



创多软件

# 创多准入安全 控制系统

主动评估 安全接入

## DISADVANTAGES

01

### 开放网络的弊端

## LAS SOLUTIONS

02

### LAS终端准入控制方案

◀ 在接入层分区	03
◀ 协同与联动	04
◀ 接入认证	05
◀ 策略强制	06
◀ 防止非授权访问	07
◀ 主机健康性检查	08
◀ 隔离与修复	08
◀ 安检报告	09
◀ 网络安全风险评估	10
◀ 安全域管理与控制	10
◀ 日志与告警	10
◀ 完整的报表系统	11
◀ 应急系统	11
◀ 网络环境适应性	12
◀ 消灭网络安全弱点	12
◀ 终端系统兼容性	12

## DEPLOYMENT DIAGRAM

13

### 典型部署示意图

## PRODUCT TYPE

14

### 产品型号参数

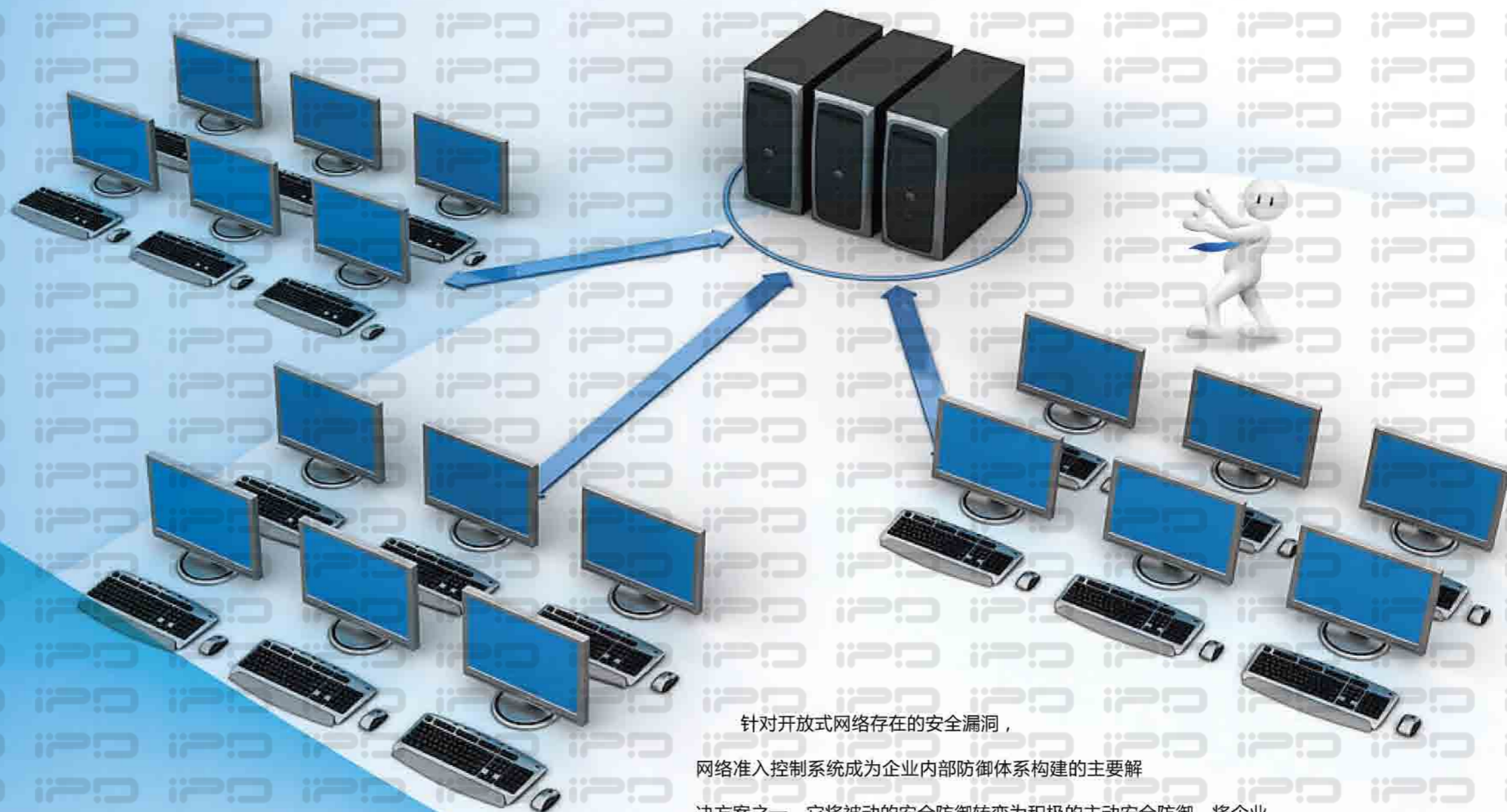
调查数据表明堡垒往往是从内部攻破的，我们过去在Internet接入安全和服务器安全领域投入了大量的投资，但是网络安全事件依然层出不穷，为什么？

