

IP SAN 抗攻击部署模型研究

杨林 霍跃华

(中国矿业大学 北京 100083)

摘要 随着 SAN 的发展和 IP 网络的普及, IP SAN 逐渐成为存储构架的首选。分析了 IP SAN 实际部署模型中存在的抗攻击能力差的问题。针对这个问题,提出了 IP SAN 抗攻击部署模型。IP SAN 抗攻击部署模型的设计思想是采用路由技术将应用服务器的广播域进行隔离,以减小其影响范围;在与应用服务器相连的三层交换机上配置安全策略来提高交换机抗攻击能力,从而在整体上提高 IP SAN 的抗攻击能力。最后通过测试证明了 IP SAN 抗攻击部署模型的性能,指出这种方案在实际应用中的可行性。

关键词 IP SAN 部署, 抗攻击模型, 安全策略

中图分类号 TP30

文献标识码 A

Research on IP SAN Deployment of Anti-attack Model

YANG Lin HUO Yue-hua

(China University of Mining & Technology, Beijing 100083, China)

Abstract IP SAN has gradually become the first choice of storage architecture as the development of the SAN and popularization of the IP network. This paper analysed the problem of anti-attack capability in the IP SAN actual deployment model, and IP SAN deployment of anti-attack model was given. The points to raise the IP SAN anti-attack capability were taking routing technology to isolated application server broadcasting domain to reduce the scope of its influence and targeting security strategy for the Layer 3 Switch which linked with Application Server. Finally, the performance of the IP SAN deployment of anti-attack model was proved by the experiment.

Keywords IP SAN deployment, Anti-attack model, Security strategy

由于 IP SAN 相比于传统的 FC SAN 具有性价比高;配置、管理、维护的复杂度低;设备互操作性强等特点,正在被越来越广泛地应用于存储的领域^[1,2]。IP SAN 在服务器和 IP SAN 存储设备之间的采用 TCP/IP 协议进行数据的传输。IP SAN 实际部署中,应用服务器和 IP SAN 存储设备之间通过二层交换技术传递数据,应用服务器和 IP SAN 设备处于同一个广播域之中,如果 IP SAN 中应用服务器中病毒或者产生针对二层的攻击,会对二层交换机的性能造成影响,从而影响整个 IP SAN 的性能。文中对 IP SAN 的实际部署模型进行分析,指出其存在的安全隐患,进而提出 IP SAN 抗攻击部署模型。

1 IP SAN 实际部署模型

1.1 IP SAN 实际部署结构

IP SAN 的实际部署结构如图 1 所示,整个结构分为两个部分,第一部分是从客户端到服务器之间的网络,这是面向应用的网络,被定义为主网络;第二部分是从服务器到存储设备之间的网络,这是面对存储的网络,被定义为辅助网络。IP SAN 实际就是指从服务器到存储设备之间的辅助网络,而这个网络是通过 IP 网来实现的。

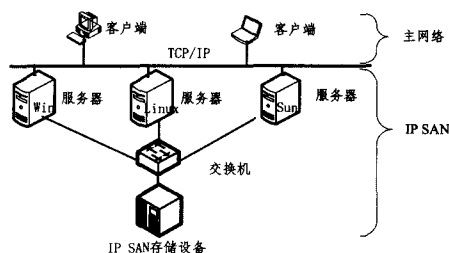


图 1 IP SAN 实际部署结构

1.2 IP SAN 实际部署结构模型问题分析

IP SAN 和 FC SAN 的体系结构相同。IP SAN 和 FC SAN 采用了不同协议进行数据传输,因此必然有各自的特点。对于 FC SAN,由于其采用了 FC 协议,这与主网络采用的是不同的协议。针对这个协议的攻击和病毒非常少。因此,即便服务器通过主网络中了病毒,并不会对 FC SAN 造成影响。IP SAN 采用了 iSCSI 协议,而 iSCSI 协议是利用 TCP/IP 协议来实现的^[3]。针对于 TCP/IP 协议的各种攻击和病毒要远远比针对 FC 协议的攻击和病毒多。尽管在逻辑上 IP SAN 和主网络是两个不同的网络,但是在物理上,却是相同的网络^[4]。因此,一旦服务器通过主网络中了病毒,很有

