基于运营商网络的防火墙部署方案的设计与实施

**摘 要：**21世纪以来，随着互联网+时代的不断发展和进步，人们的生活变得越来越智能化。而这一切都离不开网络的支持，其中计算机网络安全也引起了社会各界的广泛关注。尤其是近些年来；不法分子利用各种计算机网络漏洞窃取重要信息谋取欺诈利益，引发网络安全问题。对此，研究防火墙技术在整个计算机网络安全中的应用，可以有效预防和监管在计算机中网络安全中存在的威胁。

本论文以某运营商网络为例，根据目前该运营商企业网络的情况作出相应的防火墙部署研究与分析。遵循合法性、实用性、整体性、可靠性、安全性、高拓展性、先进性、可管理性等原则；提供一个低成本，高效率，能够保证企业级网络安全与信息安全的建设方案，通过实践表明，该方案设计合理，可以满足运营商网络的网络安全要求。

**关键词：**网络安全；运营商网络；防火墙；

**Design and Implementation of Firewall Deployment Scheme based on Operators Network**

**Abstract：**Since the 21st century, with the continuous development and progress of the Internet + era, people's life has become more and more intelligent. And all this is inseparable from the support of the network, among which computer network security has also attracted wide attention from all walks of society. Especially in recent years, criminals use various computer network loopholes to steal important information for fraud, causing network security problems. In this regard, the application of firewall technology in whole computer network security can effectively prevent and supervise threats in network security in computers.

This paper takes an operator network as an example and analyzes the current situation of the operator enterprise network. Follow the principles of legality, practicability, integrity, reliability, security, high expansion, advanced, manageability, provide a low cost, efficient, can ensure enterprise network security and information security, through practice shows that the design is reasonable, can meet the network security requirements of operator network.

**Keywords：**Network security; operator network; firewall;

# **第1章 概述**

## 1.1 课题的背景及意义

21世纪以来，随着互联网+时代的不断发展和进步，高端智能产业的发展都离不开网络技术的支持。计算机网络迅速进入我们的日常工作和学习。目前，网络系统具有信息共享、实时传输、距离相消等高质量特性，使得企业实现了高效、协作、管理和管理的精细化。然而，企业的网络汇总通常会涉及到木马、病毒、系统漏洞等安全问题。严重损害了网络的健康发展。而这一切的原因，主要还是由于企业内部员工们网络安全防范意识不强，导致企业网络安全和信息安全的不牢固。

如今，在互联网技术高速发展推动着社会生产力快速提高；然而，因为互联网技术的传递性、自由性、实时性、交换性、共享性、开放性，企业员工在上班时间会占用公司的网络资源进行一些个人的活动，比如在上班时使用公司提供的网络服务打游戏、浏览时事热点、追剧等。这类行为会使企业网络资源紧张，导致企业网络性能不佳；而且，这种上班“摸鱼”的行为，严重影响员工的工作效率，是企业的隐形损失。

另外，员工占用公司网络资源进行私用，很有可能给企业带来严重的网络安全问题，比如说因为某员工在上班时间随意浏览互联网站点，让公司电脑中毒了，一步步导致公司内部服务器受到病毒感染，情节严重者甚至会导致公司网络瘫痪，公司的重要数据文件损坏。这些网络安全问题使企业面临财务损失和不可预测的法律风险。 因此，加强网络行为管理的约束力，提高企业的运营效率，最大限度地降低经营风险就显得尤为重要。

## 1.2 国内外研究现状

随着网络技术的发展，网络安全成了新的研究热点。国内外均有很多研究机构在网络安全方面的工作。主要从数据加密技术、身份认证、数字签名、防火墙、安全审计、网络安全性分析、网络信息安全监测、信息安全标准化等方面进行研究。

防火墙研究始于90年代初，至今已发展三十多年。防火墙技术涉及到计算机网络技术、加密技术、安全技术、安全协议、安全操作系统等多方面。目前不断有新技术应用于防火墙的开发上，如 VPN、状态检测技术、无线热点、上网行为管理、防病毒技术等。目前的防火墙产品基本是多元化一体机类型，除了传统防火墙的功能外，还能提供应用识别与管理、流量分析、入侵防护、提供日志记录和统计报表等功能，并逐步实现安全与效能的最大化，成为企业网络防护的第一门神。