来自终端的威胁是很容易被我们忽视的，病毒、木马等破坏程序往往利用终端作为媒介进行入侵和感染，通过网络在堡垒内进行传播的。所以仅仅修建一个坚固的外壳是不够的。我们需要对进出堡垒的“人”进行身份甄别和安全检查以保证内部的安全。

目前大多数企业构建的还是开放式的网络，虽然在互联网接入层部署了防火墙等安全防护设施，但从内网的接入层，却依然采用开放式的网络架构，这种开放性给企业业务开展确实能够带来便捷，但随着IT技术的快速发展，各种网络应用的日益增多，病毒、木马、蠕虫以及黑客程序等等不断从内网带来威胁并入侵企业内部网络资源，使得企业网络的安全边界迅速缩小，开放的内部网络访问严重影响了企业IT基础设施的安全和稳定，因此必须构建新一代的内部网络安全防御体系。



在具体表现层面，开放式的网络使得企业内部任何一个人都能够通过便捷计算机接入企业的核心业务网络，能够访问企业的各种网络资源，获取他们感兴趣的数据。开放式的网络犹如企业没有门卫一样，任何人都可以随意进出，不受到任何检查和限制。可以想象这样的开放式网络为恶意访问提供了入侵网络的便利条件，采用非常简单的攻击技术便可以造成巨大破坏，从而不但给企业带来巨大的经济损失，更有可能对企业造成法律上的风险。



针对开放式网络存在的安全漏洞，网络准入控制系统成为企业内部防御体系构建的主要解决方案之一，它将被动的安全防护转变为积极的主动安全防护，将企业内部的网络构造起一道安全屏障，积极主动诊断多种网络访问设备的健康性，采用隔离管控和有效引导的方法，有针对性实施网络自我防御，做到可信计算机有条件访问网络，阻止非授权以及有“问题”的计算机私自访问网络带来安全隐患。

作为专业的网络安全服务提供商，创多软件LAS终端准入控制系统，有效地解决了开放式网络存在的普遍性安全问题，系统通过基于802.1X协议的身份认证、基于主机特征的身份认证、终端安全检查、设备接入授权以及重定向受限访问、LDAP集成、DHCP集成、802.11无线网络支持等等技术和手段，使最终接入到内网的终端安全性得到保证。

在接入层分区



区域名称	区域描述
工作区	正常的工作网路，用户通过身份认证和安全检查后进入的网络。
访客区	供来宾和未通过身份检查的终端进入的网络，该网络与工作区网络是隔离的。
隔离区	通过身份认证但是没有通过安全检查的计算机进入的网络，在这个网络内计算机可以完成安检修复。