到稿日期:2008-06-12

杨林(1958—),男,工学硕士,副教授,主要研究方向为通信与信息系统、计算机网络等,E-mail: yanglin@cumt.edu.cn;霍跃华(1981—),男,工学硕士,助理工程师,主要研究方向为通信与信息技术、网络安全控制等。

可能对 IP SAN 中的二层交换机进行攻击,从而影响 IP SAN 的性能。由此可以看出,IP SAN 实际部署模型中存在以下的安全问题:

1)二层交换机容易受到 MAC 泛洪的攻击。由于二层交换机是根据 MAC 地址去转发数据帧的,其在转发过程中依靠对内容可寻址存储器(CAM)表的查询来确定正确的转发接口。而交换机的 CAM 容量有限,并且要定期刷新。入侵者可以在交换机的 CAM 刷新时间内,发送大量的假冒源 MAC 地址和目的 MAC 地址的数据帧将交换机的 CAM 填满,使交换机失去转发功能。实际的 IP SAN 部署结构之中,如果 IP SAN 中的应用服务器被黑客攻破,通过这种方式对交换机进行攻击,那么将会使交换机出现故障,而交换机是 IP SAN 进行数据传输的枢纽,如果交换机出现故障,整个 IP SAN 就无法正常工作。

2)二层交换机容易受到 ARP 病毒的攻击。ARP 病毒是利用 TCP/IP 协议的漏洞而发作的病毒。应用服务器一旦中了这种病毒,通常表现为一个 MAC 地址对应多个 IP 地址,这时中毒的服务器就会向整个广播域发送大量的广播包,如果广播包的数量大大超过交换机的处理能力,交换机将不能正常工作,这时就会影响这个 IP SAN 网络正常工作^[5]。但是这个问题通过二层交换机是没有办法解决的,这将会对 IP SAN 的性能造成严重的影响。

综上所述,在 IP SAN 实际部署模型中,由于采用了二层交换机对数据进行转发,致使应用服务器和 IP SAN 存储设备在同一个广播域中。如果应用服务器一旦有了针对二层进行攻击的病毒,就会对应用服务器所在的广播域内的所有设备进行攻击,而二层交换机对于这种攻击的抵抗能力比较弱,一旦攻击的强度超过了二层交换机性能参数(CPU 占用率、CAM 容量)的承受范围,将导致二层交换机无法工作,从而致使 IP SAN 无法正常工作。可见,IP SAN 实际部署模型中采用二层交换机作为数据转发的桥梁,由于二层交换机的抗攻击能力弱,导致 IP SAN 的实际部署模型的抗攻击能力必然比较弱。

2 IP SAN 抗攻击部署模型

针对 IP SAN 实际部署模型中存在的问题,本文提出了 IP SAN 抗攻击部署模型。

2.1 设计思想

IP SAN 抗攻击部署模型的设计思想是针对 IP SAN 实际部署模型中,二层交换机抗攻击能力差的缺点,通过提高交换机的抗攻击能力,来提升 IP SAN 的抗攻击能力。在设计中,利用路由技术对 IP SAN 中的应用服务器的广播域和 IP SAN 存储设备的广播域进行隔离,从而减小了应用服务器广播域范围,这样即便是应用服务器产生了针对二层协议进行的攻击,其影响范围也将大大缩小。在此基础上,对三层交换机所在的可能产生安全隐患的广播域进行安全策略的配置,以提高交换机的抗攻击能力,从而达到提高 IP SAN 抗攻击能力的目的。

2.2 IP SAN 抗攻击部署模型广播域隔离分析

IP SAN 抗攻击部署模型如图 2 所示,这个模型并不改变 IP SAN 实际部署的物理拓扑结构,但是在逻辑上利用路由技术来对应用服务器和 IP SAN 存储设备之间的数据进行转

发,从而达到将应用服务器的和 IP SAN 存储设备的广播域进行隔离。

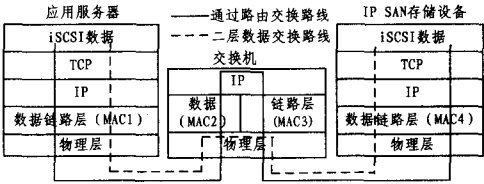


图 2 IP SAN 抗攻击部署模型

如图 2 所示,应用服务器(物理地址为:MAC1)向 IP SAN 存储设备(物理地址为:MAC4)进行数据传递时,当分别采用二层交换技术和路由技术对数据分组进行转发时,分组帧结构中的物理地址如表 1 所示。

