



整体的安全方案分成技术方案、服务方案以及支持方案三部分。

一、技术解决方案

安全产品是网络安全的基石，通过在网络中安装一定的安全设备，能够使得网络的结构更加清晰，安全性得到显著增强；同时能够有效降低安全管理的难度，提高安全管理的有效性。下面介绍在局域网中增加的安全设备的安装位置以及他们的作用。

1. 防火墙

安装位置：局域网与路由器之间；WWW 服务器与托管机房局域网之间；

局域网防火墙作用：

- 实现单向访问，允许局域网用户访问 INTERNET 资源，但是严格限制 INTERNET 用户对局域网资源的访问；
- 通过防火墙，将整个局域网划分 INTERNET，DMZ 区，内网访问区这三个逻辑上分开的区域，有利于对整个网络进行管理；
- 局域网所有工作站和服务器处于防火墙地整体防护之下，只要通过防火墙设置的修改，就能有限绝大部分防止来自 INTERNET 上的攻击，网络管理员只需要关注 DMZ 区对外提供服务的相关应用的安全漏洞；
- 通过防火墙的过滤规则，实现端口级控制，限制局域网用户对 INTERNET 的访问；
- 进行流量控制，确保重要业务对流量的要求；
- 通过过滤规则，以时间为控制要素，限制大流量网络应用在上班时间的使用。

托管机房防火墙的作用：

- 通过防火墙的过滤规则，限制 INTERNET 用户对 WWW 服务器的访问，将访问权限控制在最小的限度，在这种情况下，网络管理员可以忽略服务器系统的安全漏洞，只需要关注 WWW 应用服务软件的安全漏洞；
- 通过过滤规则，对远程更新的时间、来源(通过 IP 地址)进行限制。

2. 入侵检测

安装位置：局域网 DMZ 区以及托管机房服务器区；

IDS 的作用：

- 作为旁路设备，监控网络中的信息，统计并记录网络中的异常主机以及异常连接；
- 中断异常连接；
- 通过联动机制，向防火墙发送指令，在限定的时间内对特定的 IP 地址实施封堵。

3. 网络防病毒软件控制中心以及客户端软件

安装位置：局域网防病毒服务器以及各个终端防病毒服务器作用：

- 作为防病毒软件的控制中心，及时通过 INTERNET 更新病毒库，并强制局域网中已开机的终端及时更新病毒库软件；
- 记录各个终端的病毒库升级情况；
- 记录局域网中计算机病毒出现的时间、类型以及后续处理措施。

防病毒客户端软件的作用：

- 对本机的内存、文件的读写进行监控，根据预定的处理方法处理带毒文件；
- 监控邮件收发软件，根据预定处理方法处理带毒邮件；

4. 邮件防病毒服务器

安装位置：邮件服务器与防火墙之间

邮件防病毒软件：对来自 INTERNTE 的电子邮件进行检测，根据预先设定的处理方法处理带毒邮件。邮件防病毒软件的监控范围包括所有来自 INTERNET 的电子邮件以及所属附件(对于压缩文件同样也进行检测)

SANDIY IT SERVICE

Construction of the overall enterprise network security solutions



5. 反垃圾邮件系统

安装位置：同邮件防病毒软件，如果软硬件条件允许的话，建议安装在同一台服务器上。

反垃圾邮件系统作用：

- 拒绝转发来自 INTERNET 的垃圾邮件；
- 拒绝转发来自局域网用户的垃圾邮件并将发垃圾邮件的局域网，用户的 IP 地址通过电子邮件等方式通报网管；
- 记录发垃圾邮件的终端地址；
- 通过电子邮件等方式通知网管垃圾邮件的处理情况。

6. 动态口令认证系统

安装位置：服务器端安装在 WWW 服务器(以及其他需要进行口令加强的敏感服务器)，客户端配置给网页更新人员(或者服务器授权访问用户)；

动态口令认证系统的作用：

- 通过定期修改密码，确保密码的不可猜测性。

7. 网络管理软件

安装位置：局域网中。

网络管理软件的作用：

- 收集局域网中所有资源的硬件信息；
- 收集局域网中所有终端和服务器的操作系统、系统补丁等软件信息；
- 收集交换机等网络设备的工作状况等信息；
- 判断局域网用户是否使用了 MODEM 等非法网络设备与 INTERNET 连接；
- 显示实时网络连接情况；
- 如果交换机等核心网络设备出现异常，及时向网管中心报警；

8. QOS 流量管理

安装位置：如果是专门的产品安装在路由器和防火墙之间；部分防火墙本身就有 QOS 带宽管理模块。

QOS 流量管理的作用：

- 通过 IP 地址，为重要用户分配足够的带宽；
- 通过端口，为重要的应用分配足够的带宽资源；
- 限制非业务流量的带宽；
- 在资源闲置时期，允许其他人员使用资源，一旦重要用户或者重要应用需要使用带宽，则确保它们能够至少使用分配给他们的带宽资源。

