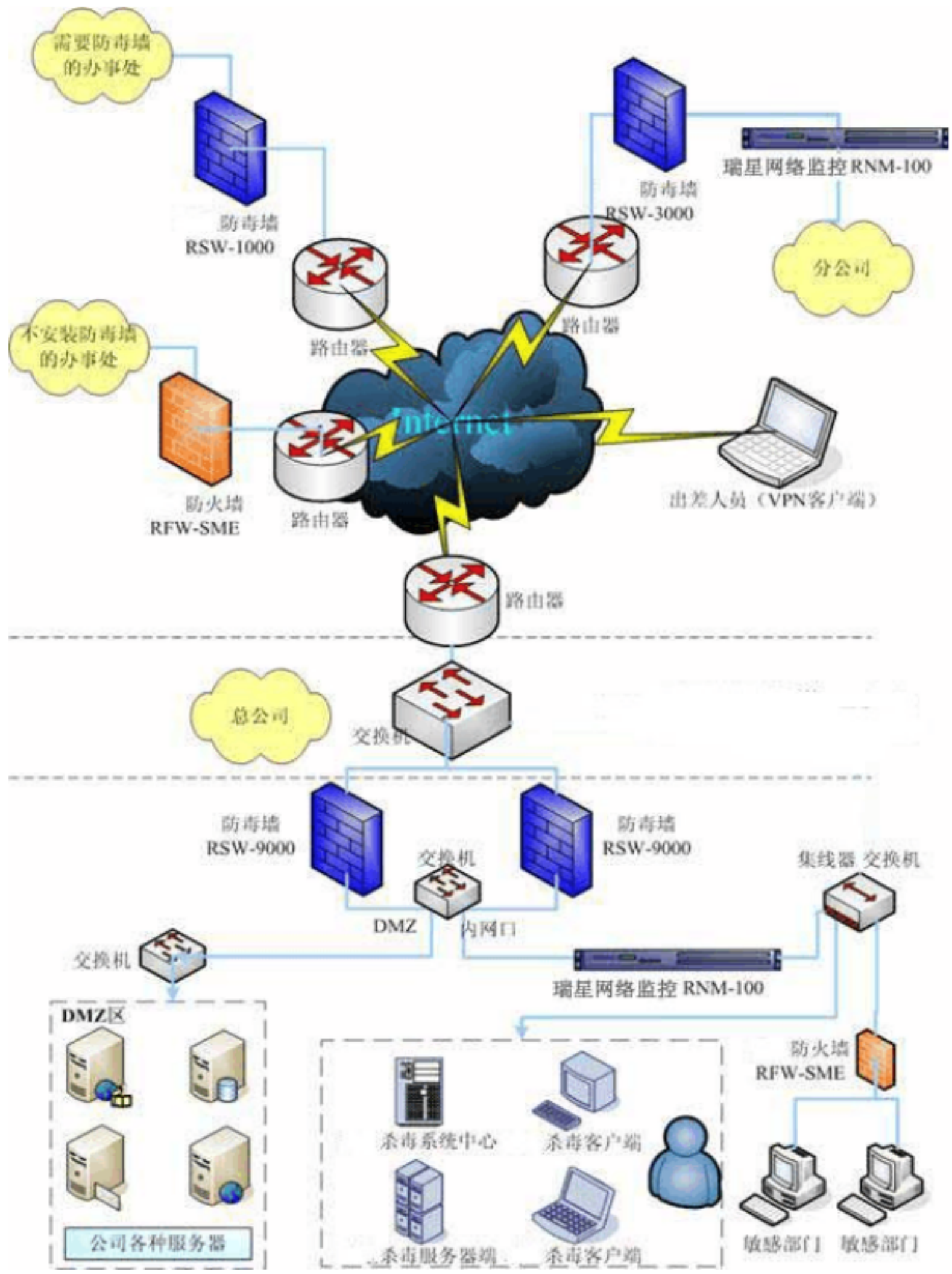
摘要： 无线网状网由网格路由器和网格客户端组成，其中网状路由器具有最小可移动性，形成了无线网状网的骨干，它们同时为网状客户端和普通客户端提供网络访问。针对大型公司，网络情况复杂，针对这种网络环境，网络安全尤其重要。无线网状网将承载大量不同应用的无线服务。 尽管近期无线网状网有了快速进步，但许多研究始终面临着各协议层的挑战。 本文将呈现给大家针对某大型公司的网络拓扑， 进行网络安全规划。本文将从分析安全需求、制定安全策略、完善安全措施、部署安全产品、强化安全管理五个方面来阐述对问题的分析和解决。