表 1 分组物理地址

	应用服务器端分组帧		IP SAN 存储设备端分组帧	
	源地址	目的地址	源地址	目的地址
二层转发技术	MAC1	MAC4	MAC1	MAC4
路由技术	MAC1	MAC2	MAC3	MAC4

可见,如果应用服务器通过二层交换技术向 IP SAN 存储设备进行数据转发的时候,分组在二层交换机处并不改变源物理地址和目的物理地址,这说明应用服务器和 IP SAN 存储设备在同一个广播域中,一旦发生针对二层的攻击,势必会影响整个广播域的设备。

如果应用服务器和 IP SAN 存储设备之间利用路由技术转发数据分组时,数据分组通过三层交换机(或者路由器)将会改变数据分组的源物理地址和目的物理地址,从而将应用服务器所在的广播域和 IP SAN 存储设备所在的广播域进行了隔离^[6]。

通过这种模型的建立,就可以将应用服务器所在的广播域范围缩小,从而减小了其针对二层协议攻击的影响范围,这样从一定程度上就提高了 IP SAN 的抗攻击能力。

2.3 IP SAN 抗攻击部署模型的安全策略

尽管采用路由技术可以减小应用服务器所在的广播域的范围,将有问题的服务器隔离在一个较小的范围之内,从而减少其影响范围,但是仍然没有办法完全解决应用服务器和三层交换机之间在同一个广播域而带来的安全问题。下面讨论在交换机上采取一些必要的安全策略来提高三层交换机本身的抗攻击能力。

1)端口 MAC 地址绑定和减少 MAC 地址学习数相结合;在三层交换机的端口处配置 MAC 绑定,并且减少交换机的 MAC 地址学习数。这样就可以基本解决 MAC 泛洪攻击对交换机造成的影响。

2)IP-MAC 地址绑定;在交换机端口开启 IP-MAC 地址绑定功能,这样就可以将接入交换机端口的服务器的 IP 地址和对应的 MAC 地址进行限定,从而在一定程度上避免 ARP 攻击和非授权用户接入网络。

3)开启广播风暴抑制功能;可以有效降低广播包的数量,这样对类似 ARP 病毒的发作和 MAC 泛洪式攻击都可以起到一个很好的抑制作用,有效降低由于在广播域中大量广播包而对交换机造成危害的可能性。

综上所述,IP SAN 抗攻击部署模型包含两个部分,一部分是利用路由技术对数据进行转发,这样可以缩小应用服

器的广播域范围;另一部分就是在三层交换机上进行安全策略的配置,这样可以大大提升交换机的抗攻击能力,从而提高 IP SAN 整体的抗攻击能力。

3 性能测试和分析

三层交换机都可以很好地支持 IP SAN 抗攻击部署模型采用的安全策略,在实际的使用环境中,可以证明那些安全策略对于提高交换机的抗攻击能力是很有效的。下面的测试,主要是验证采用路由技术进行数据转发的性能,从而验证这种模型的在实际应用中的可行性。

测试主要对带宽进行分析。带宽主要是反映存储系统的最大传输率,这是这次测试的重点。实验中通过对两种模型的带宽进行测试,考察 IP SAN 抗攻击模型的数据转发性能。

3.1 实验环境

实验拓扑结构如图 3 所示。若对 IP SAN 实际部署模型的数据转发性能进行测试,则直接用交换机将 IP SAN 储存设备和应用服务器相连,直接用二层交换技术对数据进行转发。若对 IP SAN 抗攻击模型的数据转发性能进行测试,则实验中将 IP SAN 存储器划分至 Vlan2,分别将服务器划分至 Vlan3,Vlan4,Vlan5 中。这样将各个应用服务器和 IP SAN 存储器划分在不同的 Vlan 之中,在三层交换机上通过路由协议对数据进行转发。

