思科认证辅导:十法打造安全VoIP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_ti2020/590/2021_2022__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_590385.htm 网络层加密 你可以使用IPSec加密来保护网络中的VoIP数据.如果攻击者穿越了你的物理层防护措施，并截获了VoIP数据包，他们也无法破译其中的内容。IPSec使用认证头以及压缩安全有效载荷来为IP传输提供认证性、完整性以及机密性。 VoIP上的IPSec使用隧道模式，对两头终端的身份进行保护。IPSec可以让VoIP通讯比使用传统的电话线更安全。 会话层锁定 你还可以使用TLS来保护VoIP会话，TLS使用的是数字签名和公共密钥加密，这意味着每一个端点都必须有一个可信任的、由权威CA认证的签名。或者你也可以通过一个内部CA(比如一台运行了认证服务的Windows服务器)来进行企业内部的通话，并经由一个公共CA来进行公司之外的通话。 保护应用层 你可以使用“ 安全RTP(SRTP) ”来对应用层的介质进行加密。RFC 3711定义了SRTP，让它可以提供信息认证、机密性、回放保护、阻止对RTP数据流的拒绝服务式攻击等安全机制。通过SRTP，你可以对无线网和有线网上的VoIP通讯进行有效的保护。 建立VoIP网络的冗余机制 要时刻准备着可能会遭到病毒、DoS攻击，它们可能会导致网络系统瘫痪。构建能够设置多层节点、网关、服务器、电源及呼叫路由器的网络系统，并与不只一个供应商互联。经常性的对各个网络系统进行考验，确保其工作良好，当主服务网络瘫痪时，备用设施可以迅速接管工作。 配备专用防火墙 对一个IP网络来说，边界保护通常意味着使用防火墙，不过一个老旧的防火墙是不适

合VoIP网络的。你需要一个特别设计的防火墙，他得能识别和分析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所有和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：监视进出的SIP信息，以便发现应用程式层次上的攻击.支持TLS(传输层安全).执行基于SIP 的NAT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。 内外网隔离 将电话管理系统与网络系统置于国际互联网络直接访问之外是一个不错的选择，将语音服务与其它服务器置于相分离的域中，并限制对其访问。 尽量减少软终端 VoIP软终端电话易于遭受电脑黑客攻击，即使它位于公司防火墙之后，因为这种东西是与普通的PC、VoIP软件及一对耳机一起使用的。而且，软终端电话并没有将语音和数据分开，因此，易于受到病毒和蠕虫的攻击。 限制所有的VoIP数据只能传输到一个VLAN上 Cisco建议对语音和数据分别划分VLAN，这样有助于按照优先次序来处理语音和数据。划分VLAN也有助于防御费用欺诈、DoS攻击、窃听、劫持通信等。VLAN 的划分使用户的计算机形成了一个有效的封闭的圈子，它不允许任何其它计算机访问其设备，从而也就避免了电脑的攻击，VoIP网络也就相当安全.即使受到攻击，也会将损失降到最低。 监控并跟踪网络的通信模式 监控工具和入侵探测系统能帮助用户识别那些侵入VoIP网络的企图。详细观察VoIP日志可以帮助发现一些不规则的东西，如莫名其妙的国际电话或是本公司或组织基本不联系的国际电话，多重登录试图破解密码，语音暴增等。 定期进行安全 要确信只有经过鉴别的设备和用户，才可

以访问那些经过限制的以太网端口。管理员常常被欺骗，接授那些没有经过允许的软终端电话的请求，因为黑客们能够通过插入RJ44端口轻易地模仿IP地址和MAC地址。 总结 基于IP网络及其协议的公共性质，使得VoIP天生就具备相对于传统电话网而言更易受到攻击的特质。不过，通过采取一个仔细规划的、多层次的VoIP网络防护措施，企业就可以让VoIP网络的安全程度赶上甚至是超过传统的电话系统。 