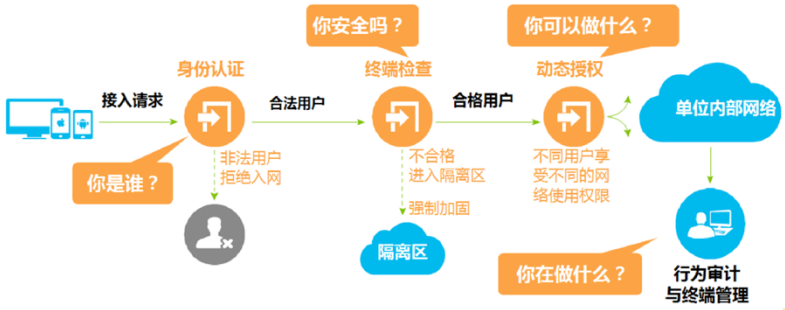
UNIS EAD 终端准入控制解决方案

目前，在企业网络中，用户的终端计算机不及时升级系统补丁和病毒库、私设代理服务器、私自访问外部网络、滥用企业禁用软件的行为比比皆是，脆弱的用户终端一旦接入网络，就等于给潜在的安全威胁敞开了大门，使安全威胁在更大范围内快速扩散，进而导致网络使用行为的“失控”。保证用户终端的安全、阻止威胁入侵网络，对用户的网络访问行为进行有效的控制，是保证企业网络安全运行的前提，也是目前企业急需解决的问题。

网络安全从本质上讲是管理问题。UNIS 终端准入控制（EAD，End user Admission Domination）解决方案从控制用户终端安全接入网络的角度入手，整合网络接入控制与终端安全产品，通过安全客户端、安全策略服务器、网络设备以及第三方软件的联动，对接入网络的用户终端强制实施企业安全策略，严格控制终端用户的网络使用行为，有效地加强了用户终端的主动防御能力，为企业网络管理人员提供了有效、易用的管理工具和手段。

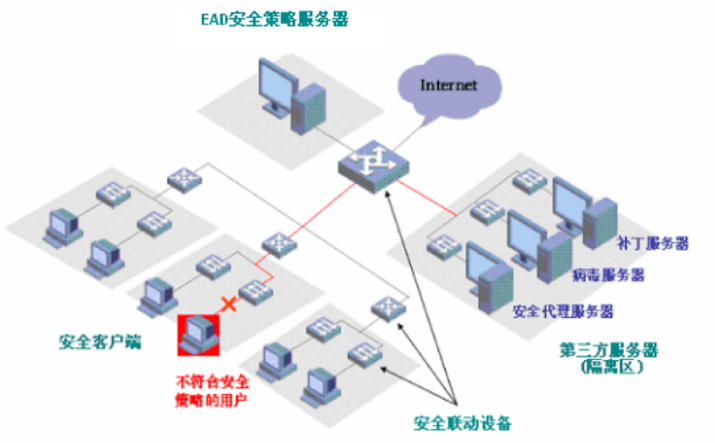
方案概述

对于要接入安全网络的用户，EAD 解决方案首先要对其进行身份认证，通过身份认证的用户进行终端的安全认证，根据网络管理员定制的安全策略进行包括病毒库更新情况、系统补丁安装情况、软件的黑白名单、U 盘外设使用情况、软硬件资产信息等内容的安全检查，根据检查的结果，EAD 对用户网络准入进行授权和控制。通过安全认证后，用户可以正常使用网络，与此同时，EAD 可以对用户终端运行情况和网络使用情况进行审计和监控。EAD 解决方案对用户网络准入的整体认证过程如下图所示：



组网模型

如下图所示，EAD 组网模型图中包括安全客户端、安全联动设备、EAD 安全策略服务器和第三方服务器。



安全客户端：是指安装了 UNIS iNode 智能客户端的用户接入终端，负责身份认证的发起和安全策略的检查。

安全联动设备：是指用户网络中的交换机、路由器、VPN 网关等设备。EAD 提供了灵活多样的组网方案，安全联动设备可以根据需要灵活部署在各层比如网络接入层和汇聚层。

