企业网络系统安全综合解决方案

网络系统的安全威胁

防火墙是目前最为流行也是使用最为广泛的一种网络安全技术。在构建安全网络环境的过程中，防火墙作为第一道安全防线，正受到越来越多用户的关注。防火墙是一个系统，主要用来执行两个网络之间的访问控制策略。它可为各类企业网络提供必要的访问控制，但又不造成网络的瓶颈，并通过安全策略控制进出系统的数据，保护企业的关键资源。

防火墙保护着内部网络的敏感数据不被窃取和破坏，并记录内外通信的有关状态信息日志，如通信发生的时间和进行的操作等等。新一代的防火墙甚至可以阻止内部人员将敏感数据向外传输。企业在把公司的局域网联入 Internet 时，肯定不希望让全世界的人随意翻阅公司内部的工资单、个人资料或是客户数据库。即使在公司内部，同样也存在这种数据非法存取的可能性。例如一些对公司不满的员工可能会修改工资表和财务报告。而在设置了防火墙以后，就可以对网络数据的流动实现有效的管理：允许公司内部员工使用电子邮件、进行 Web 浏览以及文件传输等服务，但不允许外界随意访问公司内部的计算机，同样还可以限制公司中不同部门之间互相访问。将局域网络放置于防火墙之后可以有效阻止来自外界的攻击。

防火墙负责管理风险区域和内部网络之间的访问。在没有防火墙时，内部网络上的每个节点都暴露给风险区域上的其它主机，极易受到攻击。也就是说，内部网络的安全性要由每一个主机来决定，并且整个内部网络的安全性等于其中防护能力最弱的系统。由此可见，对于联接到因特网的内部网络，一定要选用适当的防火墙。

由于大型网络系统内运行多种网络协议(TCP/IP，IPX/SPX，NETBEUA)，而这些网络协议并非专为安全通讯而设计。所以，网络系统可能存在的安全威胁来自以下方面：

1. 操作系统的安全性。目前流行的许多操作系统均存在安全漏洞，如 UNIX 及 Windows 系列产品。
2. 防火墙的安全性。防火墙产品自身是否安全，是否设置错误，需要经过检验。
3. 来自内部网用户的安全威胁。

4. 缺乏有效的手段监视、评估网络系统的安全性。
5. 采用的 TCP/IP 协议族软件，本身缺乏安全性。
6. 未能对来自 Internet 的电子邮件挟带的病毒及 Web 浏览可能存在的恶意 Java/ActiveX 控件进行有效控制。
7. 应用服务的安全。许多应用服务系统在访问控制及安全通讯方面考虑较少，并且，如果系统设置错误，很容易造成损失。

系统的安全应具备以下功能

- 访问控制。通过对特定网段、服务建立的访问控制体系，将绝大多数攻击阻止在到达攻击目标之前。
- 检查安全漏洞。通过对安全漏洞的周期检查，即使攻击可到达攻击目标，也可使绝大多数攻击无效。
- 攻击监控。通过对特定网段、服务建立的攻击监控体系，可实时检测出绝大多数攻击，并采取响应的行动（如断开网络连接、记录攻击过程、跟踪攻击源等）。
- 加密通讯。主动的加密通讯，可使攻击者不能了解、修改敏感信息。
- 认证。良好的认证体系可防止攻击者假冒合法用户。
- 备份和恢复。良好的备份和恢复机制，可在攻击造成损失时，尽快地恢复数据和系统服务。
- 多层防御。攻击者在突破第一道防线后，延缓或阻断其到达攻击目标。
- 设立安全监控中心，为信息系统提供安全体系管理、监控、保护及紧急情况服务。

局域网安全解决方案

由于局域网中采用广播方式,因此,若在某个广播域中可以侦听到所有的信息包，黑客就可以对信息包进行分析，那么本广播域的信息传递都会暴露在黑客面前。

网络分段

网络分段是保证安全的一项重措施，同时也是一项基本措施，其指导思想在于将非法用户与网络资源相互隔离，从而达到限制用户非法访问的目的。

网络分段可分为物理分段和逻辑分段两种方式：

物理分段通常是指将网络从物理层和数据链路层（ISO/OSI 模型中的第一层和第二层）上分为若干网段，各网段相互之间无法进行直接通讯。目前，许多交换机都有一定的访问控制能力，可实现对网络的物理分段。

逻辑分段则是指将整个系统在网络层（ISO/OSI 模型中的第三层）上进行分段。例如，对于 TCP/IP 网络，可把网络分成若干 IP 子网，各子网间必须通过路由器、路由交换机、网关或防火墙等设备进行连接，利用这些中间设备（含软件、硬件）的安全机制来控制各子网间的访问。

在实际应用过程中，通常采取物理分段与逻辑分段相结合的方法来实现对网络系统的安全性控制。

VLAN 的实现

虚拟网技术主要基于近年发展的局域网交换技术（ATM 和以太网交换）。交换技术将传统的基于广播的局域网技术发展为面向连接的技术。因此，网管系统有能力限制局域网通讯的范围而无需通过开销很大的路由器。

