企业安全进步从V 走向T PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/264/2021_2022__E4_BC_81_E4_B8_9A_E5_AE_89_E5_c67_264863.htm 企业对VPN都不会陌生，因为信息的共享有网络互联的需求，客观上需要将分布在异地的局域网络进行互联。 随着网络互联的进行，整个网络平台已经越来越成为企业以及政府单位运行的基础设施。这些基础设施，安全可信是最重要的。 可信平台建设包括了边界、内网、主机、接入等部分。目前来看，企业可以用各种技术来确保这四部分成为有机整体。而安达通在其中提供的就是可信专用网技术TPN.TPN与VPN的主要区别，就在于融合了可信任的内网技术，从而产生互联以后全网的可信任安全平台。 事实上，网络平台的演变，是从最简单的互联网开始的。此后，随着应用需求的发展，越来越多的企业要求将分流的网络进行互联，从而产生专网、专线。而VPN产生的动力，一方面是安全的需求，一方面是廉价的需求。所以，从专网发展成虚拟网络是一种需求，而安达通也认为，从虚拟专网发展到可信专网也会是一种趋势。 目前来看，一套完整的TPN模型需要实现所有传统安全设备所提供的安全功能：包括虚拟专网、防火墙、入侵检测、漏洞扫描、病毒防护、网络审计、身份认证、桌面安全等。而TPN应对的问题则包括了：远程接入用户带进木马和病毒、网络边界防护力度不够、分支机构的统一、垃圾邮件和病毒、越权访问/盗取机密、非法接入/非法外联、补丁和病毒库的统一升级、以及聊天、游戏、下载等网络滥用。 在边界防御上，TPN可以做到： 支持动态防火墙，实现基于“ 身份-角色-资源 ”的动态

访问控制，内置全状态检测防火墙和入侵检测微引擎；支持VPN；和主机威胁引擎联动，构成“主动防御体系”，阻断有安全隐患和未通过身份认证的内网主机访问互联网；可以对QQ、BT、MSN、Skype等各种P2P软件进行拦截，也可以按照管理员的定义；能够为不同角色的用户分配不同的带宽和上网优先级，确保关键业务的顺畅运行。 在内网防御上，TPN可以做到： 支持内网用户强制身份认证，基于角色对内网服务器进行严格的访问控制，防止越权访问；非法接入检测；IP和MAC绑定；问题主机自动隔离：对于有安全问题的主机，主机威胁引擎发现后会告警，并可主动断开问题PC的网络连接，防止威胁扩散，并实现内网病毒爆发点定位。 在主机防御上，TPN可以做到： 禁用/恶意/强制运行软件检测和基于“网关联动技术”的封堵；主机风险评估：对主机系统的安全状况进行检测和评估；强制软件/补丁分发；IP地址固定：防止主机IP被非法篡改；主机端口统一管理；主机反垃圾邮件：作为主机威胁引擎的一个组件，采用业界最先进的反垃圾邮件技术，进行垃圾邮件分析和堵截；主机外设控制。 在接入威胁防护上，TPN可以做到： VPN移动用户准入控制，禁止VPN移动用户的主机在没有达到安全级别时对内网的接入，确保外网的威胁不会通过内部用户传播进内网；远地VPN网络用户准入控制：禁止远地VPN网络内的用户主机在没有达到管理员规定的安全级别时，对TPN安全网关保护内网的接入。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com