广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):360~361
Vol. 23,No. 4 November 2007

一种基于NAS的安全镜像解决方案
A Solution of Security Image Based on NAS Units

唐忠平,王 宾
TANG Zhong-ping,WANG Bin

(广州军区综合训练基地,广西桂林 541002)
(Comprehensive Training Base of Guangzhou Theater,Guilin,Guangxi 541002,China)

摘要:以Storway NAS为硬件平台,利用NAS数据镜像功能,提出一种安全镜像解决方案,并分析其安全性和实用性。该方案能够实现数据的存储、备份及同步更新,能够保证数据复制的单向性、合法性,内部数据的及时更新,镜像操作在较短的时间内完成。实践证明该方案安全性高,实用性好。

关键词:安全镜像 NAS 数据一致性
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2007)04-0360-02

Abstract:Based on the image function of the Storyway NAS, this paper gives a solution to the security image between the Internet and Intranet WEB data, then analyses its security and usability. The design can store, backup and synchronously renew the data, ensure that the data is one-way and legal when being copied. The intranet data can be renewed on time and quickly. The practice shows that the solution is characterized by its security and great practicability.
Key words:security image,NAS,data integrity

基于信息安全方面的考虑,某些公司、军事单位及政府部门往往将自己的网络划分为两个部分:内网和外网。内网为内部人员提供服务,外网为Internet用户提供服务,两部分往往是物理隔绝的。这样的拓扑结构虽然满足了信息安全要求,但是给内外网的数据交换带来不便。一个典型的案例:内外网分别基于不同的目的部署了WEB服务器,为各自的用户提供服务,但内网中的某些用户也想准实时(在此将用户对信息实时性要求不高,比如可以接受延迟1~10min,定义为准实时)地查看外网WEB服务器中更新的内容。这就给网络管理员提出了一个难题:如何能自动将外网中相关的数据复制到内网中。目前多数网络管理员是通过USB硬盘或刻录光盘的方式,定期将外网服务器中更新的数据复制到内网服务器。也有少数网络管理员在内外网之间添加一台主机作为缓冲器,然后在这台主机与给内外网提供服务的服务器之间使用物理电子开关。由于物理电子开关不支持编程,管理员很难写出相应的自动复制程序,最后依赖手工操作来实现。

上述两种方案由于太多人为的数据拷贝操作,不仅无法保证内网用户及时查看外网的最新数据,也可能会引起内外网WEB数据的不一致。因此,在新的解决方案中,应该做到以下2点:(1)保证外网服务器更新的数据及时完整地更新到内网的WEB服务器中,以便内网用户查阅;(2)防范外部攻击,保证内部网络的安全。

1 解决方案

基于NAS(网络附加存储器)在内外网之间构建一条安全的通道,使内网数据得到及时自动的更新。NAS一般用于以太网中,通过CIFS、NFS、AFP和FTP等协议,向Windows、Unix/Linux和Mac OS等操作系统提供稳定、高效的文件共享服务。其数据镜像功能可以为解决上述难题提供技术支撑。选择上海圣桥信息科技有限公司生产的Storway NAS作为硬件平台。如图1所示,针对上述典型案例,外网部署了一台WEB服务器和一台NAS,NAS和WEB服务器直连,并提供WEB数据存储空间,WEB服务器则向Internet用户提供WEB和BBS等访问。类似于外网,内网也部署一台WEB服务器

收稿日期:2007-09-02
作者简介:唐忠平(1976-),男,讲师,主要从事流媒体服务器技术及计算机网络安全研究。

和一台NAS，NAS和WEB服务器直连，并提供WEB数据存储空间，向内网提供WEB和BBS服务。两台NAS间通过网线直连，由于其数据镜像功能，保证了两台WEB服务器的数据一致性。