以太网从本质上基于广播机制，但应用了交换机和 VLAN 技术后，实际上转变为点到点通讯，除非设置了监听口，信息交换也不会存在监听和插入（改变）问题。

由以上运行机制带来的网络安全的好处是显而易见的:信息只到达应该到达的地点。因此，防止了大部分基于网络监听的入侵手段。通过虚拟网设置的访问控制，使在虚拟网外的网络节点不能直接访问虚拟网内节点。但是，虚拟网技术也带来了新的问题：

执行虚拟网交换的设备越来越复杂，从而成为被攻击的对象。

基于网络广播原理的入侵监控技术在高速交换网络内需要特殊的设置。

基于 MAC 的 VLAN 不能防止 MAC 欺骗攻击。

采用基于 MAC 的 VLAN 划分将面临假冒 MAC 地址的攻击。

因此，VLAN 的划分最好基于交换机端口。但这要求整个网络桌面使用交换端口或每

个交换端口所在的网段机器均属于相同的 VLAN。

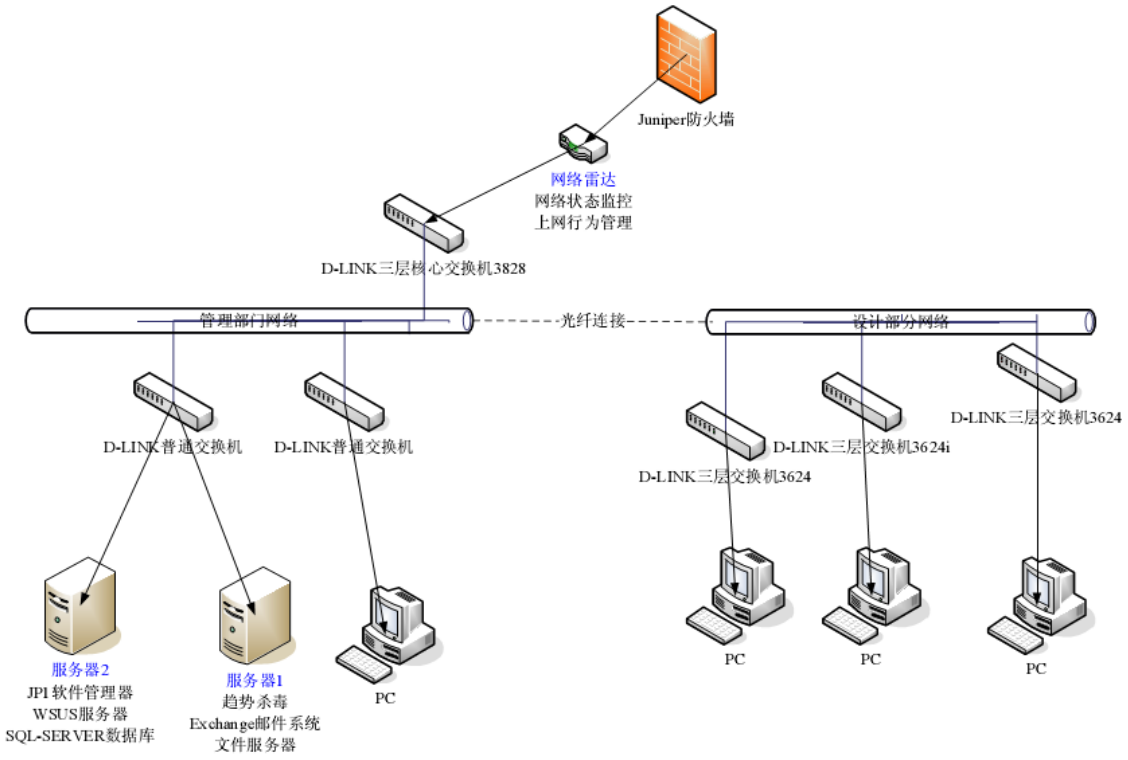
VLAN 之间的划分原则

VLAN 的划分方式的目的是保证系统的安全性。因此，可以按照系统的安全性来划分 VLAN：

可以将总部中的服务器系统单独划作一个 VLAN，如数据库服务器、电子邮件服务器等。

也可以按照机构的设置来划分 VLAN,如将领导所在的网络单独作为一个 Leader VLAN（LVLAN），其它司局（或下级机构）分别作为一个 VLAN，并且控制 LVLAN 与其它 VLAN 之间的单向信息流向，即允许 LVLAN 查看其他 VLAN 的相关信息，其他 VLAN 不能访问 LVLAN 的信息。

VLAN 之内的连接采用交换技术实现，VLAN 与 VLAN 之间采用路由实现。由于路由控制的能力有限,不能实现 LVLAN 与其他 VLAN 之间的单向信息流动,需要在 LVLAN 与其他 VLAN 之间设置一个 PAL-NetS 防火墙作为安全隔离设备，控制 VLAN 与 VLAN 之间的信息交换。