协同与联动



联动方式	实现功能
联动网络设备	联动网络层设备实现有效的网络控制的协同。
联动终端	联合防御，将控制的终端都加入到防御体系中，构建联合防御的“统一战线”。

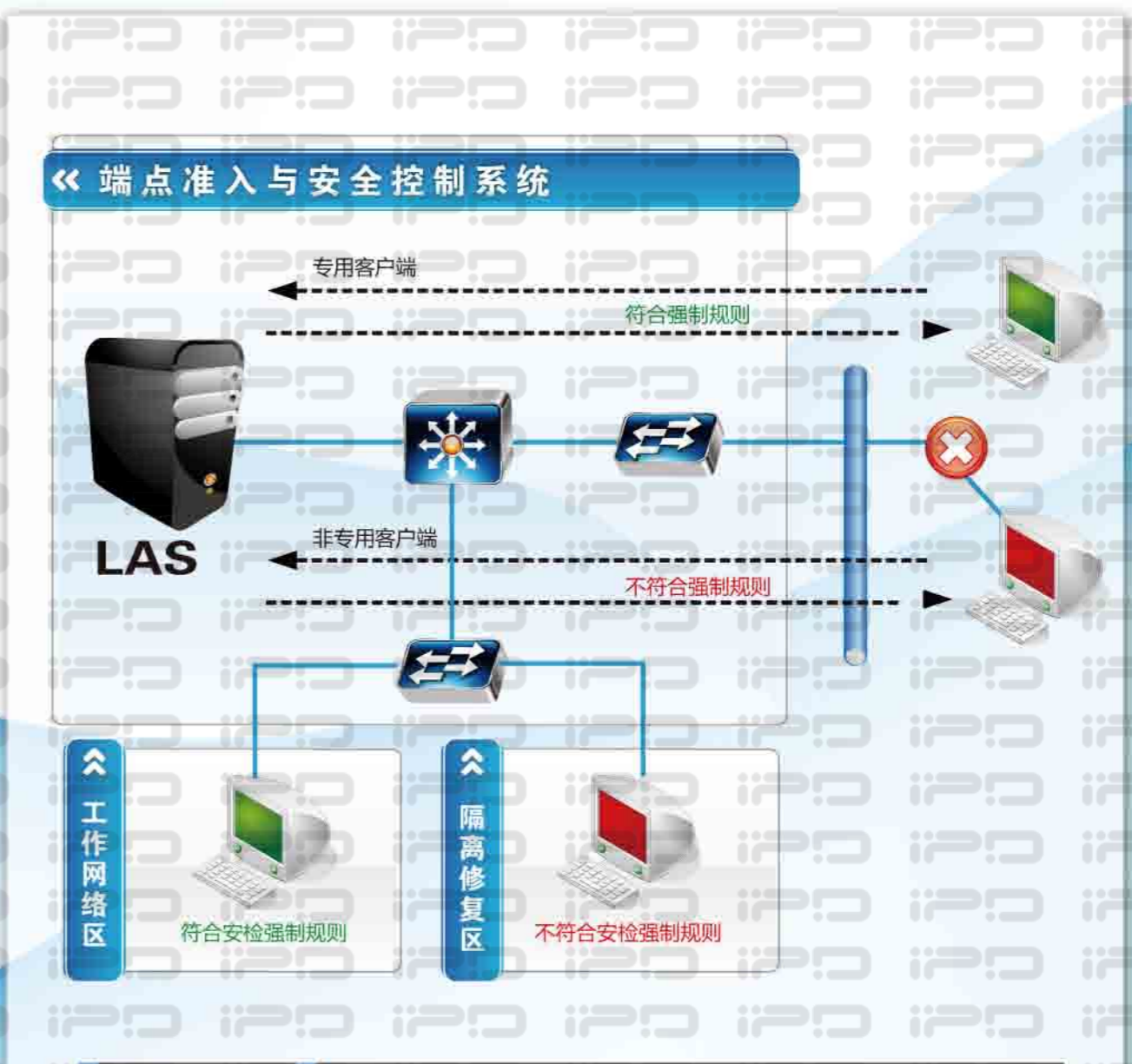
接入认证



**认证网络接入过程**

接入网络前用户必须提供身份凭据，如果认证通过网络可以正常使用，否则网络是不通的。

策略强制



强制类型	实现功能
认证强制	网络设备的dot1x认证强制协议层强制, 认证客户端类型强制。
安检强制	技术手段强制接入的终端进行安全检查, 建立安全检查与网络接入的互动机制。



