网络访问控制来强化 LV 网络安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E7_BD_91_E7_BB_9C_E8_AE_BF_E9_c101_461755.htm 很多公司已经改进了其IPsec VPN，有的甚至用基于SSL的远程访问解决方案替换掉了IPsec VPN.SSL VPN能够在任何未经管理的家用或公用电脑上使用，当要决定是否允许访问公司网络资源时，评价远程端点的安全性是至关重要的。 本文将探讨用网络访问控制（NAC）功能来加强SSL VPN网络的安全性的原因和措施，并讨论其与NAC 优先权的关系。 机会与风险 将浏览器用作客户端平台，SSL VPN使用户远程访问IT难以控制的设备成为可能，无论从家用PC还是商业伙伴的便携式电脑或者PDA设备都是如此。这种“ 任何时间、任何地方 ”的方法可以将访问扩展到更多的工作人员而其成本却会大大减少。据Gartner估计，到2008年，SSL VPN对三分之二的远程工作人员来说将会成为主要的远程访问方法，而且约有90%的雇员需要使用临时性的远程访问。 然而，将未被管理的端点设备连接到公司网络会增加风险。如果一个远程工作人员的家用PC感染了蠕虫或木马，其VPN通道可将这些威胁转播到公司网络资源。如果Internet信息站点有一个键盘记录器，那么用户的全部的VPN会话，包括登录名和口令都将被窃取。在这两种情况下，用户趋向于将敏感数据—无论是缓存中的口令还是临时文件，置于其他人可发现的地方。很明显，要确保安全地访问未被管理的端点就需要减轻这些风险。 过滤空白点 可喜的是，SSL VPN厂商一直努力着手解决这些问题。当今的SSL VPN设备提供了一套相当成熟的NAC（网络访问

控制）功能来抗击这些威胁。 身份识别：SSL VPN支持用户身份验证和目录，创建一个基于用户标识的访问控制基础。但是一个特定的用户可能会从任何未经管理的和被管理的端点设备来进行连接。因为，既要根据用户的身份标识来判断，又要根据设备的标识和类型来决定。以产品为基础，SSL VPN可以使用HostID（主机ID）识别被信任的端点、计算机/域名、设备证书、驻留文件、注册表项或硬件标识。SSL VPN还可以识别端点的操作系统和浏览器，并相应地做出响应。 端点完整性：多年来，VPN仅仅假定被管理的设备是可信赖的。未被管理的设备有极大的风险，但是假定端点将会免于受恶意软件的侵害却并非真正安全。如今，大多数VPN产品都检查端点的完整性，并且使用管理员定义的配置文件来检测遗漏的补丁、老病毒特征、非活动的或被破坏的反病毒程序、反间谍软件和防火墙程序、不正常的进程或监听端口以及恶意软件的迹象等。 为了简化配置，许多产品提供可供选择的模板、检查列表或者图形化的规则生成器。有一些甚至可以与被管理端点的端点安全程序进行交互。而且，大多数SSL VPN产品还可以执行进入前检查，有一些产品还支持后进入完整性审计，确保端点保持清洁。 授权认可：通过操作在一个更高的层次上，SSL VPN提供比IPsec更加精细的授权策略。与对整个子网授权相反，许多SSL VPN将访问缩小到单个服务器、应用程序、命令、URL、文件夹和其它数据对象。将这些精细过滤器与用户身份验证、设备标识相结合，端点安全检查就会有更大的威力。例如，使用公司桌面PC的工作人员可以被授权使用宽带应用访问，而对于从公用PC访问公司资源则被限制为只能使用远程终端会话。如果

端点的完整性检查失败，工作人员就会转到一个自助页面来寻求补救。一些SSL VPN产品将用户和设备与小组结合起来，简化了管理并可促进连续性。。 增强： SSL VPN通道的建立并不意味着安全的终止。VPN必须实施过滤器来决定用户可以发送的应用程序消息，发往何处，在传输中如何进行保护。大多数SSL VPN产品都得到了强化，以减轻那些未被管理的端点的风险。在会话期间，用户可以在一个安全工作区中（一个将活动和数据与其它端点过程隔离开的虚拟化的环境）操作。 会话结束后（由于显式退出或非活动超时），SSL VPN可以删除所有的会话数据，包括Web的cache（高速缓存）、历史数据、cookies、表单记录及口令等。在这里，措施是基于策略的。例如，在允许文件被存到一个策略一致的公司膝上型电脑上时，在一个高风险的平台上要求安全的工作空间。 这些网络访问控制功能也有可能没有存在于你喜欢的SSL VPN产品中。特定端点的限制也可以执行安全检查，这些检查并不能通过管理员权限来执行，也不能通过只能建立在Win32 PC上的虚拟环境来执行。SSL VPN特性在过去的几年里已经有了极大的扩充，这都反映了这个领域经验和技术的成熟。好好看一下你可以使用的NAC功能吧，你也许会大吃一惊的。 与NAC的关系 熟悉思科 Network Admission Control（NAC），微软Network Access Protection或者TCG的Trusted Network Connect的读者可能会想“ 等一下，这些功能怎么这么像NAC、NAP、TNC？ ”事实上，许多概念和技术都是起源于SSL VPN市场，从端点的安全检查到基于浏览器的客户端软件。 SSL VPN有望在NAC的使用中大展风采。Infonetics 预计到2008年超过2/3的SSL VPN网关可以用作一

个NAC部署的部分。在有些情况下，这些SSP VPN 会成为一个更宽泛的NAC策略的一部分。许多SSL VPN供应商已经宣布NAC体系结构或参与到一个或多个NAC项目中。例如，Cicso，Microsoft，Juniper都销售分别适合NAC、NAP和TNC的设备。Caymas Systems甚至还有一种产品既支持NAC又支持NAP. 在部署为一个更宽泛的NAC策略的局部时，一个明显的方法就是使SSL VPN设备集中于控制离站的远程用户的网络访问，远程用户包括：旅途中的工作人员，远程工作人员等等。然而，一些分析人士相信，SSL VPN可以在NAC中扮演明星的角色。特别是，随着网络外围的消失，越来越多的设备可被认为是“ 远程的 ”（外部的）。一些企业可能会选择运行所有的网络访问，无论是在站的还是离站的，这些访问都通过一个SSL VPN设备实施，这样就能提供更安全的访问控制。 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