9. 重要终端个人防护软件

安装位置：重要终端

个人防护软件的作用：

- 保护个人终端不受攻击；
- 不允许任何主机(包括局域网主机)非授权访问重要终端资源；
- 防止局域网感染病毒主机通过攻击的方式感染重要终端。

10. 页面防篡改系统

安装位置：WWW 服务器

页面防篡改系统的作用：

- 定期比对发布页面文件与备份文件，一旦发现不匹配，用备份文件替换发布文件；
- 通过特殊的认证机制，允许授权用户修改页面文件；
- 能够对数据库文件进行比对。

SANDIY IT SERVICE

Construction of the overall enterprise network security solutions



二、安全服务解决方案

在安全服务方案中，采用不同的安全服务，定期对网络进行检测、改进，以达到动态增进网络安全性，最大限度发挥安全设备作用的目的。安全服务分为以下几类：

1. 网络拓扑分析

服务对象：整个网络

服务周期：半年一次

服务内容：

- (1) 根据网络的实际情况，绘制网络拓扑图；
- (2) 分析网络中存在的安全缺陷并提出整改建议意见。

服务作用：针对网络的整体情况，进行总体、框架性分析。一方面，通过网络拓扑分析，能够形成网络整体拓扑图，为网络规划、网络日常管理等管理行为提供必要的技术资料；另一方面，通过整体的安全性分析，能够找出网络设计上的安全缺陷，找到各种网络设备在协同工作中可能产生的安全问题。

2. 中心机房管理制度制订以及修改

服务对象：中心机房

服务周期：半年一次

服务内容：协助用户制订并修改机房管理制度。制度内容涉及人员进出机房的登记制度、设备进出机房的登记制度、设备配置修改的登记制度等。

服务作用：严格控制中心机房的人员进出、设备进出并及时登记设备的配置更新情况，有助于网络核心设备的监控，确保网络的正常运行。

3. 操作系统补丁升级

服务对象：服务器、工作站、终端

服务周期：不定期

服务内容：

- (1) 一旦出现重大安全补丁，及时更新所有相关系统；
- (2) 出现大型补丁(如微软的 SP)，及时更新所有相关系统；

服务作用：通过及时、有效的补丁升级，能够有效防止局域网主机和服务器相互之间的攻击，降低现代网络蠕虫病毒对网络的整体影响，增加网络带宽的有效利用率。

4. 防病毒软件病毒库定期升级

服务对象：防病毒服务器、安装防病毒客户端的终端

服务周期：每周一次

服务内荐：

- (1) 防病毒服务器通过 INTERNET 更新病毒库；
 - (2) 防病毒服务器强制所有在线客户端更新病毒库
- 服务作用：通过不断升级病毒库确保防病毒软件能够及时发现新的病毒。

5. 服务器定期扫描、加固

服务对象：服务器

服务周期：半年一次

服务内容：使用专用的扫描工具，在用户网络管理人员的配合，对主要的服务器进行扫描。

服务作用：

- (1) 找出对应服务器操作系统中存在的系统漏洞；
- (2) 找出服务器对应应用服务中存在的系统漏洞；
- (3) 找出安全强度较低的用户名和用户密码。

6. 防火墙日志备份、分析

服务对象：防火墙设备

服务周期：一周一次

服务内容：导出防火墙日志并进行分析。

服务作用：通过流量简图找出流量异常的时间段，通过检查流量较大的主机，找出局域网中的异常主机。

7. 入侵检测等安全设备日志备份

服务对象：入侵检测等安全设备

服务周期：一周一次

服务内容：备份安全设备日志。

服务作用：防止日志过大导致检索、分析的难度，另一方面也有利于事后的检查。

8. 服务器日志备份

服务对象：主要服务器(如 WWW 服务器、文件服务器等)

服务周期：一周一次

服务内容：备份服务器访问日志

服务作用：防止日志过大导致检索、分析的难度，另一方面也有利于事后的检查。

SANDIY IT SERVICE

→ Construction of the overall enterprise network security solutions

9. 白客渗透

服务对象：对INTERNET 提供服务的服务器

服务周期：半年一次

服务内容：服务商在用户指定的时间段内，通过INTERNET，使用各种工具在不破坏应用的前提下攻击服务器，最终提供检测报告。

服务作用：先于黑客进行探测性攻击以检测系统漏洞。根据最终检测报告进一步增强系统的安全性

10. 设备备份系统

服务对象：骨干交换机、路由器等网络骨干设备

服务周期：实时

服务内容：根据用户的网络情况，提供骨干交换机、路由器等核心网络设备的备份。备份设备可以在段时间内替代网络中实际使用的设备。

服务作用：一旦核心设备出现故障，使用备件替换以减少网络故障时间。

11. 信息备份系统

服务对象：所有重要信息

服务周期：根据网络情况定完全备份和增量备份的时间

服务内容：定期备份电子信息

服务作用：防止核心服务器崩溃导致网络应用瘫痪。

12. 定期总体安全分析报告

服务对象：整个网络

服务周期：半年一次

服务内容：综合网络拓扑报告、各种安全设备日志、服务器日志等信息，对网络进行总体安全综合性分析，分析内容包括网络安全现状、网络安全隐患分析，并提出改进建议意见。

服务作用：提供综合性、全面的安全报告，针对全网络进行安全性讨论，为全面提高网络的安全性提供技术资料。

以上是服务解决方案，众所周知，安全产品一般是共性的产品，通过安全服务，能够配制出适合本网络的安全设备，使得安全产品在特定的网络中发挥最大的效能，使得各种设备协同工作，增强网络的安全性和可用性。

