心得体会:细数不同VPN产品的安全功能思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/629/2021_2022__E5_BF_83_E5_BE_97_E4_BD_93_E4_c101_629085.htm 短短两三年时间，vpn已从初出茅庐的业界新人迅速窜升为当红小生，除其自然状态下的茁壮成长外，市场的需求以及技术和产品的定向刺激，都使得如今的it市场上vpn产品真可谓各有来头、琳琅满目。 vpn实现的是一块更为广袤的“ 私密空间 ”和一条更为隐秘的“ 安全通道 ”。 随着网络应用的遍地开花，安全技术逐渐成为vpn产品的一个拳头支撑，基于ipsec和ssl协议的不同vpn产品也正表现着vpn的不同安全特色…… 在如今的网络时代，信息共享正在被赋予越来越丰富的外延，诸如本地信息的远程化、远程资源的本地化等，但凡能通过网络方式实现的，人们都乐此不疲地琢磨并尝试着。 vpn（虚拟专用网络）作为一种虚拟通道技术，其最初的设想只是为了满足远程访问的专用接入需求，并且能够避开ip地址资源有限的尴尬，而最终大量产品的市场需求以及后续vpn技术的不断延伸发展，也足以说明网络信息化对这一专用通道技术的强烈呼唤。 伴随着社会本身的进步以及信息化进程的大副进展，各种网络应用随即接踵而至，越来越多的安全需求成为vpn技术的关键。 总览vpn的安全实现 在原先维持网络更多虚拟空间的前提下，如何保证接入用户的合法性、保证网络访问的安全性以及系统本身的安全可靠性等等，都成为vpn需要面对的问题。 首先，vpn能保障哪些安全呢？很容易想象，vpn的实现技术和方式有很多，但是所有的vpn产品都应该保证通过公用网络平台传输数据的专用性和安全性。如在非面向连接的

公用ip网络上建立一个隧道，利用加密技术对经过隧道传输的数据进行加密，以保证数据的私有性和安全性。此外，还需要防止非法用户对网络资源或私有信息的访问。 其次，vpn还应当为不同网络的数据提供不同等级的服务质量保证（qos）。如对移动办公的用户，随意自主的连接性和信号的覆盖性就是vpn服务质量保证的一个主要因素；而当分支机构某用户通过vpn专有网对总部系统网络进行访问的话，整个总部系统的网络需要保持良好的稳定性。 此外，对于带宽和流量的控制，则是对网络优化的一个重要方面。充分有效地利用有限的广域网资源，保证重要数据的有效且可靠的带宽，将是关系网络整体稳定性的一个重要指标。通过流量预测与流量控制策略，可以按照优先级实现带宽资源的合理配置和管理，从而净化所处的网络。 ipsec vpn：端对端的安全 隧道技术是最典型、也是应用最为广泛的vpn技术，通过匹配四层网络模型中的不同层协议，可以生成不同的vpn技术及产品，如ipsec vpn就是第三层隧道协议匹配ip层（第三层）的ipsec协议生成的，而ssl vpn则是第四层隧道协议匹配应用层（第四层）的ssl协议生成的，这两种vpn也是当前业内最为流行的vpn技术及产品。 ipsec工作于网络层，是一个开放的结构，定义在ip数据包格式中，不同的加密算法都可以利用ipsec定义的体系结构在网络数据传输过程中实施。ipsec协议可以设置成在两种模式下运行：一种是隧道（tunnel）模式，一种是（transport）模式。隧道模式下，ipsec把ipv4数据包封装在安全的ip帧中。传输模式是为了保护端到端的安全性，即在这种模式下不会隐藏路由信息。ipsec几乎可以为所有的应用提供访问，包括客户端/服务器模式和某些传统的应用，但是由