## 1.3 本次课题的主要内容

本人此次论文主要是以国内某运营商网络的防火墙部署方案的设计与实施来书写的，一开始我认真学习了防火墙技术及其在网络安全中的作用的理论知识，探索国内外防火墙的历史和现状，分析特定运营商的日常网络需求以及在构建研究型网络安全方面的差距，为本文提供坚实的理论基础。

# **第2章 相关技术简介**

## 2.1 防火墙简介

### 2.1.1 防火墙的定义

防火墙是在不同网络（如受信任的内网和不受信任的公共网络）或网络安全域之间配置的组件的组合。它监视、限制和修改通过防火墙的数据流，从外部尽可能地保护网络的内部信息、结构和运行状态，并保护网络。

### 2.1.2 防火墙的发展史

纵观历史长河，传统防火墙技术经过了四个阶段；

1、第一阶段防火墙是基于路由器的防火墙。由于大多数路由器都具有包过滤功能，因此可以通过路由控制来实现网络访问控制功能，具有包过滤功能的路由器成为第一代防火墙产品。

2、第二阶段的防火墙其是一个自定义防火墙工具包。第二级防火墙将防火墙的过滤能力与原有路由器分离，增加告警和审计能力，提供满足用户和用户需求的模块化软件包（通过网络发送）。 使得用户可以自行构造防火墙。第二代防火墙具有低成本，高安全等特点。但因为它是纯软件型产品，所以他的实际处理速度和适用人群都有一定的局限性。

3、第三阶段的防火墙产品是建立在通用操作系统之上的防火墙。其主要功能包括具有专用代理系统的数据包过滤、所有协议的数据和指令监控、用户编程保护和用户可配置的防火墙内核参数配置，它靠着出色的性能、安全性和速度将第二代防火墙远远甩在身后。第三代防火墙的软硬件实现方式较为灵活，但伴随着网络安全与信息安全需求的变化和使用时间的延伸，仍表现出不少问题，比如说：作为基础的操作系统及其内核往往不为管理者所知，由于源码的保密使得安全性无从保证，而通用操作系统供应商通常不对操作系统的安全性负责。

4、第四阶段的防火墙是具有安全系统的防火墙。其本身就是一个操作系统，所以在安全性上比前三阶段的防火墙有质的飞跃。第四代防火墙有两种方法可以获得安全的操作系统。一种是通过许可证获取操作系统源代码；另一种是通过固化操作系统内核来提高可靠性。

### 2.1.3 防火墙的工作原理

包过滤防火墙运行在OSI网络参考模型的第3/4层，使用ACL技术发现数据包的源IP地址、目的IP地址、源端口、目的端口和协议类型。只有满足过滤条件的数据包才会被发送到相应的目的地，其余的数据包将从数据流中丢弃。数据包过滤是一种通用、廉价且有效的安全方法。之所以通用，是因为它处理简单且资源消耗少。

应用代理防火墙运行在OSI网络参考模型的3/4/5/7层，他能通过对所有应用层的信息数据包进行检查，其决策过程也将放入检查的内容，这样网络的安全性就大大提高了。不过相对来说应用代理防火墙的可伸缩性较差，无法快速上手，且占用资源过多。

状态检测防火墙运行在OSI网络参考模型的3/4/5层，这种类型的防火墙能够通过记录数据流的五元组形成一个会话状态，并个根据建立状态连接表中每一个会话状态，实现对整个数据传输的完整控制。这种方法显著提高了防火墙的性能，可以应用于各种网络环境，甚至是规则复杂的大型网络。

## 2.2 下一代防火墙主要功能

### 2.2.1识别和可视性

1、应用识别与控制

（1）应用管理

下一代防火墙内置应用识别库，支持多种应用识别。在配置界面上为用户提供应用列表，并可将应用进行5维度分类，包括按风险等级分类（1-5级威胁度），按商业类别、子类别分类（如媒体类，图片视频子类），按实现技术分类（如P2P），以及按照特征标签分类（如消耗带宽类，传输文件类应用等）。同时支持以上五个维度的任意组合，方便用户详细查询和识别应用。