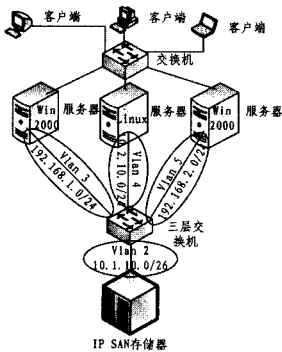


图 3 实验拓扑结构图

在实验中用到 3 台服务器,要求配置千兆网卡;锐捷 5750 以太网交换机 1 台;6 类网线 4 根;锐捷 RG-iS2000 存储 1 台。3 台服务器、锐捷 RG-iS2000 和锐捷 5750 以太网交换机都是以千兆链路相连。在 2 台服务器上运行 windows server2003 操作系统,并在服务器上安装 iSCSI 协议软件。在服务器上用 IOMeter2003 软件对存储空间进行连续读写,连续测试 1 小时以上。

3.2 实验结论和分析

图 4 是两种模型中数据块大小与带宽的关系曲线图。在数据块小的时候,IP SAN 抗攻击部署模型的数据转发能力比 IP SAN 实际部署模型的数据转发能力要弱,但是随着数据块的增大,这两种模型的数据转发能力逐渐接近。在实验中,选择具有良好转发性能的交换机将在很大程度上提高 IP SAN 抗攻击部署模型的数据转发性能。

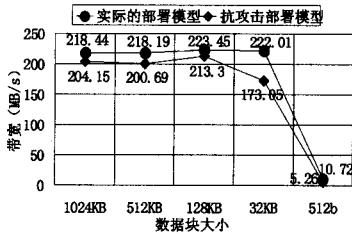


图 4 两种模型带宽比较

通过这个实验可以证明,IP SAN 抗攻击部署模型的最大带宽和 IP SAN 实际部署模型的最大带宽相差不大,IP SAN 抗攻击模型在实际部署中是具有可行性的。

结束语 综上所述,本文针对目前 IP SAN 实际部署中二层交换机抗攻击能力差的缺点,提出了 IP SAN 抗攻击部署模型。IP SAN 抗攻击部署模型的设计思想是采用路由技术将应用服务器所在的广播域隔离,缩小其广播域的范围,之后通过配置相应的安全策略,提高交换机的抗攻击能力,从而提高 IP SAN 整体的抗攻击能力。最后经过实际测试,证明了 IP SAN 抗攻击部署模型的性能,指出可以将这种模型应用于实际的 IP SAN 构架之中。

参考文献

[1] 白广思. FC SAN 和 IP SAN 构架比较新论. 情报科学, 2007, 25 (9): 1369-1372, 1377

[2] 叶宾, 须文波. IP2SAN 环境下 RA ID 远程管理系统设计与实现. 微型计算机应用, 2007, 28(7): 747-750

[3] 高增荣. 存储区域网络 IP SAN 与 FC SAN 技术. 甘肃科技纵横, 2007, 35(6): 16, 145

[4] 谢长生, 罗益辉. IP-SAN 的研究与设计. 小型微型计算机系统, 2005(06): 912-915

[5] 王佳, 李志蜀. 基于 ARP 协议的攻击原理分析. 微电子学与计算机, 2004, 21(4): 10-12

[6] Forouzan, Behrouz A. TCP / IP Protocol Suite. 2nd. United States; McGraw-Hill, 2003

(上接第 108 页)

[2] 赵耿, 方锦清. 现代信息安全与混沌保密通信应用研究的进展[J]. 物理学进展, 2003, 23(2): 212-230

[3] 杜月林, 陆婷. 混沌扩频序列在 CDMA 通信系统中的应用[J]. 国外电子测量技术, 2006, 25(7): 69-72

[4] 易雄书, 崔华, 余少波, 等. 扩频通信系统中基本扩频序列性能分析与设计[J]. 计算机仿真, 2008, 25(6): 134-137

[5] 戴志诚, 汪秉文. 基于混沌同步的保密通信[J]. 系统工程与电子技术, 2007, 29(5): 699-702

[6] Fang Jin-qing, Ali M K. Control and Synchronization of Spatio-temporal chaos//Chen G R. Controlling chaos and bifurcation in engineering system. USA; CRC Press, 1999: 104-127

[7] 刘嘉辉, 颜景斌, 宋大华. 基于混沌的网络通信数据加密方法[J]. 哈尔滨理工大学学报, 2007, 12(1): 32-35