当然，在网络中，不全是绝对的，即使采取种种措施，网络也可能遭到应用某种原因无法正常运作，这时候，就需要有及时有效的技术支持，使得网络在尽可能短的时间内恢复正常。下面将提出技术支持解决方案。

SANDIY IT SERVICE

Construction of the overall enterprise network security solutions

三、持解决方案

技术支持是整个安全方案的重要补充。其主要作用是在用户网络发生重要安全事件后，通过及时、高效的安全服务，达到尽快恢复网络应用的目的。技术支持主要包括以下几方面：

1、故障排除

支持范围：

- a 用户无法访问网络(如局域网用户无法访问 INTERNET)；
- b 应用服务无法访问(如不能对外提供 WWW 服务)；
- c 网络访问异常(如访问速度慢)。

作用：一旦网络出现异常，为用户提供及时、有效的网络服务。在最短的时间内恢复网络应用。

2、灾难恢复

- a 支持范围：设备遇到物理损害网络应用异常。
作用：通过备品备件，快速恢复网络硬件环境；通过备份文件的复原，尽快恢复网络的电子资源；由此可在最短的时间内恢复整个网络应用。

3、查找攻击源

- a 支持范围：网络管理员发现网络遭到攻击，并需要确定攻击来源。
作用：通过日志文件等信息，确定攻击的来源，为进一步采取措施提供依据。

4、实时检索日志文件

- a 支持范围：遭到实时的攻击(如 DOS, SYN FLOODING 等)，需要及时了解攻击源以及攻击强度。
作用：通过实时检索日志文件，可以当时存在的针对本网络的攻击并查找出攻击源。如果攻击强度超出网络能够承受的范围，可采取进一步措施进行防范。

5、即时查杀病毒

- a 支持范围：由不可确定的因素导致网络中出现计算机病毒。
作用：即使网络中出现病毒，通过及时有效的技术支持，在最短的时间内查处感染病毒的主机并即时查杀病毒，恢复网络应用。

6、即时网络监控

- a 支持范围：网络出现异常，但应用基本正常。
作用：通过网络监控，近可能发现网络中存在的前期网络故障，在故障扩大化以前及时进行防治。

以上是技术支持解决方案，技术支持是安全服务的重要补充部分，即使在完善的安全体系下，也存在不可预测的因素导致网络故障，此时，需要及时、有效的技术支持服务，在尽可能短的时间内恢复网络的正常运行。

综上所述，局域网的安全由三大部分组成，涵盖设备、技术、制度、管理、服务等各个部分。

SANDIY IT SERVICE

→ Construction of the overall enterprise network security solutions



四、实施建议意见

网络安全涉及面相当广，同时进行建设的可行性较差，因此，建议按照以下方式进行分阶段实施。

1. 第一阶段

- a 技术方面，采用防火墙、网络防病毒软件、页面防篡改系统来建立一个结构上较完善的网络系统。
- b 服务方面，进行网络拓扑分析、建立中心机房管理制度、建立操作系统以及防病毒软件定期升级机制、对重要服务器的访问日志进行备份，通过这些服务，增强网络的抗干扰性。
- c 支持方面，要求服务商提供故障排除服务，以提高网络的可靠性，降低网络故障对网络的整体影响。

2. 第二阶段

在第一阶段安全建设的基础上，进一步增加网络安全设备，采纳新的安全服务和技术支持来增强网络的可用性。

- a 技术方面，采用入侵检测、邮件防病毒软件、动态口令认证系统、并在重要客户端安装个人版防护软件。
- b 服务方面，对服务器进行定期扫描与加固、对防火墙日志进行备份与分析、对入侵检测设备的日志进行备份、建立设备备份系统以及文件备份系统。
- c 支持方面，要求服务商提供灾难恢复、实时日志检索、实时查杀病毒、实时网络监控等技术支持。

3. 第三阶段

在这一阶段，采取的措施以进一步提高网络效率为主。

- a 技术方面，采用反垃圾邮件系统、网络管理软件、QOS 流量管理软件。
- b 服务方面，采用白客渗透测试，要求服务商定期提供整体安全分析报告。
- c 支持方面，要求能够实时或者时候查找攻击源。

以上针对用户网络分别从三个方面提出了安全解决方案，并按照实施的紧迫性分成三个阶段来实现，但是实际针对某个用户，对于安全的要求可能各不相同，具体网络情况也可能有很大的差异，因此建议用户根据实际情况建立网络安全建设的时间表。

另外，随着新技术、新产品的不断涌现，网络技术的不断发展，对于网络安全的要求不断提高，在实际实施过程中采取的措施完全可能超越文中提及的产品、服务、支持，这也是安全建设的最基本原则：不断改进，不断增强，安全无止境。