（2）自定义应用

随时更新的内置应用库已经涵盖当今互联网、企业绝大多数应用，然而如遇特殊需求，下一代防火墙支持应用自定义功能。通过指定应用特征识别码、特征域名、数据包大小、识别起止范围、端口号以及服务模式，用户可定义对特殊应用的识别方法，并可将该应用进行5维度归类，实现对应用特征的标识。

（3）应用过滤器

虽然下一代防火墙已经对应用进行了5维度分类，但在实际环境中，应用程序仍然可以被用户以其他方式进行归类，并在一体化应用配置策略中进行引用。应用过滤器功能就是为满足用户上述需求而产生。用户可先在应用过滤器中根据需求对应用进行多维查询，当确认过滤出的应用正是所需时，即可对此过滤器进行冠名保存。在之后的一体化应用策略配置中，用户可任意选择多个冠名过滤器，设备将会对过滤器中的归类应用，执行一致的识别和控制策略，极大地方便了用户的应用策略管理和使用。

2、用户身份识别

作为下一代防火墙最重要的特性之一，下一代防火墙为在线用户识别提供全面细致的支持。 不同于传统的防火墙策略设置中混入用户认证策略，下一代防火墙将用户认证与复杂的防火墙策略设置分开，创建一个逻辑上更合理、更清晰的视图。

用户可以为每个安全区域创建不同的认证策略，并为每个场景选择不同的识别方案。例如，可从域控服务器直接获取身份信息，与第三方认证服务器（Radius、AD、LDAP）认证，本地账号库认证，证书认证，以及结合以上多种认证方式于一体的多因素认证。

同时，为方便用户理解和使用，下一代防火墙对用户账号进行了集中管理和控制。只需集中配置好账户信息（包括Radius、AD、LDAP、本地数据库、证书账号等）即可在用户认证策略、VPN授权、设备管理员授权等多处便捷使用。

3、日志记录和统计报表

下一代防火墙让用户了解他们当前网络上发生的事情。 具体来说，可以实时掌握当前网络受到何种威胁（入侵攻击、病毒、恶意站点、机密信息等）的攻击、对应的威胁级别和攻击次数。

4、无线热点发现

下一代防火墙可以针对非法热点发现并阻断，加强对移动应用的管理（提高APP应用识别数量和准确度，对APP进行限制和审计以及流量管理等）

同时，用户可实时了解当前网络中一段时间以来各网络接口带宽使用情况，流量排名前十的应用以及流量使用排名前十的用户，并可实时互查应用与用户流量间的使用关系。

除了实时网络状况，下一代防火墙为用户提供按日、按周、按月、按年的安全趋势分析报表以及以往所有的访问控制和安全日志。从而让用户对安全威胁、业务应用、用户流量、网络负载从时间、数量、程度上通过各种形象化图形和数据手段有了高度可视化的跟踪和了解。

### 2.2.2 一体化策略和控制

1、一体化配置策略

基于安全引擎的一体化设计，下一代防火墙在配置界面上为用户提供了较传统防火墙和UTM完全不同的清晰和简洁的管理体验，即一体化配置策略。

一体化配置策略将传统五元组访问控制与具有下一代防火墙特征的用户识别、应用识别控制有机地结合起来，同时对其他防火墙产品一贯分离且重复的安全策略配置方式，进行了高度集中和融合。

在一条策略中即可全部或部分选择：入侵防护、防病毒、URL过滤、内容过滤。免去用户以往在多个不同安全配置页面间频繁切换，重复配置的不便。其结果是在其它防火墙产品上需要配置5、6条策略才能实现的功能，现在在下一代防火墙上，只需要一条策略即可完成，且逻辑上更加清晰简单，便于理解，极大地提高了管理易用性和可维护性，防止了繁琐配置引起的错误风险。

2、流量管理和分析

基于强大细致的用户、应用识别能力，下一代防火墙支持用户以安全区、IP地址（网段）、时间、用户、应用多维度的对流量进行管理和控制，包括限制应用上下行最大带宽、保证应用上下行最小带宽、保证带宽下的优先级排序以及每IP的进行应用流量控制，从而做到合理分配网络带宽，保证重要业务的正常优质运行，限制或防范非法滥用网络资源的应用对流量的过度占用等。