关键词： 网络安全；安全审计；路由协议；安全策略；

一. 网络结构示意图以及安全设计要求

1.网络拓扑图如下



2.安全设计要求

设计一套基于入侵检测、安全审计、安全扫描的安全解决方案。

要求从分析安全需求、指定安全策略、完善安全措施、部署安全产品、 强化安全管理五个方面来阐述设计的安全方案。

二. 网络安全需求分析

1.主要网络安全威胁

网络系统的可靠于准是基于通讯子网、计算机硬件和操作系统及各种应用软件等各方面、各层次的良好运行。 因此， 它的风险将来自于企业的各个关键点可能造成的威胁， 这些威胁可能造成总体功能的失效。 由于在这种广域网分布式计算环境中， 相对于过去的局域网、主机环境、 单机环境， 安全问题变得越来越复杂和突出， 所以网络安全分析成为制定有效的安全管理策略和选择有作用的安全技术实施措施的基础。 安全保障不能完成基于思想教育或新任。而应基于“ 最低权限 ”和“ 互相监督 ”法则，减少保密信息的介入范围，尽力消除使用者为使用资源不得不信任他人或被他人信任的问题， 建立起完整的安全控制体系和保证体系。

通过以上对该网络结构的分析和阐述， 目前该网络的规模大， 结构复杂， 包括下属多个分公司和办事处，通过 VPN 和总公司联通的出差人员。该网络上运行着各种各样的主机和应用程序，使用了多种网络设备；同时，由于多种业务需求，又和许多其他网络进行连接。因此，该计算机网络安全应该从以下几个方面进行考虑：

（**1**）外部网络连接及数据访问

出差在外的移动用户的连接；

分公司主机对总公司和其他分公司办事处的连接；

各种类型的办事处对总公司和分公司的连接；

托管服务器网站对外提供的公共服务；

（**2**）内部网络连接

通过 DDN 专线连接的托管服务器网站；

办公自动化网络；

（**3**）同一网段中不同部门间的连接

连接在同一交换机上的不同部门的主机和工作站的安全问题；

其中外部网络攻击威胁主要来自（ 1），内部网络安全问题集中在（ 2）、（3）。

2.来自外部网络与内部网络的安全威胁

（**1**）来自外部网络的安全威胁

由于业务的需要， 网络与外部网络进行了连接， 这些安全威胁主要包括： 内部网络和这些外部网络之间的连接为直接连接，外部网络可以直接访问内部 网络主机。由于外部和内部通过一条 VPN 隧道相连通没有相应的隔离措施，内部系统比较容易遭到攻击。

由于业务需要， 公司员工经常需要出差， 并且该移动用户使用当地的 ISP 拨号上网连接上 Internet 进入内部网网络，这时非法的 Internet 用户也可以通过各种手段访问内部网络。这种连接使内部网络很容易受到来自 Internet 的攻击。

对于来自外网的各种攻击， 我们可以利用防病毒、 防火墙和防黑客技术加以防范。 在本次分析的拓扑图中对于总公司的内网， 在内网口分别加入了网络监控设备， 杀毒中心和防火墙，能够有效的抵御来自外网的大部分攻击。

（**2**）来自内部网络的安全威胁

从拓扑图中可以看到， 该企业整个计算机网络有一定的规模， 分为多个层次， 网络上的节点众多，网络应用复杂，网络管理困难。管理的难点主要有：网络实际结构无法控制；网管人员无法及时了解网络的运行状况； 无法了解网络的漏洞和可能发生的攻击； 对于已经或正在发生的攻击缺乏有效的追查手段。

内部网络的安全涉及到技术、 应用以及管理等多方面的因素， 只有及时发现问题， 确定网络安全威胁的来源才能制定全面的安全策略，有效的保证网络安全。

三．安全策略制定

安全策略分安全管理策略和安全技术实施策略两个方面：

（**1**）安全管理策略

安全系统需要人来执行， 即使是最好的、 最值得信赖的系统安全措施， 也不能完全由计算机系统来完全承担安全保证任务，因此必须建立完备的安全组织和管理制度。

（**2**）安全技术策略

技术策略要针对网络、操作系统、数据库、信息共享授权提出具体措施。

由于网络的互连是在链路层、网络层、传输层、 应用层不同协议层来实现，各个层的功能特性和安全特性也不同，因而其网络安全措施也不相同。

物理层安全涉及传输介质的安全特性， 抗干扰、防窃听将是物理层安全措施制定的重点。在链路层， 通过“ 桥 ”这一互连设备的见识和控制作用，使我们可以建立一定程度的虚拟局域网，对物理和逻辑网段进行有效的分割和隔离， 消除不同安全级别逻辑网段间的窃听可能。在网络层，可以通过对不同子网的定义和对路由器的路由表控制来限制子网间的接点通信，通过对主机路由表的控制来控制与之直接通信的节点。 同时， 利用网关的安全控制能力， 可以限制节点的通信、 应用服务， 并加强外部用户识别和验证能力。 对网络进行级别划分与控制，网络级别的划分大致包括 Internet—企业网、骨干网—区域网、区域网—部门网、部门网—工作组网等。其中 internet —企业网的接口要采用专业防火墙，骨干网—区域网、区域网—部门网的接口利用路由器的可控路由表、 安全邮件服务器、 安全拨号验证服务器和安全级别较高的操作系统。增强网络互连的分割和过滤控制，也可以大大提高安全保密性。