INTERNET 互连安全解决方案

众所周知，作为全球使用范围最大的信息网，Internet 自身协议的开放性极大地方便了各种计算机入网，拓宽了共享资源。但是，由于在早期网络协议设计上对安全问题的忽视，以及在使用和管理的无政府状态，逐渐使 Internet 自身的安全受到严重威胁，与它有关的安全事故屡有发生。对网络安全的威胁主要表现在：非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒、线路窃听等方面。这就要求我们对与 Internet 互连所带来的安全性问题予以足够重视。

在大型网络系统与 Internet 互连的第一道屏障就是防火墙，防火墙的主要作用是在网络入口点检查网络通讯，根据客户设定的安全规则，在保护内部网络安全的前提下，提供内外网络通讯。

使用 Firewall 的益处

1. 保护脆弱的服务

通过过滤不安全的服务，Firewall 可以极大地提高网络安全和减少子网中主机的风险。例如，Firewall 可以禁止 NIS、NFS 服务通过，Firewall 同时可以拒绝源路由和 ICMP 重定向封包。

2. 控制对系统的访问

Firewall 可以提供对系统的访问控制。如允许从外部访问某些主机，同时禁止访问另外的主机。例如，Firewall 允许外部访问特定的 Mail Server 和 Web Server。

3. 集中的安全管理

Firewall 对企业内部网实现集中的安全管理，在 Firewall 定义的安全规则可

以运行于整个内部网络系统，而无须在内部网每台机器上分别设立安全策略。Firewall 可以定义不同的认证方法，而不需要在每台机器上分别安装特定的认证软件。外部用户也只需要经过一次认证即可访问内部网。

4. 增强的保密性

使用 Firewall 可以阻止攻击者获取攻击网络系统的有用信息,如 Figer 和 DNS。

5. 记录和统计网络利用数据以及非法使用数据

Firewall 可以记录和统计通过 Firewall 的网络通讯，提供关于网络使用的统计数据，并且，Firewall 可以提供统计数据，来判断可能的攻击和探测。

6. 策略执行

Firewall 提供了制定和执行网络安全策略的手段。未设置 Firewall 时，网络安全取决于每台主机的用户。

设置防火墙的要素

网络策略

影响 Firewall 系统设计、安装和使用的网络策略可分为两级，高级的网络策略定义允许和禁止的服务以及如何使用服务,低级的网络策略描述 Firewall 如何限制和过滤在高级策略中定义的服务。

服务访问策略

服务访问策略集中在 Internet 访问服务以及外部网络访问（如拨入策略、SLIP/PPP 连接等)。

服务访问策略必须是可行的和合理的。可行的策略必须在阻止已知的网络风险和提供用户服务之间获得平衡。典型的服务访问策略是：允许通过增强认证的用户在必要的情况下从 Internet 访问某些内部主机和服务；允许内部用户访问指定的 Internet 主机和服务。

防火墙设计策略

防火墙设计策略基于特定的 Firewall，定义完成服务访问策略的规则。通常有两种基本的设计策略：

允许任何服务除非被明确禁止；禁止任何服务除非被明确允许。第一种的特点是安全但不好用，第二种是好用但不安全，通常采用第二种类型的设计策略。 而多数防火墙都在两种之间采取折衷。

增强的认证

许多在 Internet 上发生的入侵事件源于脆弱的传统用户/口令机制。多年来，用户被告知使用难于猜测和破译口令，虽然如此，攻击者仍然在 Internet 上监视传输的口令明文，使传统的口令机制形同虚设。

增强的认证机制包含智能卡，认证令牌，生理特征（指纹）以及基于软件（RSA）等技术，来克服传统口令的弱点。

虽然存在多种认证技术，它们均使用增强的认证机制产生难被攻击者重用的口令和密钥。目前许多流行的增强机制使用一次有效的口令和密钥（如 SmartCard 和认证令牌）。

防火墙在大型网络系统中的部署

- 根据网络系统的安全需要，可以在如下位置部署防火墙：
- 局域网内的 VLAN 之间控制信息流向时。
- Intranet 与 Internet 之间连接时(企业单位与外网连接时的应用网关)。
- 在广域网系统中，由于安全的需要，总部的局域网可以将各分支机构的局域网看成不安全的系统，（通过公网 ChinaPac，ChinaDDN，Frame Relay 等连接）在总部的局域网和各分支机构连接时采用防火墙隔离，并利用 VPN 构成虚拟专网。
- 总部的局域网和分支机构的局域网是通过 Internet 连接，需要各自安装防火墙，并利用 PAL-NetS 的 VPN 组成虚拟专网。
- 在远程用户拨号访问时，加入虚拟专网。
- ISP 可利用 PAL-NetS 的负载平衡功能在公共访问服务器和客户端间加入防火墙

进行负载分担、存取控制、用户认证、流量控制、日志纪录等功能。

- 两网对接时，可利用 PAL-NetS 硬件防火墙作为网关设备实现地址转换(NAT)，地址映射（MAP），网络隔离（DMZ），存取安全控制，消除传统软件防火墙的瓶颈问题。

防火墙在网络系统中的作用

防火墙能有效地防止外来的入侵，它在网络系统中的作用是：

- 控制进出网络的信息流向和信息包；
- 提供使用和流量的日志和审计；
- 隐藏内部 IP 地址及网络结构的细节；
- 提供 VPN 功能；