## 防止非授权访问内部网络资源

企业复杂的网络环境是选择网络准入控制系统的难题，如今，企业网络包含着多种多样的网络设备和网络终端，用户访问内部网络也呈现出多样化发展。

为解决这些难题，LAS网络准入控制系统提出3不原则，即：不升级网络、不改变网络结构、不影响业务系统。最大化的支持企业内部网络准入控制系统，从而使内部网络管理变得安全、透明、可控。

- ◆ 支持被动式无客户端方式认证。
- ◆ 支持主动式客户端认证。
- ◆ 多样化的用户认证方式，完美支持与AD、LDAP整合，支持内建用户。
- ◆ 支持用户身份访问认证方式。
- ◆ 支持账户、IP、MAC、端口、时间绑定。
- ◆ 支持主机身份的访问认证方式，按照主机或设备的硬件ID进行认证。
- ◆ 支持基于用户身份接入点限制，管理者授权用户或终端只能在某接入点进行认证。
- ◆ 支持基于主机接入时间限制，管理授权用户接入使用时间。
- ◆ 支持802.1x、DHCP、VPN、HUB、无线等网络接入访问管理。
- ◆ 支持密码、令牌多因素认证。
- ◆ 动态检测系统与IP和MAC欺骗保护，防止私自更改IP。



## 主机健康性检查

LAS终端准入控制系统持续监视网络状态，能快速发现网络接入设备和计算机终端，并利用其独特的隔离管控技术立即将这个设备与网络上的其它设备隔离起来，同时依照安全策略条件进行认证授权管理。对于已授权的计算机终端或用户，如发现其已不符合安全策略，则LAS调用安全策略引擎立对该终端或网络设备的安全状态进行二次检查，期间禁止其访问企业网络，并引导修复安全漏洞，及时提供预警信息。在LAS安全策略配置中心，管理者可轻松定义安全策略，在设备与终端接入认证授权前或是认证授权后有效。

LAS支持安全检查内容：

- ◆ 操作系统检查，OS版本，SP版本、语言。
- ◆ 补丁检查，检查补丁完整性，检查指定补丁的安装情况。
- ◆ 防病毒检查，检查防病毒厂商，版本、病毒库版本。
- ◆ 自定义软件，检查用户指定软件的存在，可联动防病毒软件或防火墙。
- ◆ 关键位置文件检查，检查指定位置文件存在性。
- ◆ 外设使用安全，对移动存储设备自动播放检查，是否有接入移动存储设备。
- ◆ 系统账户检查，用户密码强度检查，用户的密码合规性，guest账户状态。
- ◆ 支持主机系统屏保检查，帮组用户开启屏幕保护。
- ◆ 注册表检查，检查注册表关键值是否存在。
- ◆ 支持网络配置检查，IP地址获取方式，域名欺骗检查，网络共享配置检查。



## 隔离与修复

### ◆ 终端软隔离

终端用户安全检查未通过时，终端计算机将进入隔离区进行相关不合规项目的修复，由于配置环境的差异，隔离区的实效效果会有所不同。在这里我们通过终端的专有客户在系统原有隔离区的基础上又在终端上增加的终端的网络访问限制，实现了硬件配置无关的软隔离。