四．安全措施完善

中心的网络结构中采用了大量的交换机， 作为骨干交换设备的交换机往往也是攻击者发起攻击的对象， 一旦交换机被攻击， 整个网络可能存在瘫痪的严重后果， 交换机内依赖的是固有的网络操作系统 ios，解决交换机的安全问题也应依靠口令和自身漏洞修补等多方面来考虑。

中心互连设备中使用了大量的路由、交换设备。他们都支持 SNMP 简单网管协议，并且目前我们的监控体系是符合 SNMP 协议来实现监控功能的，这些设备都维护着一个含有设备运行状态、接口信息等资料的 MIBS 库，运行着 SNMP 的主机或设备可以成为 SNMP AGENT 。SNMP 管理端和代理端的通信验证问题仅仅取决两个 community 值，一个是 RO 值，另一个是 RW 值，拥有 RO 值的管理端可以查看设备的一些信息包括名称、接口、 ip 地址等；拥有 RW 值得管理端则可以完全管理该设备。但大多支持 SNMP 的互连设备都是出于运行模式，至少有一个 RO 的默认值为 public，这样会泄露很多的重要信息。另外，拥有 RW 默认值的设备在互联网上也很多，导致互联网设备的瘫痪和流量不正常，如果没有冗余设备，那样整个内部网络就会瘫痪。

另外还需要在内网对 VLAN 进行安全划分。在骨干将还击上按不同应用划分 VLAN ，并配置三层路由，按照应用和职责平直访问控制列表，重点保护内网中重要的部门 VLAN ，在其他交换机上配置 trunk on，使其识别骨干交换机的 VLAN 划分和安全策略配置。 将网络

设备的管理 IP 设置在受保护的 VLAN 中，并修改 ACL 使得其他网段的主机无法远程登录到交换机系统。登录交换机后对链路实施加密传输，保证信息不被窃取。

五. 部署安全产品

在进行网络安全方案的产品选择时，要求安全产品至少应包含以下功能：

（1）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；

（2）检查安全漏洞：通过对安全漏洞的周期检查，即使攻击可以达到目标，也可使绝大多数攻击无效；

（3）攻击监控：通过对特定网段、服务建立的攻击监控体系，可实时监测出绝大多数攻击，并采取相应的行动（如断开网络连接、记录攻击过程、跟踪攻击源等）；

（4）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；

（5）认证：良好的认证体系可防止攻击者假冒合法用户；

（6）备份和回复：良好的备份和恢复机制，可以在攻击造成损失时，尽快的恢复数据和系统服务；

（7）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；

（8）隐藏内部信息：使攻击者不能了解系统内部的基本情况；

（9）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。

六. 强化安全管理

计算机信息系统的安全管理主要基于三个原则：

（1）多人负责原则

每项与安全有关的活动必须有两人或多人在场。

（2）任期有限原则

一般来说，任何人最好不要长期担任与安全有关的职务。

（3）职责分离原则

除非系统主管领导批准， 在信息处理系统工作的人员不要打听、 了解或参与职责外、 与安全有关的任何事。

信息系统的安全管理部门应根据以上管理原则和该系统处理数据的保密性， 指定相应的管理制度或采用相应的规范， 其具体工作有： 确定该系统的安全等级； 根据确定的安全等级，

确定安全管理的范围；　制定相应的机房出入管理制度，　对安全等级要求较高的系统，　要实行分区控制，　限制工作人员出入与己无关的区域；　制定严格的操作规程，　操作规程要根据职责分离和多人负责原则，各负其责，不能超越自己的管辖范围；　指定完备的系统维护制度，维护时要首先经过主管部门的批准，　并有安全管理人员在场，　故障原因、 维护内容和维护前后的情况要详细记录；指定应急措施，要制定在紧急情况下，系统如何尽快恢复的应急措施，使损失减至最小。

安全系统需要由人来计划和管理，　任何系统安全设施也不能完全由计算机系统独立承担系统安全保障的任务。　对各级用户的培训十分重要，　只有当用户对网络安全性有了深入了解之后，才能降低网络信息系统的安全风险。