园区网安全解决方案

当前企业园区网面临的安全挑战呈现多样化、复杂化，因此企业用户需要的也不再是单一层面的安全产品，需要的是立体、全面，可靠的安全解决方案。企业迫切需要找到一种稳定，可靠，策略强大，端到端的园区网整体安全解决方案，以保证企业园区网实现从内到外，从单一到整体，立体全面的信息安全建设。

园区网安全解决方案概述

华为公司以世界级的安全能力中心，优秀的安全解决方案团队为基石，立足于强大的电信级安全硬件系列产品，整合其它多功能软件安全产品，为企业客户打造环境适应性强、体验友好、可靠性高的园区网安全整体解决方案。

该解决方案立着眼于企业当前安全威胁痛点，如：“外来人员随意接入，企业内部人员越权访问导致企业信息泄密；园区网的网络边界隔离手段单一，内部网络区域划分不合理，容易遭受攻击和传播病毒，造成核心业务中断，网络瘫痪；远程分支机构或移动办公人员缺乏有效的安全机制接入园区网络；缺乏有效的分析，管理，审计手段，跟踪安全事件等，以防、控、管、治，审为根本手段，通过多项易于部署和管理的精细化设计，给客户带来安全可靠、运行无忧的管理体验，并且能够最大限度的帮助企业减少因安全问题造成的经济损失，节约企业的运营成本。

方案组成

通过分析园区网的安全诉求，华为公司给出立体层次，全面防护，安全可靠的安全解决方案。园区网安全解决方案立足于强大可靠的安全准入机制，安全可靠的远程接入方式，强大的攻击防护和入侵检测能力，高业务连续性的设计，实时智能的统一安全运行状态的监控和管理平台，为企业用户打造立体的安全防护体系。整个解决方案涵盖五个维度（内网安全准入，远程安全接入，攻击防护，网络边界防护，安全管控/设备管理/安全审计），包括多个子安全解决方案。全景图如下：

华为园区网安全解决方案全景图

华为园区网安全解决方案以立体层次，全面防护，安全可靠为出发点，立足于领先的技术优势，为客户的园区带来良好的运营态势，成就客户的业务价值。

立体层次：关注园区网的安全准入，远程接入，边界防护和攻击防护等安全维度，并对园区网由外到内的安全设备和行为进行管理和审计，助力企业打造立体的安防体系。

全面防护：立足于防、控、管、治、审等安全防护面，提供全系列的信息安全防护产品与专业化的安全解决方案，为园区网企业客户提供全方位的安全保障。

安全可靠：以业界最强的网络协议分析团队以及最全的协议知识库为根本，以业界领先的研发能力和专利技术为导向，设计出由业界最稳定最可靠的安全产品组成的安全解决方案，保障园区网的可持续运营，业务永续。

方案特点

华为园区网安全解决方案拥有业界网络准入控制环境适应能力最强，应用识别能力最高的安全准入解决方案；拥有全面融合，功能丰富，性能可靠，安全性高的远程安全接入解决方案；拥有全面防护，高性能，高检测率，高攻击响应，高可靠性，并能足够细致地评估和保证企业安全解决方案合理性的攻击防护安全解决方案；拥有提供完整防火墙功能和 UTM 扩展能力，高病毒检测率，涵盖有线到无线统一安全接入的边界防护安全解决方案；拥有领先的全面设备日志采集性能，强大的关联分析引擎感知安全态势，完善的安全服务体系，可视化和高效率的安全设备管理，全面审计安全行为的安全管控、管理和审计安全解决方案。

华为园区安全解决方案是业界领先且能提供全面防护的安全解决方案，各子方案使用的安全产品拥有业界领先的安全能力，并且可靠性高，管理平台开发兼容第三方厂家的安全产品，方便扩容和管理。

园区网安全解决方案之安全准入

终端安全接入控制解决方案

华为终端安全接入控制解决方案，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。

华为终端安全接入控制解决方案的网络准入控制环境适应性强，终端用户体验一致且友好；管理方便，能有效降低运维工作量；能灵活扩展，支持云知识库更新；安全可靠，运行无忧；功能全面，涵盖终端安全管理所有方面。

上网行为管理安全解决方案

华为上网行为管理安全解决方案，专注于 Web 安全威胁，Web 以及应用控制两个维度，拥有业界最丰富的应用识别库，最全面的威胁防护库，并提供 URL 过滤，应用行为控制，流量管理，恶意软件防护，数据防泄密，上网行为审计等多项功能。它是为企业机构提供员工工作效率，营造安全办公环境，以及法规遵从的一体化上网行为管理安全解决方案。

华为上网行为管理安全解决方案，以覆盖超过 6500+的 URL 分类库，超过 1200 种应用的识别能力，助力员工高效办公，高速上网；以由高检出率，全面检测，迅速感知的 Web 信誉构成的多重威胁防护体系，确保员工上网安全。