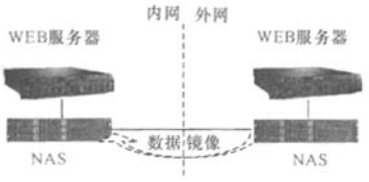

图1 基于NAS数据镜像功能的内外网数据复制

2 方案分析

Storway NAS是专门针对于文件服务优化的操作系统，只提供和文件共享相关的服务，关闭了任何其他不使用的系统端口，结合系统内嵌的防火墙等安全措施，理论上避免了黑客利用系统漏洞进行攻击的可能性。而且管理系统固定在DOM中，与数据存储区域分离，具有较强的病毒免疫能力，比Windows系统更安全，更可靠[1]。

如图1所示，Storway NAS和WEB服务器间采用点对点的直连方式，只有WEB服务器可以直接访问NAS。而且NAS通过其内嵌防火墙的设置，只允许WEB服务器访问其中的文件资源，禁止访问其它服务，也无法登录NAS系统，进一步提高了NAS系统的安全性。

内外网之间的网络连接只有NAS之间的直连网线。通过内网NAS的防火墙设置，禁止外网的任何设备主动访问内网NAS，只允许内网NAS从外网NAS中获取镜像数据，阻止其它任何操作。如图2所示数据镜像采用基于整数有限域离散对数难题的公钥密码算法进行安全验证，从而实现安全的信息通道，保证镜像数据的安全传输。

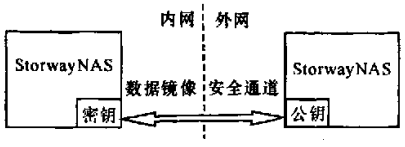

图2 数据安全模型

安全通道只用于外网对内网的数据传输，外网NAS无法利用它登录到内网NAS中，避免了黑客利用外网系统攻击内网系统的可能性。但是，由于内部用户对网络的结构和应用模式都比较了解，因此来自内部的安全威胁也不容忽视，该方案也避免了内部用户通过内网NAS向外网传输数据的可能性，提高了内部网络的安全性。

Storway NAS是基于IP的远程镜像，在使用公钥算法建立安全的信息通道后，通过校验信息判断文件是否被修改，镜像新数据和经过改动的数据，减少了数据传输所需要的时间和对网络带宽的要求。同时采用"copy－on－first－write"的快照技术，获得文件系统某个时刻的系统影像，从而保证NAS系统间数据的一致性。在内网的NAS中配置镜像管理模块，通过其任务管理，使得内网NAS可自动获得外网NAS中更新的数据（如每隔1分钟自动更新一次），以保证内网用户实时查看。

该方案具有如下4个特点。

（1）由于NAS系统采用基于Linux的嵌入式系统，并且关闭了任何不使用的系统端口，其中内嵌的防火墙功能保证数据复制的单向性，合法性，大大提高了NAS系统的安全性，为内外网数据复制提供了可以与物理隔绝相匹配的安全保障；

（2）采用NAS自动化的镜像管理功能，最大程度地减少人工操作，避免了人工操作带来数据不一致性，保证了内部数据的及时更新，提高了系统维护效率。

（3）Storway NAS只镜像新数据和经过改动的数据，降低了对磁盘空间和广域网带宽的要求，保证镜像操作可以在最短的时间内完成，大大提高了数据更新的速度。

（4）采用Storway NAS的数据备份功能，灵活地备份WEB及BBS数据，以提高了用户和系统数据的可靠性。

3 结束语

基于NAS的安全镜像解决方案，能实现数据存储、备份及同步更新等三个方面的功能。保证了外网服务器更新的数据及时完整的更新到内网的WEB服务器中，防范了外部攻击。实践证明它能保证数据的安全性，一致性，同时运行稳定，具有较强的实用性。

参考文献：

[1] 上海圣桥信息科技有限公司. 圣桥Storway NAS用户手册[EB/OL]. [2004-07-21]. http://www.shengqiao.com.cn/support/product/storway/storway-nas-usermanual-2.1.0512.pdf.

（责任编辑：尹 闯）