### 2.2.3 应用层防护

1、入侵防护

下一代防火墙内置大量威胁特征库，并将威胁入侵分为5大类，分别是按攻击手段分类（如获取权限、信息收集类），按技术手段分类（如蠕虫、P2P），按流行程度分类（非常流行、中等流行），按危险程度分类，按服务类型分类等（如WWW、FTP事件等）。

下一代防火墙可防护远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等各种网络及应用攻击。同时支持用户自定义规则，建立规则组等功能。并能够对检测到的入侵事件实时告警、阻断、记录和提供统计报表。

2、URL过滤

下一代防火墙具有业界领先的基于云端的URL分类库，内含按照不同类型（如不良言论、色情暴力、网络“钓鱼”、论坛聊天等）划分的超过上亿条记录的URL信息，可实现对工作无关网站、不良信息、高风险网站的准确、高效过滤；

同时下一代防火墙内置的Web信誉库，通过对互联网站点资源（域名、IP地址、URL等）进行威胁分析和信誉评级，将含有恶意代码的网站列入Web信誉库，可有效阻挡用户对挂马等不良信誉网站的有意或无意访问，实现对终端用户的安全保护。

3、防病毒

下一代防火墙采用流模式和启发式文件扫描技术，对利用HTTP、SMTP、POP3、FTP、IM等多种协议进行传播的病毒进行扫描，完成对木马病毒、蠕虫病毒、宏病毒、脚本病毒等的查杀，同时支持多线程迸发控制、深层次压缩文件杀毒、病毒白名单等功能。

此外，下一代防火墙将专业防病毒引擎和多核并行处理技术完美融合，实现高速病毒处理性能。

4、内容过滤

通过内容安全关键字，下一代防火墙可对任意安全区域间交互的网页内容、搜索引擎信息内容、文件传输（文件名、格式、内容）、邮件收发（包括收发人、标题、内容、文件等）、论坛发言、服务器操作、以及即时通信内容等进行基于内容关键字的准确检测、阻断、告警、记录和信息还原，实现深度内容安全管理与跟踪，避免用户机密信息、重要文件通过网络外泄，也避免了非法言论及不良信息的传播。

### 2.2.4 基础特性

下一代防火墙兼容传统防火墙所有功能特性，包括NAT、交换/路由、IPSec/SSL VPN等边界网络特性，A-A/A-S双机热备、软硬件Bypass等高可靠性特性，以及支持虚拟线部署、二/三层/混合/旁路部署等网络部署适应性。

# **第3章 运营商网络安全分析与设计**

## 3.1 方案设计原则

由于本方案的内容涉及多方面，分析应本着多层次、多角度的原则，从理论到实践，从软件到硬件，制定详细的实施方案和策略。避免遗漏。为保证本项目后期的顺利推进和实施，将遵循以下原则：

1、合法性原则。安全体系的建立必须遵循相关法规，不能与现行法规产生任何冲突；

2、实用性原则：系统的安全设计必须与实际需求相匹配，所采取的安全措施必须解决尚未解决的安全问题。

3、整体性原则：安全产品必须能相互配套，并与现有网络与应用软件兼容，从而组成一个完整的信息系统；

4、可靠性和安全性：系统设计要具备较高可靠性和安全性，保证网络故障尽可能小的影响内部业务系统；

5、高扩展性：系统设计所选择的软硬件产品应具有一定的通用性，采用标准的技术、结构、系统组件和用户接口，支持所有流行的网络标准及协议，便于今后网络规模和业务的扩展；

6、先进性原则。安全技术应具有一定的先进性、前瞻性，以实现整个安全体系的相对稳定性；

7、可管理性：保证整个信息系统应具备较高的资源利用率并便于管理和维护。

## 3.2 网络综合防护

### 3.2.1 现状分析

中国移动（湖南）总公司企业内网如图 3.1所示，内部网络按照办公区域不同划分为多个分区，将内网服务器单独分区管理以向公司内网提供相关服务，同时将部分对外服务置于DMZ区域当中。由于企业网络老旧，防火墙设备即将到达报废期。