园区网安全解决方案之远程安全接入

远程安全接入解决方案

华为远程安全接入解决方案能够给客户提供一个安全稳定的网络互联及数据交互平台，有助于提供企业信息化程度，实现实时的信息分享，优化企业商业运作的效率。通过运营商或专网部署企业 VPN（企业大中型分支机构互联），对企业的不同业务实现安全隔离，保证企业业务高质量的运行，同时可针对不同的业务作不同的 QoS。通过部署专业的 SSL VPN，可以为出差员工提供用户接入认证和数据加密，以保障出差员工可以随时随地接入企业园区，同时保障员工与企业之间数据交换的安全。

华为远程安全接入解决方案提供可提供丰富的接入方式，包括 L2TP、IPSec、GRE、MPLS、SSL 等单一 VPN 接入方式，还支持 L2TP over IPSEC、GRE over IPSEC 等复合 VPN 接入方式，可以满足用户的大多数 VPN 接入需求；并且配置灵活，可靠性高，易维护，支持在线并发用户数与隧道数升级。

移动终端安全接入解决方案

华为移动终端安全接入解决方案从移动终端安全、网络传输安全、应用安全、敏感数据安全，以及安全管理五个维度对移动办公进行全方位防护，帮助企业在 BYOD 的高效率与信息安全之间找到最佳平衡点。同时，为应对日益复杂的移动化环境，通过一个简单的平台，支持各种应用的移动化迁移，给开发工作带来良好的扩展性，更好的控制成本，使企业在全球化业务中获得竞争力。

华为移动终端安全接入解决方案，拥有强大的移动办公安全接入能力，能提供最广泛的移动终端适应性，支持 7 大等主流平台，用户可自由选择移动终端类型；并且具有最丰富的移动终端安全接入方式，支持 Web 代理、网络扩展、虚拟桌面、应用集成、L2TP/IPSec VPN，用户可灵活选择使用。

另外，该方案还提供完备的整体安全防护，采用主机检查、访问痕迹清除和安全桌面技术，确保用户终端设备安全访问业务资源，避免成为攻击跳板。同时以丰富的身份认证和灵活的授权管理为根本，提供基于 IP、端口、URL 的细粒度访问控制，保证了用户访问的可控可管。

园区网安全解决方案之攻击防护

DDoS 攻击防御安全解决方案

华为 Anti-DDoS 解决方案采用 DPI 检测技术，深入分析报文的每个字节，精心打造的“七层净化”架构可以有效识别流量型攻击、应用型攻击、扫描窥测型攻击和畸形包攻击等多种类型，确保流向客户的流量均为安全、正确的业务流量，基于应用的信誉防护体系和会话检测技术，提供业界首个“零误判”方案，支持所有攻击类型 IPv4/IPv6 共栈防御，防御种类业界第一。

华为 Anti-DDoS 解决方案是业界最“高”的解决方案，以基于 DPI 检测技术的高检出率，确保网络稳定运行；以秒级攻击响应的高响应速度，确保网络稳定运行。同时，它还是业界最“易”解决方案，易管理：低 OPEX，图形化管理，灵活取证，方便管理；易扩容：低扩容成本。

实时入侵检测安全解决方案

华为提供防护-检测-响应一体化的实时入侵检测安全解决方案，帮助用户定位各种网络威胁，以及违反安全策略的流量，并提供详实、有效的指导措施。入侵检测安全解决方案面向 Web2.0 及云时代的网络安全问题，提供了虚拟补丁、Web 应用防护、客户端保护、恶意软件防御、网络应用管控、网络及应用层 DoS 保护等功能。为园区网提供对网络基础设施、网络带宽性能、服务器及客户端的全面防护。

华为实时入侵检测安全解决方案，提供覆盖网络，从系统服务到应用软件的全面防护；以高速高效的检测引擎，进行全面的攻击检测；同时采用了虚拟引擎技术，可分区域部署检测规则；另外还提供完备的攻击特征库和专业的攻防团队以帮助改善方案。

安全渗透测试

华为安全渗透测试服务是由华为公司渗透测试专家从黑客的角度，对网络系统安全现状进行评估的一种方法。华为汇聚了一支多年从事安全攻防工作的信息系统安全渗透专家队伍，在业内具有较高声誉。渗透测试专家对园区网络环境进行深入的安全探测，识别网络漏洞，找出系统脆弱的环节，从而帮助用户快速地评估网络的安全状况。
华为安全渗透测试能足够细致地评估和保证企业安全解决方案的合理性，同时提供渗透测试报告来分析企业解决方案的合理性。

园区网安全解决方案之边界防护

边界访问控制安全解决方案

华为提供边界访问控制安全解决方案，对园区网内外网进行安全隔离，对园区网不同等级的安全区域进行安全隔离。阻止来自 Internet 的威胁，降低企业的安全风险，多安全区域隔离防护，确保企业内部威胁不能肆意扩散。

华为边界访问控制安全解决方案采用高性能的安全设备，最高可达 200G 吞吐量，为企业 Internet 出口提供可靠安全防护，并可以承载多业务；部署灵活，产品型号齐全，可以为企业总部，以及特定分支机构提供全面 Internet 出口安全防护。