于基于网络层，不能穿越通常的nat、防火墙。 ipsec为internet业务提供最强的安全功能，与其他隧道和安全技术相比，其优越性在于它的安全性和互操作性，但是管理相对复杂。ipsec得到各厂商广泛支持，非常适合于组建远程网络互联vpn。如果需要相对安全、保密的通道、网络流量有限、对业务实时性要求不高，应首选ipsec建立vpn。 ipsec vpn是基于ipsec协议的vpn产品，由ipsec协议提供隧道安全保障。ipsec是一种由ietf设计的端到端的确保基于ip通讯的数据安全性的机制。ipsec隧道模式具有以下特点：只能支持ip数据流；工作在ip栈的底层，因此，应用程序和高层协议可以继承ipsec的行为；由一个安全策略（一整套过滤机制）进行控制。安全策略按照优先级的先后顺序创建可供使用的加密和隧道机制以及验证方式。当需要建立通讯时，双方机器执行相互验证，然后协商使用何种加密方式。此后的所有数据流都将使用双方协商的加密机制进行加密，然后封装在隧道包头内。目前防火墙产品中集成的vpn使用较多的是ipsec 协议，在中国其发展处于蓬勃状态。 ssl vpn：web应用表现出众 第四层隧道协议最著名的是ssl，ssl（secure socket layer，安全套接字层）工作于会话/应用层，应用于web浏览程序和web服务程序，提供对等的身份认证和应用数据的加密，一般而言，典型的ssl vpn被认为最适合于普通远程员工访问基于web的应用。ssl是一个端到端的协议，因而是在处于通信线路端点的机器上实现，而不需要在通信通路的中间节点（如路由器或防火墙）上实现，并且由于不需要安装客户端软件，仅仅通过浏览器就可以实现vpn的连接，ssl vpn正在成为远程访问vpn的新宠。 除了具备与ipsec vpn相当的安全性外，还增加了访问控

制机制，客户端只需要拥有支持ssl的浏览器即可，可以说是零配置，非常适合远程用户访问企业内部网。因此ssl vpn相对成本比较低，而且不受网络环境的限制，不过这类产品对非web应用的支持不够理想，虽然理论上ssl可以用于保护tcp/ip通信，但事实上ssl的应用几乎只限于访问基于web服务器的应用。 不管怎样，ssl vpn是一种低成本、高安全性、简便易用的远程访问vpn解决方案，具备相当大的发展潜力。随着越来越多的公司将自己的应用转向web平台，ssl vpn将会得到更为广泛的应用。 mpls vpn：成就vpn大趋势 mpls vpn集隧道技术和路由技术于一身，吸取基于虚电路的vpn的qos保证的优点，并克服了它们未能解决的缺点。mpls组网具有极好的灵活性、扩展性，用户只需一条线路接入mpls网，便可以实现任何节点之间的直接通信，可实现用户节点之间的星型、全网状以及其他任何形式的逻辑拓扑。 mpls vpn非常适合对qos、cos（服务级别）、网络带宽、可靠性等要求高的vpn业务，适合于远程互联的大中型企业专用网络。mpls vpn不仅满足vpn用户对安全性的要求，还减少了网络运营商和用户方的工作量。mpls vpn便于实现三网合一，即在同一网络平台上实现基于ip的数据、语音和视频的远程通信。不过mpls vpn技术本身还有一个成熟的过程，但是它代表了vpn的发展方向。 产品选购尚存问题 无论是ipsec vpn还是ssl vpn，一个是国内常用的协议，一个是国外常用的协议，在产品选购中都同样面临用户认知和确保性能的问题： 首先，vpn在企业网络安全产品中的认知度尚低，其被优先选择的比例只占到9%。 从应用上来讲，目前我国的vpn产品应用主要集中在互联网/计算机行业、电信行业、金融机构等大型企业及

政府机构，从2004年开始中小企业和教育行业应用也逐渐受到青睐，应用比例有所提高。根据艾瑞2005年11－12月对500多家企业的调研发现，使用vpn产品企业中45.5%的属于互联网/计算机行业，10.4%企业属于电信通讯，政府机关和科研教育机构的占6.8%和4.3%。 不断拓展的市场需求将为vpn的应用提供了广阔的发展空间，无论从需求的范围还是传输的内容上来看，网络数据的传输需求越来越宽泛。目前很多企业，尤其是分支机构遍布各地的大型企业，协同管理和数据传输的需求也越来越大，使得vpn产品应用范围呈上升趋势。iresearch预计未来2年内，vpn产品将在企业内广泛应用，迅速向中小企业拓展，vpn产品成为各行业竞相采购的焦点。
其次，产品性能是企业选择vpn产品的第一因素。 从vpn产品的选购来看，由于很多vpn厂商的技术和解决方案良莠不齐，vpn的安全性、可靠性给人的印象并不深，也很难树立起高端产品的品牌形象。在技术同质化的鼓噪下，频频上演价格战，这样的市场环境非常不利于市场的培育和正常发展。iresearch调研数据显示，用户在选择网络安全产品时主要考虑的主要因素依次是产品的性能质量、品牌的可靠度、产品价格和厂商服务的能力，对于vpn产品而言“ 性能 ”的因素过半，所占比例达到60.3%，其次是品牌、价格和服务，所占比例分别为13.8%、12.7%和11.3%。 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