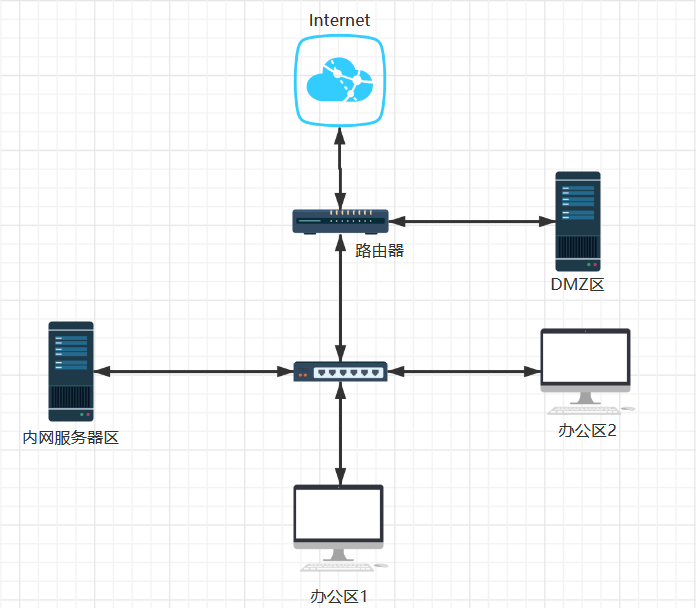


图 3.1 中国移动（湖南）总公司内网网络拓扑简图

### 3.2.2 安全风险分析

3.2.2.1 组网风险

1、网络出口位置的公网IP数量已经远远不能满足当前企业用户的上网需要，经常出现网页连接失败的情况，端口的利用率较低。

2、出口链路有限，但运营商总流量较高，并存在VoIP电话、视频电话等通信业务，但在出口设备上并未对视频或语音通信业务做出足够保证，导致出口链路负载提高时，正常的视频会议将出现延时增大甚至是断线问题。

3、内网服务器和DMZ区缺乏必要的访问控制，区域划分并未进行严格控制，可能导致大量非法访问的出现。

4、网络内部采用动态IP地址分配，可能导致网络内部的安全事件溯源无法进行，同时在策略管理和日志呈现上仅能通过IP地址进行控制，实现起来较为复杂，大大增加了企业的安全管理成本。

3.2.2.2 DMZ风险

DMZ区域需要承担对外提供业务的功能，所以会遭受较多外网攻击。同时由于还要向内网办公区提供一部分服务，所以可能遭受来自内网的威胁。

1、外部恶意攻击

DMZ区域服务器可能面临大量来自Internet的扫描和入侵攻击，黑客可针对服务器情况制定专门的攻击策略，最终控制服务器，以实现黑客的商业目的或其他目的。同时黑客还可通过DDoS攻击对DMZ区域服务器造成冲击，直接中断业务或阻塞业务。这些将对运营商企业造成信息财产和商誉的损失，甚至是政治上的风险。

2、WEB应用威胁

当前DMZ区域主要业务为WEB业务，而在系统安全问题之外，利用WEB应用漏洞进行攻击是当前被黑客利用最多的攻击手段，大量的SQL注入、XSS跨站脚本、网站挂马等动作可能造成关键数据泄露、服务器提权、网站被黑客利用或控制等问题，会对网站本身和网站相关用户造成极大威胁，对商誉和信息资产都有极其不良的影响。

3、内网攻击

DMZ区域本身还承担着为内网提供服务的功能，这就造成内网安全问题可能会扩散到DMZ区域，内网的病毒和木马可能会扩散到DMZ区域进而导致关键信息资产的损毁和泄露。而不加控制的非法访问更是加重了以上问题。

3.2.2.3 办公区风险

内网办公区是企业员工日常办公使用的区域，由于大多数企业员工的安全意识和计算机操作能力一般甚至是薄弱，内网办公区一般是安全问题多发区域。

1、内网病毒泛滥

内网办公人员在日常办公中可能接触到不良网站或挂马网站，这些都将导致员工主机遭受恶意软件或病毒侵入从而成为黑客“肉鸡”，然后通过这些“肉鸡”一步步入侵企业内网。

2、带宽滥用

办公人员可能使用P2P，在线视频等消耗大量，此部分功能将导致公司仅有的出口链路被大量与工作无关的业务占据，此时出口设备上并无专业的流量控制和管理方案将导致正常业务流量无法得到保证，进而影响到正常的办公。

