教你如何用多层次方法保VoIP安全 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/250/2021_2022__E6_95_99_E4_BD_A0_E5_A6_82_E4_c101_250963.htm 现在流行的IP网络模型将网络通信进程分成了不同层面这样让人更易于理解，部署和调试。不管是国际标准组织制定的7层模型，或是美国国防部开发的4层模型，都能让人更好地理解每一层面上运作的协议，对所有IP加密来说也都是必要的（包括VoIP）。 当然，在所有安全措施当中，多层次方法的效果最好。例如，你可能会为保护自己的家庭财产免遭盗贼毒手而实施一个多层次方法：在房子周围竖起篱笆，并锁上了篱笆的大门；在院子里养一条大狗；又在门上和窗户上安装防盗锁；然后又安装了一套防盗报警系统；最后还把家里值钱的东西放在一个很隐秘的地方，以防万一有人可以绕过你以上所有安全措施并偷走值钱东西。 同样，要保护你的VoIP网络，最好的方法也是采取一种多层次安全机制，在潜在入侵者的攻击路线上尽可能多地制造各种障碍。 分离语音和数据网络 要建立一个安全的VoIP网络，首要的步骤就是将其从你的数据网络中独立出来。 然将所有网络集成到一起，可能在管理的简易性及协同工作方面更加理想，但并不安全。最好的选择是使用VLAN交换机将数据网络和语音网络从逻辑上分离开来这意味着对数据网络进行的攻击将不会影响到你的VoIP系统。要将VoIP网络从数据网络中分离出来，首先要将分离VLAN上的VoIP话机设为非路由的地址；然后禁止连接互联网的电脑与VoIP之间有任何交流；接下来还要使用存取控制列表（Access control lists）来阻止VLAN之间的通讯。 配备VoIP专

用防火墙 对一个IP网络来说，边界保护通常意味着使用防火墙，但是一个老旧的防?星际遣皇屎oIP网络的。你需要一个特别设计的防火墙，它得能识别和分析VoIP协议，能对VoIP的数据包进行深度检查，并能分析VoIP的有效载荷以便发现任何与攻击有关的蛛丝马迹。 如果你的VoIP部署使用了SIP协议（Session Initiation Protocol），那么防火墙就应当能执行下述操作：监控进出的SIP信息，以便发现应用程序层次上的攻击；支持TLS（传输层安全）；执行基于SIP 的NAT以及介质端口管理；检测非正常的呼叫模式；记录SIP信息的详情，特别是未经授权的呼叫。 保护好VoIP网关 网关是数据进出VoIP网络的关键点，它会同时连接不同的网络，如IP网络和公共电话交换网（PSTN）。你应当在网关上使用授权机制以及存取控制，以便控制可通过VoIP系统拨打和接听电话，以及设定可以执行管理任务的不同人员权限等等。 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