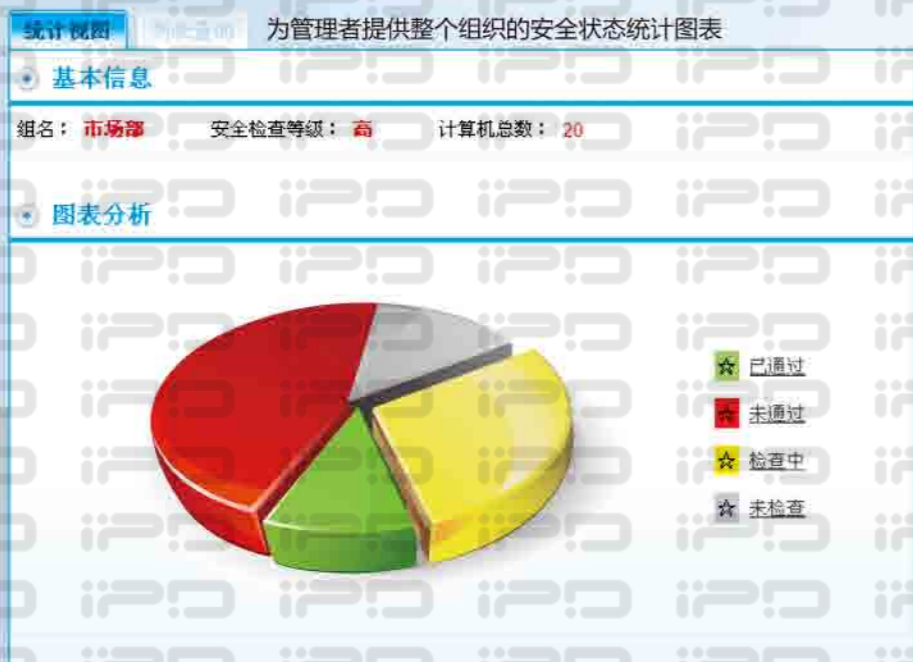
### ◆ 提示与修复



检查不是最终目标，要使接入计算机最终满足安全检查策略的各项要求，系统可以帮助用户和管理员一起完成计算机实现安全合规，同时还可以和公司的其他产品进行联动以提高自动化程度。

## 安检报告

安全状态统计图



终端安检明细报告

检查报告

计算机信息  
名称: zhangjun IP地址: 129.168.1.25 组名: 市场部

检查信息  
安全级别: 高 报告摘要: 共检查20项, 已通过16项, 未通过4项。

检查明细

检查项	当前系统危险项描述	描述
操作系统检查		
检查操作系统版本	XP 3.0	VISTA 3.0
检查操作系统语言	简体中文	简体中文
检查操作系统补丁包	补丁包	补丁包
补丁检查		
检查少选补丁安装情况	补丁检查不符合要求	
检查禁止安装补丁情况	补丁检查不符合要求	
配置检查		
检查IE版本	当前IE版本: 9	策略要求不低于: 9
检查IE的默认主页设置	当前主页: *	策略要求主页为: *
检查IE的代理设置	代理设置不符合要求	
检查IE的本地安全设置	本地安全级别为: *	策略要求的安全级别: *
检查IE的Internet安全设置	Internet安全级别为: *	策略要求的安全级别: *
防病毒软件检查		

## 网络安全风险评估



主动安全风险评估是LAS网络访问控制系统的另一特点, 根据积极主动的安全防御建设思想, 加强企业网络安全进行风险评估就显得尤为重要。LAS帮助管理者实现企业网络总体安全风险评估、部门安全风险评估以及指定计算机终端安全风险评估, 从而促使企业不断提高内部网络信息安全管理水平。

## 安全域管理与控制

利用LAS的动态检测技术, 针对接入内部网络的计算机终端实行多种安全策略的管理。



- ◆ 不符合安全策略的计算机终端进行友好提示, 提供向导式的安全修复指引。
- ◆ 拦截可疑的计算机终端或设备、恶意尝试认证的用户, 支持强制隔离下线和锁定功能。
- ◆ 支持访客管理, 外来访客仅能进入规划的安全访客区, 允许访问Internet, 但安全访客区与内网完全隔离。

## 日志与告警

LAS预警中心的快速检测扫描技术, 可迅速发现网络中非法接入者以及不符合安全检查条件的计算机终端用户。实时的安全信息通报机制, 帮助管理者快速查找和排除安全隐患。例如: 认证失败、非法尝试认证、不符合安全规则等。

用户的每次的网络接入认证、安全检查系统都会有详细的记录; 管理员对系统的所有管理操作也都会有详细的日志记录; 对日志的管理是分权的, 只有日志审计员才能进行日志的删除操作。



