分级式部署

对于分支机构规模较大，且分支机构拥有较为充足的 IT 管理资源，可以采取分级部署模式，并通过总部管理中心实现分级部署集中管理，如下图所示：



在分级部署模式下，UniNAC 分级管理模式可由最上级的管理员进行基础策略的统一定制，而后再进行逐层的下发。下级的管理员可以依据一级 UniNAC 管理服务器下发的策略进行继承和自定义等操作，从而生成更加满足本地需要的策略；

由各分级 UniNAC 服务器在本地实施准入控制策略。

同时，下级 UniNAC 服务器也支持通过信息上报的方式将相关的安全事件、审计信息上报给上一级 UniNAC 服务器，上级 UniNAC 服务器可以对这些统计数据进行查询以及汇总，并基于上报的统计数据给出统计报表。

分级部署模式下，即使分支机构与总部的广域网连接中断，也不影响分支结构的正常业务操作，且大量的审计信息保存在分支机构本地，可选择在合适的时间段上传至总部一级 UniNAC 服务器，从而实现最大的管理灵活性和稳定性。

五 方案优势与价值

5.1 方案价值

5.1.1 全网资产可视

自动设备发现、类型识别，生成网络拓扑快速定位；自动收集终端软硬件资产信息构建资产库；

自动识别设备与用户行为，可视化展现访问关系和使用习惯；

攻击可视化，智能识别网络攻击，可视化展现攻击入侵路径、横向移动过程、攻击方式等。

5.1.2 建立终端安全基线

终端安全合规控制：强制式与自助引导式结合，根据终端安全基线要求智能引导用户按步骤安全地接入网络；

真正的最小授权：直接与网络设备联动，自动下发 VLAN 和 ACL，安全控制粒度细，与安全助手结合可感知应用类别，实现资源访问控制，保障内网终端满足安全基线要求，够防止非法外联，减少终端违规行为；

主动防御安全对抗：生成大批量的幻影设备，并通过主动诱捕技术将攻击行为引诱到幻影设备上。

5.1.3 基于角色访问控制

用户通过角色与权限进行关联，实现最小权限原则的访问控制，减少内部被横向渗透的风险。

5.1.4 统一管理简单运维

集中化全面管控平台，降低安全管理复杂度，提高管理效率，减少人力投资。

5.1.5 满足安全合规遵从

解决内网安全管理问题，让各种安全管理规范落地。

5.2 方案优势

5.2.1 适应各种复杂网络环境

- 各种网络接入场景：支持 802.1x、Portal、NACC 网关等多种准入控制技术，不依赖于任何一家硬件设备厂商，适用于 LAN、WLAN、VPN、NAT、分支机构接入等各类复杂环境，UniNAC 真正实现了，让每一台接入网络的终端，都接受客户的管理；
- 多种部署模式：支持有代理、无代理终端部署模式，兼容各厂商网络设备，准入实施经验丰富；
- 产品可靠性高：技术成熟稳定，通过五重冗余保障技术实现网络准入的高可用性，金融、企业、运营商等各行各业案例多。

5.2.2 平台级解决方案

- 一体化平台：同一管控中心、同一 Agent、统一管控策略、统一账号管理、统一流程管理；
- 扩展性强：可在同一平台扩展终端安全、数据防泄密、移动安全等功能模块，支持未来大容量网络审计数据查询及分析；
- 开放集成：提供第三方功能扩展开发接口，可与用户 OA、AD、SOC、上网行为管理等系统集成联动。

5.2.3 业界领先与可靠的网络准入控制解决方案

UniNAC 为众多高端企业客户追捧的原因，在于 UniNAC 能够为高端企业客户提供业界最为先进与可靠性的 NAC 解决方案。其先进性体现在：

- 产品架构

准入控制架构最为简单，最为丰富、灵活的准入控制策略，最可靠的准入控制。部署方便，组网灵活、支持大规模组网；不用改变网络的结构、路由，不会带来性能瓶颈与新的故障隐患。

- 适用各种环境

支持的接入方式最为完善，支持 LAN 方式的 802.1x，WLAN 方式的 802.1x，以及远程、VPN、HUB 等接入方式的准入控制。

- 高可靠性

Radius 双机、Policy Cache 技术、Account Cache 技术，消除了准入控制中的单点故障；对于紧急故障处理，无需人工干预，自动撤防，启用 AAA Down Policy 或一键式撤防；接入故障诊断一目了然，一个界面分析出所有问题（如：端口、认证、策略、绑定）。

- 高性能

每分钟 48000-96000 终端的准入验证效率，每秒 800-1600 用户。

- 全面支持信创

5.2.4 与网络设备紧密集成，既方便管理又减少投资

UniNAC 通过直接与网络设备联动的方式，控制终端的接入、控制终端的访问权限、定位终端的位置等，大大简化了终端管理的工作的复杂度，提高了效率。例如：UniNAC 能够依据 IP、MAC 地址等，快速找到对应的终端设备所连接的交换机端口，并且需要时候可以对交换机的端口直接进行“关闭、启用”这样的操作。

UniNAC 能够自动对网络设备（如：Cisco、华为、H3C 品牌）的配置进行自动备份，减轻网络管理员的工作量，提高网络的安全性。

UniNAC 是业界第一家，也是目前唯一一家将终端安全管理与网络设备紧密集成的产品。UniNAC 不需要专用的硬件设备，即可实现网络准入控制与终端的各种管理任务，而这种方案和技术，既方便对终端的管理又减少了硬件设备投资。