降低基本 SAN 易损性

有效的 SAN 安全计划不但要能保护用户、客户机、应用、数据、数据存储设备、服务器和网络，还必须保证这些元素中没有任何漏洞。由于 SAN 中包含了多种多样的元素，因此，本文将从功能角度讨论 SAN 的安全性，即先讨论需要实现的安全功能，然后将这些功能应用到所有元素中，而不是独立保护每种元素。

功能 1—身份验证

验证的目的是保证只让授权用户访问 SAN，该功能通常通过问题响应协议实现，最常用的是用户 ID 和密码。验证会引发许多问题，例如，如果使用了用户 ID 和密码，则应该使用基本的密码控制最佳实践，包括使用不易猜测的密码，经常修改密码等。除了“社会工程”即让用户履行适当的密码程序之外，还必须解决很多技术问题，例如不通过网络传输未加密的密码，尤其是带外通道。尽管如此，个人验证问题可能是各种 SAN 安全问题中人们理解最透彻的问题，因为它是最常见的计算机安全问题。

思科系统公司提倡将 CHAP 验证作为从 IPSec VPN 到 iSCSI 主机验证的各种用途的标准 AAA，整个 CMDS 9000 多层交换机系列都支持 CHAP。CHAP 即将被 ANSI T-11 委员会推选为最佳验证方法。目前该委员会已经将 CHAP 作为 SAN 必须使用的第一个验证方法。（参见白皮书“思科 MDS 系列多协议服务模块”）

功能 2—访问

只允许相关人员接入 SAN 并根据相应等级访问信息的概念相对容易理解。虽然存储管理员的控制力正在不断加强，但与验证相比，提供访问功能遇到的技术问题更难解决。最基本的访问概念是确定和控制谁拥有对数据和 SAN 本身的哪种权限才能访问哪些信息。由于不同 SAN 的访问控制功能和实施方式各不相同，因此，第一步是确定管理员可以使用哪些工具和设备管理访问，一般包括设置数据的读/写/删除权限，限制谁可以访问配置等 SAN 管理功能，以及分区和 LUN 掩膜等特性。

分区 – 这个功能能够超越不同设备使用不同操作的障碍。由于它允许为某个用户组设置访问权限，将该组的设备与网络中的其它设备隔离开，因而能有效保护机密数据。利用这种方法，存储管理员可以在不影响其它分区的情况下安装、测试和升级某些设备。

思科矩阵交换机同时提供基于硬件和软件的分区，并能够按照地址、物理端口或名称等不同条件划分节点。这样既能为分区成员提供任意点之间的连接，又能有效隔离非该分区的成员。基于硬件的分区包括端口类型控制和软分区。在基于硬件的分区中，当接收到启用命令时，端口类型控制能够保证交换机将自动感应连接类型。这个步骤能够区分通用交换机端口（G 端口）、矩阵端口（F 端口）或者同时与两台交换机相连的 E 端口。利用端口类型配置，存储管理员可以限制某交换机只能使用某类端口，从而防止存储端口受到攻击或者被误用。当光纤通道设备在不同端口之间移动时，软分区可以跟踪该设备。基于软件的分区可以使用基于交换机的简单名称服务器（SNS），即利用全球节点名称和全球端口名称确定分区成员。在这种情况下，当主机访问 SAN，并请求可用的存储设备时，SNS 将只返回分区表中允许的设备。

另外，分区还能防止存储网络在新设备部署和测试过程中出现故障。管理员可以利用交换机将其分成多个区域，例如管理流量或测试网段，以便保护网络。这个功能对系统集成商尤其有用，因为在安装新网络组件时，他们可以锁定客户的网络，以防出现意外更改。利用这种方法，可以更简单、更安全地支持集成商在工作 SAN 上安装和测试新设备。但是，分区并非没有限制。思科建议，矩阵分区应该与 VSAN 配合使用（参见“利用 VSAN 增强分区”）。

降低基本 SAN 易损性

LUN 掩膜 - LUN（逻辑单元号）掩膜能够进一步遏制非法主机绕过 SNS 的企图。LUN 掩膜能够在组件水平上控制对 SAN 上每台存储设备的访问。LUN 掩膜可以让主机无法看到阵列上的某组磁盘或磁带库中的某个磁盘驱动器。与分区相似，LUN 掩膜也可以同时使用硬件和软件方法，即通过路由器和控制器等硬件设备实现，或者通过主机上的程序实现。由于 LUN 掩膜需要耗费大量人力，因而最适合小型 SAN。

组合使用分区和 LUN 掩膜时，一般需要花费很多时间和人力进行设置和维护，因为其中包含很多变量，必须细致、认真地设置。事实上，为每个用户独立设置将需要耗费大量的时间。另外，还必须定期检查访问权限，并根据职责的变化不断修改。

功能 3—审查和监控

审查访问、配置变更和用户行为不但对安全至关重要，还直接影响到能否持续跟踪网络变化并可能会影响网络性能的各种趋势。有效的审查计划应该包括 SAN 访问、配置修改和用户行为的连续记录。目前，这些记录都可以由 Cisco MDS 9000 多层交换机系列提供。根据这些信息，审查系统应该能够同时识别正常和异常行为，并制订各种响应措施。与访问控制相似，审查也需要编制可用工具目录，并有效利用这些工具。但是，如果希望制订出有效的 SAN 审查计划，需要经过一定的思考和研究。

确定基线后，应严格执行监控，这样才能及时发现偏差并予以更正。为了将不太严重的小事故与严重威胁区分开，存储管理员应该注重计划和研究。制订有效的监控战略时，第一步是确定 SAN 上的“正常”行为模式。除流量数据外，还包括管理工具的使用情况以及对 SAN 作的各种修改。确定基线之后，下一步是确定在 SAN 行为偏离正常值多大比例之后触发警报。除明确分析 SAN 行为参数变化外，还应包括商业行为模式和可能出现的外部事件。

利用 VSAN 增强安全性

为增强网络的可扩展性和可用性，并进一步增加矩阵分区提供的安全服务，思科系统公司在其 MDS 9000 系列多层导向器和矩阵交换机内提供了一种称为虚拟 SAN（VSAN）的新技术。最近，VSAN 已经被 ANSI T-11 委员会定为标准，如果与硬件分区配合使用，将能够为 SAN 设计者提供更加先进的工具，同时在可扩展性、安全和管理方面大大优化 SAN 部署。

如果想了解怎样利用分区和 VSAN 实现更加全面的 SAN 安全性，请点击这里。

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街 1 号东方广场东方经贸城东一办公楼 19-21 层
邮政编码：100738
电话：(8610) 85155000
传真：(8610) 85181881

上海
上海市淮海中路 222 号力宝广场 32-33 层
邮政编码：200021
电话：(8621) 33104777
传真：(8621) 53966750

广州
广州市天河北路 233 号中信广场 43 楼
邮政编码：510620
电话：(8620) 85193000
传真：(8620) 38770077

成都
成都市顺城大街 308 号冠城广场 23 层
邮政编码：610017
电话：(8628) 86961000
传真：(8628) 86528999

如需了解思科公司的更多信息，请浏览 http://www.cisco.com /cn

2005 年 4 月翻译