### 完整的报表系统

完整的报表能让管理者清楚地了解企业内网网络访问和使用情况，详细的日志信息帮助管理者轻松实现内网安全风险评估。及时掌握第一手安全资料，立即调整和加强安全策略。

- ◆ 实时记录认证信息和保存历史记录。
- ◆ 收集MAC、IP、使用者名称和接入点数据。
- ◆ 检索用户、群组、所在位置、状态。
- ◆ 输出PDF等报表格式。



### 网络环境适应性

早期的网络准入控制系统解决方案已被实践证明是过于复杂，不够灵活和难以部署。而LAS网络准入控制系统具有很强的网络环境适应能力，不要求用户升级网络，兼容新老设备，支持旁路部署，不构成单点故障。



### 应急系统

网络基础架构是IT基础架构中负责信息传输最核心的环节，因此为了保证服务的持续性和稳定性，对认证系统的稳定性提出了很高的要求，系统在如下几个环节作了充分的考虑。

#### ◆ 认证缓冲

当和外部身份认证系统集成使用时，为了提高效率和稳定性，系统会对认证的信息进行缓冲，即使外部系统暂时不可用时，认证依然可以正常进行。

#### ◆ Bypass开关

在认证链路出现重大问题时，为了保证网络的可用性，可以开启这个开关。开启后所有的网路接入认证暂时停止，关闭后恢复认证。

这个开关在紧急的时候很有用。

#### ◆ 旁路部署方式

LAS服务器是旁路部署对现有的网络拓扑结构没有变更，不但简化了部署还可以规避拓扑变更给稳定性带来的风险。

#### ◆ 双机热备



### 消灭网络安全弱点

LAS强制的安全策略让未通过授权的用户和设备远离网络，即在一个IPD LAS环境下，每一台访问网络的设备及其用户都必须通过严谨的认证、授权、健康度检查。未授权用户不得访问网络，而未通过健康检查的计算机终端则可以根据发现的漏洞或安全弱点来引导其进行修补，满足管理员设定的安全条件后访问合法的网络资源。



