在Cisco的PIX上来实现VPN PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/245/2021_2022__E5_9C_A8Cisco_E7_9A_c101_245842.htm 在Cisco的PIX防火墙用共享密钥配置IPSec加密主要涉及到4个关键任务： 一、为IPSec做准备 为IPSec做准备涉及到确定详细的加密策略，包括确定我们要保护的主机和网络，选择一种认证方法，确定有关IPSec对等体的详细信息，确定我们所需的IPSec特性，并确认现有的访问控制列表允许IPSec数据流通过； 1：根据对等体的数量和位置在IPSec对等体间确定一个IKE（IKE阶段1，或者主模式）策略； 2：确定IPSec（IKE阶段2，或快捷模式）策略，包括IPSec对等体的细节信息，例如IP地址及IPSec变换集和模式； 3：用“ write terminal ”、“ show isakmp ”、“ show isakmp policy ”、“ show crypto map ”命令及其他“ show ”命令来检查当前的配置； 4：确认在没有使用加密前网络能够正常工作，用“ ping ”命令并在加密前运行测试数据流来排除基本的路由故障； 5：确认在边界路由器和PIX防火墙中已有的访问控制列表允许IPSec数据流通过，或者想要的数据流将可以被过滤出来。 二、配置IKE 配置IKE涉及到启用IKE（和isakmp是同义词），创建IKE策略，和验证我们的配置； 1：用“ isakmp enable ”命令来启用或关闭IKE； 2：用“ isakmp policy ”命令创建IKE策略； 3：用“ isakmp key ”命令和相关命令来配置预共享密钥； 4：用“ show isakmp [policy] ”命令来验证IKE的配置。 三、配置IPSec IPSec配置包括创建加密用访问控制列表，定义变换集，创建加密图条目，并将加密集应用到接口上去； 1：用access-list命令来配置加密用访问控制

列表；例如：access-list acl-name {permit|deny} protocol src_addr src_mask [operator port [port]] dest_addr dest_mask [operator prot [port]] 2：用crypto ipsec transform-set 命令配置变换集；例如：crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]] 3：（任选）用crypto ipsec security-association lifetime命令来配置全局性的IPSec 安全关联的生存期；4：用crypto map 命令来配置加密图；5：用interface 命令和crypto map map-name interface应用到接口上；6：用各种可用的show命令来验证IPSec的配置。