V 网络建设安全环节概要 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/252/2021_2022_V__E7_BD_91_E7_BB_9C_E5_BB_c101_252855.htm 识别和IPSec接入控制 设备验证采用了预共享密钥或数字证书，以提供设备身份，预共享密钥有三种：通配符、分组和独立。独立预共享密钥与某一IP地址有关，分组预共享密钥与一组名称有关，仅适用于当今的远程接入。通配符共享密钥不可应用于站点到站点设备验证。数字证书与独立预共享密钥相比，可更理想地扩展，因为它允许一台设备验证其他设备，但不具备通配符密钥的安全特性。数字证书与IP地址无关，而是与企业CA认证的设备上独特的标志信息有关。 IPSec IPSec提供了多种安全特性，对于管理员如何确定其工作方式提供了可配置选择：数据加密、设备验证，以及保密、数据完整性、地址隐藏和安全机构（SA） 密钥老化等功能。IPSec标准要求使用数据完整性或数据加密两种功能之一，具体使用哪个可任选。思科公司强烈建议加密和完整性二者都使用。而改变以上那些数值会提高安全水平，但与此同时， 也增加了处理器开支。 IP编址 正确的IP编址对于用作大型IP网络的VPN的成功有着重要意义。为保持可扩展性、性能和可管理性，强烈建议远程站点使用主网的子网，以便进行归纳。增加 ACL输入会降低性能，使故障查寻复杂化并影响可扩展性，适当的子网化还可支持简化的路由器头端配置，以实现分支到分支相互交流，要对所有设备的信息流进行归类，所需的隧道也较少。IP编址还可影响VPN的多个方面，包括重叠网络的远程管理连接。 多协议隧道 IPSec作为一种标准，只支持单点广播流量。

对于多协议或IP多点广播隧道，必须使用另一种隧道协议。网络地址转换 NAT可发生于IPSec之前或之后。了解NAT何时发生是十分重要的，因为在某些情况下，由于隧道构建受阻或信息流穿过隧道，NAT都可能对IPSec构成影响。除非提供接入是必须的，否则将NAT应用于VPN流量将不失为上策。单一目的和多目的设备 在网络设计过程中，您需要选择是在联网或安全设备中采用集成功能，还是采用VPN设备的特殊功能。集成功能通常是很吸引人的，因为您可以在现行设备上实施，且该设备经济有效，其特性可与其他设备互操作，从而提供功能更理想的解决方案。指定的VPN设备通常在对功能的要求很高或性能要求使用特殊硬件时，才会使用。当决定了采取何种选项，可根据设备的容量和功能对决策进行权衡，并与集成设备的功能优势相对照。在整个体系结构中，两类系统都有所使用。由于 IPSec是一种要求严格的功能，随着设计规模的提高，选择VPN设备取代集成型路由器或防火墙的可行性也日趋增大。注意，对VPN设备这一概念的了解不是件容易的事情。当今的许多VPN设备可提供理想的性能和VPN管理选项，与此同时，也提供有限的路由选择、防火墙或CoS功能，而它们可能与集成设备有关。如果所有这些高级功能都得以实现，从性能和部署选项的角度来看，这种设备也开始越来越像集成型设备。同样，除了路由选择和安全特性的全面实施以外，可支持全部VPN功能的VPN路由器，可在VPN单独环境中进行配置，其特征更象一种应用。