### 终端系统兼容性

◆ 为了最大限度保护用户的现有投资，系统在设计时充分考虑了系统对环境的适应性，尝试为用户屏蔽环境的复杂性，实现一个全认证的接入层网络。

◆ 兼容802.1x认证协议体系。

◆ 支持有线以太网网络，无线局域网、远程接入VPN网络的接入认证。

◆ 支持复杂的网络拓扑结构，例如：交换机级联、非802.1x网络。

◆ 网络设备兼容性：兼容思科、H3C、华为等厂商的设备。

◆ 客户端兼容性：

支持Windows 2000 family

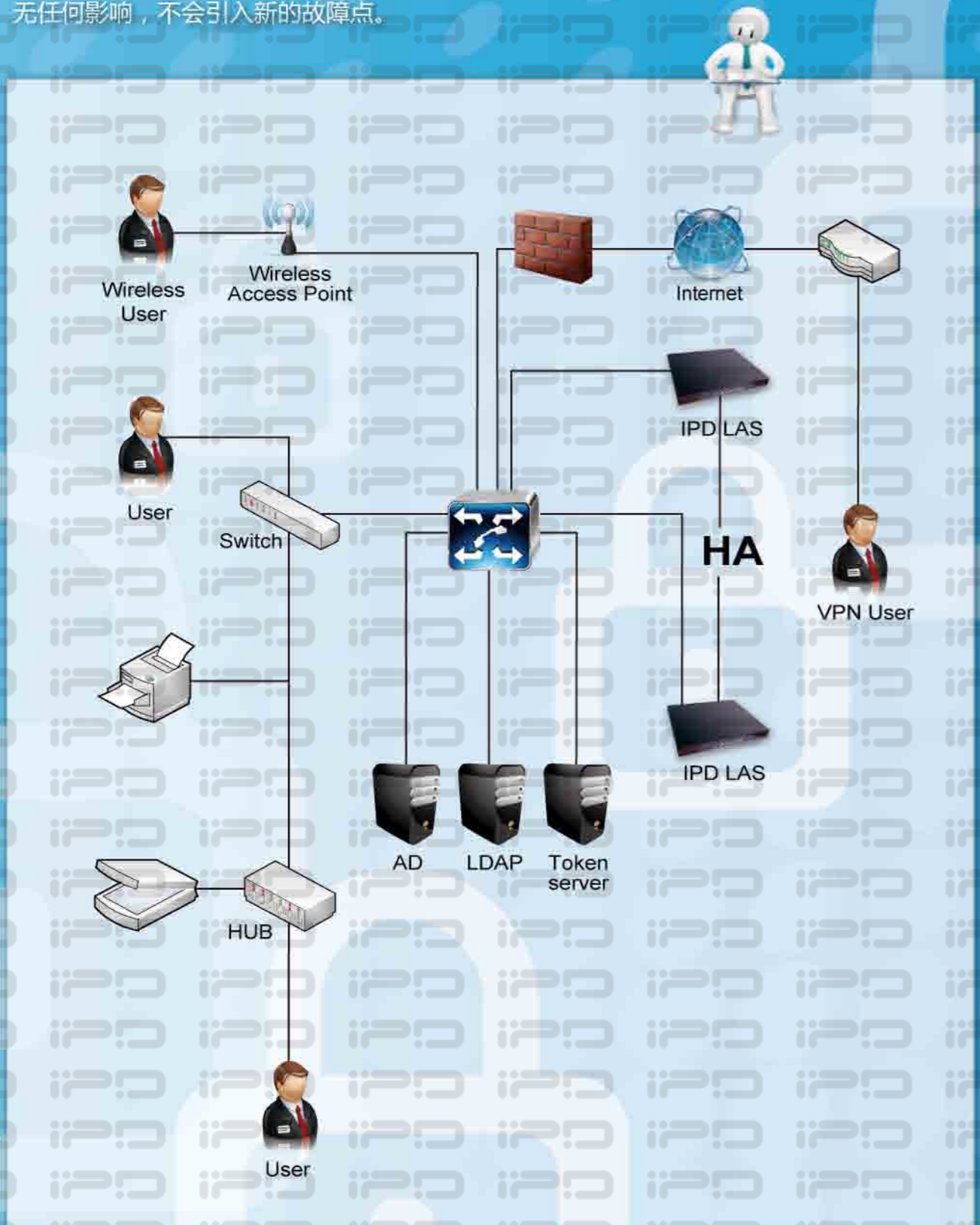
支持Windows xp family

支持Windows server 2003 family

支持Windows vista

支持Windows 7

LAS网络准入控制系统采用旁路部署，可减少对企业现有网络环境的改动，也避免造成单点故障。对于那些对网络连续性要求极高的企业，其优点是它对客户网络环境和网络性能无任何影响，不会引入新的故障点。



型号	L1100	L3500	L5100
可管理数量	100台	500台	1000台
<b>硬件配置</b>			
网络接口数(千兆)	6	6	6
Console接口(RS232)	1	1	1
内存	最大4G	最大4G	最大4G
存储	SATA HDD/CF	SATA HDD/CF	SATA HDD/CF
<b>物理参数</b>			
机箱尺寸(W×D×H)	1U (430×395×44.5) ±0.2毫米	1U (430×395×44.5) ±0.2毫米	1U (430×395×44.5) ±0.2毫米
重量(千克)	10KG	10KG	10KG
<b>电气指标</b>			
输入范围	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz
额定功率	200~250W	200~250W	200~250W
电磁兼容	USA-Title 47 CFR, Part 15	USA-Title 47 CFR, Part 15	USA-Title 47 CFR, Part 15
抗干扰性	CISPR 24	CISPR 24	CISPR 24
<b>使用/储存环境</b>			
储存环境温度	-40 - 75°C	-40 - 65°C	-40 - 65°C
工作环境温度	0 - 40°C	0 - 40°C	0 - 40°C
工作环境湿度	8 - 90% 无结霜	8 - 90% 无结霜	8 - 90% 无结霜