EAD 安全策略服务器：它要求和安全联动设备路由可达。负责给客户端下发安全策略、接收客户端安全策略检查结果并进行审核，向安全联动设备发送网络访问的授权指令。

第三方服务器：是指补丁服务器、病毒服务器和安全代理服务器等，被部署在隔离区中。当用户通过身份认证但安全认证失败时，将被隔离到隔离区，此时用户能且仅能访问隔离区中的服务器，通过第三方服务器进行自身安全修复，直到满足安全策略要求。

功能特点

◆ 全方位准入控制

EAD 解决方案提供完善的接入控制，可以支持局域网、广域网、VPN、无线各种接入方式，支持包括 HUB 在内的各种复杂网络、思科等异构网络环境下的部署，保证从任何地点、任何方式下的接入安全。

◆ 严格的身份认证

除基于用户名和密码的身份认证外，EAD 还支持身份与接入终端的 MAC 地址、IP 地址、所在 VLAN、接入设备 IP、接入设备端口号等信息进行绑定，支持智能卡、数字证书认证，增强身份认证的安全性。

◆ 完备的安全状态评估

根据管理员配置的安全策略，用户可以进行的安全认证检查包括终端病毒库版本检查、终端补丁检查、终端安装的应用软件检查、是否有代理、拨号配置、U 盘审计、外设管理、桌面资产管理等；EAD 客户端支持和瑞星、江民、金山、Symantec、MacAfee、Trend Micro、安博士、卡巴斯基等国内外主流病毒厂商联动，同时为了更好的满足客户的需求，也支持与微软 SMS、LANDesk、BigFix 等业界高端的桌面安全产品的配合使用。例如已经购买微软的桌面管理工具 SMS 的用户，EAD 可以与 SMS 配合，由 EAD 实现终端用户的准入控制，由 SMS 实现各种 Windows 环境下用户的桌面管理需求：资产管理、补丁管理、软件分发和安装等。

◆ 精细化的权限控制

在用户终端通过病毒、补丁等安全信息检查后，EAD 可基于终端用户的角色，向安全联动设备下发事先配置的接入控制策略，按照用户角色权限规范用户的网络使用行为。终端用户的所属 VLAN、ACL 访问策略、是否禁止使用代理、是否禁止使用双网卡等安全措施均可由管理员统一配置实施。

◆ 灵活方便的执行方式

EAD 按照网络管理员配置的安全策略区别对待不同身份的用户，定制不同的安全检查和处理模式，包括监控模式、提醒模式、隔离模式和下线模式。用户可以根据自己的实际需要，为 VIP 客户、内部员工、外来访客等不同人群，定义不同的安全策略执行方式。

◆ 桌面资产及外设管理

EAD 解决方案提供了对终端资产全方位的监控和管理的功能，可以对终端软硬件使用情况、变更情况进行监控，同时还支持终端资产的配置管理和软件的统一分发、远程桌面控制，实现对桌面资产的有效管理。EAD 解决方案还提供了对 U 盘和其他外设的管理功能，可以对终端用户的各种外设进行控制，有效防止重要信息的泄密，同时提供 U 盘文件的监控功能，可以查看重要文件通过 U 盘拷贝时，有无存在不当使用行为。

◆ 易于部署的无客户端

EAD 解决方案提供了免安装的易用部署方式，用户事先不需要安装客户端，上网时 EAD 系统会自动载入客户端，对用户身份和终端安全状态进行检查，用户不需要改变上网习惯的同时，可以享受 EAD 带来的安全保障。

◆ 多种层次的高可用性

EAD 解决方案提供了双机冷备和双机热备功能，可以避免单台 EAD 服务器当机引起的认证中断，同时还支持单机故障的逃生方案，临时允许客户端不用认证就可以使用网络，保证了经济敏感用户的利益。

◆ 扩展开放的解决方案

EAD 解决方案为客户提供了一个扩展、开放的结构框架，最大限度的保护了用户已有的投资。EAD 广泛、深入的和国内外防病毒、操作系统、桌面安全等厂商展开合作，融合各家所长；EAD 与第三方认证服务器、安全联动设备等之间的交互基于标准、开放的协议架构和规范，易于互联互通。

北京紫光恒越网络科技有限公司

http://www.unishy.com

北京基地
北京市海淀区中关村东路 1 号院 2 号楼 402 室
邮编：100084
电话：010-62166890
传真：010-51652020-116
版本：

客户服务热线
400-910-9998