解析IPv6网络协议安全与安全机制思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_A7_A3_E6_9E_90IPv6_c101_644074.htm 与IPv4相比，IPV6具有许多优势。首先，IPV6解决了IP地址数量短缺的问题.其次，IPV6对IPv4协议中诸多不完善之处进行了较大的改进。其中最为显著的就是将IPSec集成到协议内部，从此IPSec将不再单独存在，而是作为IPV6协议固有的一部分贯穿于IPV6的各个领域。当然，IPSec的大规模使用将不可避免地对网络设备的转发性能产生影响，这就需要更高的硬件性能保障。本文主要介绍IPV6网络的安全性、安全机制。 1. 协议安全 在协议安全层面上，IPV6全面支持认证头(AH)认证和封装安全有效负荷(ESP)信息安全封装扩展头。AH认证支持hmac_md5_96、hmac_sha_1_96认证加密算法，ESP封装支持DES_CBC、3DES_CBC以及Null等三种算法。 2. 网络安全 (1) 端到端的安全保证。在两端主机上对报文进行IPSec封装，中间路由器实现对有IPSec扩展头的IPV6报文进行透传，从而实现端到端的安全。 (2) 对内部网络的保密。当内部主机与因特网上其他主机进行通信时，为了保证内部网络的安全，可以通过配置的IPSec网关实现。因为 IPSec作为IPV6的扩展报头不能被中间路由器而只能被目的节点解析处理，因此IPSec网关可以通过IPSec隧道的方式实现，也可以通过IPV6 扩展头中提供的路由头和逐跳选项头结合应用层网关技术来实现。后者的实现方式更加灵活，有利于提供完善的内部网络安全，但是比较复杂。 (3) 通过安全隧道构建安全的VPN。此处的VPN是通过IPV6的IPSec隧道实现的。在路由器之间建立IPSec的安全隧

道，构成安全的VPN是最常用的安全网络组建方式。IPSec网关的路由器实际上就是IPSec隧道的终点和起点，为了满足转发性能的要求，该路由器需要专用的加密板卡。 (4) 通过隧道嵌套实现网络安全。通过隧道嵌套的方式可以获得多重的安全保护。当配置了IPSec的主机通过安全隧道接入到配置了IPSee网关的路由器，并且该路由器作为外部隧道的终结点将外部隧道封装剥除时，嵌套的内部安全隧道就构成了对内部网络的安全隔离。 3. 其他安全保障 IPSec为网络数据和信息内容的有效性、一致性以及完整性提供了保证，但是数据网络的安全威胁是多层面的，它们分布在物理层、数据链路层、网络层、传输层和应用层等各个部分。 对于物理层的安全隐患，可以通过配置冗余设备、冗余线路、安全供电、保障电磁兼容环境以及加强安全管理来防护。对于物理层以上层面的安全隐患，可以采用以下防护手段：通过诸如AAA、TACACS、RADIUS等安全访问控制协议控制用户对网络的访问权限来防止针对应用层的攻击.通过MAC地址和IP地址绑定、限制每端口的MAC地址使用数量、设立每端口广播包流量门限、使用基于端口和VLAN的ACL、建立安全用户隧道等来防范针对二层网络的攻击.通过进行路由过滤、对路由信息的加密和认证、定向组播控制、提高路由收敛速度、减轻路由振荡的影响等措施来加强三层网络的安全性。路由器和交换机对IPSec的完善支持保证了网络数据和信息内容的有效性、一致性以及完整性，并且为网络安全提供了诸多解决办法。 