做好局域网安全保护从VoIP安全说起 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/461/2021_2022__E5_81_9A_E5_A5_BD_E5_B1_80_E5_c101_461756.htm 最近我听说了比较多的有关新型局域网攻击的消息，例如VoIP攻击，或者使用打印机作为攻击源的探测。那么局域网安全措施如何保护我们免受这些攻击困扰呢？ 这些攻击正在上升，这绝对是个事实。实际上，SANs研究机构最近将客户端攻击列为当今最为严重的弱点之一。然而如果我们中的任何人认为我们可以充分保护，免受此类攻击的话，那么就是有勇无谋的了，当有攻击威胁到你的企业的时候，你当然可以有一些强有力的措施来减轻威胁。 要采用的第一个步骤就是在你的局域网中实现一个认证的机制，这个局域网中包括了设备还有用户。如果你购买了一些类似802.1x的产品，它们并不充分，因为电话、打印机、体检设备，机器人，以及其他一些设备绝大部分都不支持802.1x的要求。 你需要一种方式去确保你知道每个插入网络的非用户设备，你也会知道它是什么样的设备。寻找一种认证方式，让你可以将你的某些特定的设备列入优良者名单，或者更好是，帮助你自动识别那些设备，通过使用反向DNS来讲设备名与设备类型联系起来。 接下来，你需要一种方式将这些非用户设备放入一个角色，并给这个角色分配访问权限。例如，你可以订一个打印机角色，可以应用给你的环境中的所有的打印机和打印机服务器。至于访问权限，你可以指定打印机只能与打印机服务器通讯，所有的用户设备都只能够与打印机服务器进行通讯。通过这种类型的策略，你可以访问用户设备和打印机之间的直接通讯。 在VoIP

方面也类似，你可以指定VoIP电话给VoIP角色，然后定义这些VoIP电话只可以与呼叫管理器通讯。你甚至可以使用基于应用的策略来超越这种基于地域的保护。例如，你可以说，具有VoIP角色的设备应该只使用SIP，H.323，或者SKINNY来进行通信，例如，更进一步地保护免受基于数据的攻击。 这种类型的领域划分在保护电话、打印机或者其他可能作为攻击发起点的设备方面非常有帮助。例如，被约束的打印机，并且有漏洞扫描软件安装在上面的话，它是不会被寻找开放端口的所有网络设备触及的。还有VoIP电话不能用于发起一个针对其他服务器或者终端用户机器的攻击；通过应用保护，它甚至不能使用数据协议攻击呼叫管理器。 那么你用何种方式能够获得这样的局域网安全保护呢？你有很多选择。下一代局域网交换机，带有802.1x之外的认证，可以对用户和设备应用基于策略的访问控制，这是将这种能力直接引入你的局域网的非常不错的方式。如果你还不想升级交换机，那么考虑一下具有认证用户和设备能力，能够给设备自动分配角色，并且可以根据领域和应用采用基于策略的控制的安全设备。 无论是选择了访问交换或者设备，关键是要把保护正确应用到局域网的用户边缘上。这个地点对于减少这些基于客户的攻击是至关重要的。否则，你就没有工具在他们开始的地方去阻断运输流量。 