网络防病毒安全解决方案

华为网络防病毒安全解决方案采用源自 Symantec 的杀毒引擎及病毒签名库，支持对 HTTP、SMTP、POP3 及 FTP 协议的病毒查杀，支持对蠕虫、木马、扫描机间谍软件等攻击行为的检测和防御。AVE 防病毒网关能全面防御网络中的病毒攻击和传播； 终端 AV 引擎保护终端免受病毒感染，阻止病毒向外传播； 服务器防毒软件保护服务器免受病毒感染。

华为网络防病毒安全解决方案采用文件级病毒扫描方式，保证病毒检测的完整性；提供仿真环境，虚拟执行技术，让病毒暴露其不良企图或者现出原形；通过静态启发式引擎实现一条签名覆盖上万种病毒变种；同时可在几小时内开发出新的脚本引擎并发布到工作的反病毒引擎上；以双引擎，立体防御，全面构建企业园区防病毒体系。

园区网安全解决方案之安全管控，设备管理和安全审计

统一安全管控中心安全解决方案

华为统一安全管控中心安全解决方案，能对 IT 设备和业务系统的日志集中采集、分类存储、关联分析，从海量安全事件中产生精确告警、定位安全问题，提升安全运维管理效率，并满足相关安全合规的要求。

华为统一安全管控中心安全解决方案能全面采集设备日志，实现集中化的企业日志管理，保护日志的完整性，使其满足日志合规性的要求。同时以领先的时间采集性能，实现海量数据的收集和分析，通过强大的关联分析引擎，帮助客户快速定位 IT 安全事件。

华为已经建立了安全基础库、安全能力研究中心、攻防试验室以及应急响应中心，并有一支强大的专业安全服务队伍，为统一安全管控中心安全解决方案提供安全能力保障，使其为客户实现最大价值。

统一设备管理安全解决方案

华为统一设备管理安全解决方案能够对现网中的安全设备进行统一管理，是安全解决方案的基础部分。 除了普通网管系统所具有的网元、拓扑、性能管理等通用功能外，针对安全设备特别开发了业务管理功能，包括安全策略集中统一配置，VPN 集中管理，实时性能监控，IPS 与 NAT 配置下发管理等功能，为用户提供了一个网络设备和安全设备统一的集中管理安全解决方案。

华为统一设备管理安全解决方案能够一网打尽全网的网络设备，轻松掌握设备最全面的状态数据；能够及时发现，快速精准的定位网络故障；以百万级的性能指标，监控并全面掌握网络和设备的运行状况；以高效的批量部署，轻松完成安全策略下发；提供最专业的 VPN 网络管理能力；同时以友好的拓扑管理功能，直观的了解网络结构，轻松定位网络设备。

上网行为审计

上网行为审计以可视化的审计报表，助力企业治理：面向管理层，提供办公效率、带宽利用、法律合规等综合和专项分析报表，协助发现问题，完善公司治理；面向技术层，提供 10 余种查询日志以及数十种单项分析报表，轻松发现、定位、处理问题。同时详尽记录用户上网行为和外发内容，并提供多种查询方式，满足企业内部治理和国家法规的要求。

运维安全审计

华为统一运维审计安全解决方案提供支撑系统维护的统一接入点，对维护操作进行集中管理，管理人员可以对支撑系统的用户和资源进行集中管理、集中授权、集中控制和集中审计；从技术上保证业务支撑系统安全策略的实施，保障业务支撑系统安全、高效的运行。

另外，华为统一运维审计安全解决方案支持字符终端、图形终端、数据库、应用终端、文件传输以及 KVM 运维方式，对运维操作全程跟踪和记录，提供事后快速故障定位和责任追踪，同时提供多种格式的审计报表和图表展示模板，最大程度满足数据中心运维管理需求。

方案涉及产品

维度	子方案	相关产品
安全准入	终端安全接入控制	TSM； 外部认证源（Windows AD、Novell ED、IBM Tivoli、Sun One、JIT Galaxy、标准 CSP 接口的 USBKEY）； USG2000/5000（SACG 设备）； 标准 802.1X 交换机（标准 802.1X）； 华为 NAC 交换机（扩展的 802.1X、Portal 认证）；
	上网行为管理	ASG（上网行为管理）；
远程安全接入	远程安全接入	USG2000/5000/9000（IPSec 网关）； SVN2000/5000（SSL VPN 网关）；
	移动终端安全接入	SVN2000/5000（移动办公接入网关）； 移动安全客户端（支持 IOS、Android、Windows mobile、Blackberry 操作系统）； MDM 管理平台； USG2000/5000/9000（边界安全网关）；
攻击防护	DDoS 攻击防御安全解决方案	Anti-DDoS1000/8000；
	实时入侵检测安全解决方案	NIP 2000/5000
	安全渗透测试服务	安捷信服务；
边界防护	边界访问控制安全解决方案	USG2000/5000/9000（边界安全网关）；
	网络防病毒安全解决方案	NAC(网络接入控制)； AVE（防病毒网关）；
安全管控，设备管理和安全审计	统一安全管控解决方案	iSOC；
	统一安全设备管理解决方案	VSM；
	安全审计方案	TSM（终端合规、资产审计）； ASG（上网行为审计）；

		UMA（堡垒主机，运维操作审计）；