3、违规外联

微博、在线视频、在线游戏、在线炒股、访问非法网站、访问不良网站等操作将对企业员工的工作效率造成不良影响，同时会增加企业面临潜在安全风险的可能。如果不加以限制将导致公司管理成本提高。

4、敏感信息泄露

办公区域内部，员工会在本地使用大量内部使用级、机密级甚至是绝密级文档和企业运营数据，这部分信息是严禁外泄的，但是受限于当前的网络安全管理情况，企业尚无有效手段限制员工外发相关文档，这将导致公司大量信息资产的外泄。

5、违禁内容发送

员工在正常上网当中，可能会在论坛等公共网络场景流量相关内容，此部分可能在不加控制的情况下可能会包括企业内部的一些敏感信息、非法言论内容、代表公司的错误观点、公司员工岗位分配等信息，这些信息将会对公司的运营造成不良影响。

3.2.2.4 内网服务器风险

内网服务器往往存放有公司内部使用级以上的相关数据，对运营商企业极为重要，但同时也是恶意攻击者和利益关注者较为关心的攻击目标，会承受来自多方面的安全威胁。

1、恶意攻击

由于内网服务器内存放有重要企业级数据，所以成为攻击者的主要目标。当攻击者成功控制一台或多台内网办公PC后，会尝试对内网服务器进行渗透，入侵，提权等相关操作，最终实现对重要数据的窃取。

2、非授权访问

企业内部已按照数据的使用部门和文档密级制定相关规范，需要严格控制访问，如果不加以控制，将会造成员工越权访问的情况出现，此时会造成信息不必要的泄露，为信息安全留下隐患。

3、资源滥用

内网服务器区含有对内公开的资源，可以提供给相关员工使用，但是如果对资源的使用不加以限度限制，可能会导致资源滥用，进而占用内网服务器区出口带宽，最终导致正常业务受到影响。

### 3.2.3 需求分析

通过对当前运营商内网现状和安全风险的分析，可以明确企业内部需要使用一定的安全管理和防护手段来保证网络系统的安全可靠运营。

1、访问控制

需要能够对DMZ和内网服务器区的重要业务进行访问控制，防止非授权访问事件的发生。

2、防入侵攻击

能够有效防御入侵攻击，防止来自外网攻击者和内网被控制主机的攻击，保护关键服务器上的信息财产安全。并提供相应的日志记录和告警信息，能够帮助进行攻击行为的审查。

3、恶意软件、病毒防护

能够有效防护内网办公区域不受外网潜在威胁侵害，能够有效识别病毒、木马和恶意软件，同时能够防止内网不同区域间的病毒、蠕虫扩散，将安全威胁控制在一定区域。能够对邮件、HTTP等应用中附带的文件进行扫描，对恶意文件进行屏蔽并做出相应提示。

4、流量控制

能够根据应用和用户信息进行有效的流量控制，包括流量保证，流量整形，流量限速，按事件限制流量等相关功能，从而有效地保护企业网络避免受到某一类流量冲击，保证企业的业务系统能够正常运行。

5、防钓鱼，防恶意站点

当企业员工浏览钓鱼网站，被挂马站点等存在较大安全风险的网站时，需要能够提供相应安全提示或直接进行屏蔽。

6、数据防泄漏

防止企业内部的关键文件外传，能够对内容进行扫描和判断，并且能够通过解压缩动作对压缩文件进行解压扫描。需要屏蔽企业的源代码或设计图纸等文件传输，为企业降低信息资产外泄带来的损失。

7、IP地址数量受限

需要能够在不增加公网IP的情况下，有效缓解当前出口防火墙NAT连接数量受限的问题，保证大部分正常网络访问还能够进行。

8、用户管理

可以与内网用户管理服务器进行对接，能够按照用户名进行相应的策略管理，报表生成。帮助企业管理人员快速地对安全事件进行溯源。

### 3.2.4 解决方案

针对中国移动（湖南）总公司当前的网络现状，建议在企业出口部署下一代防火墙一台，承担网络出口的转发和安全防护等相关工作，在内部服务器区域出口位置部署下一代防火墙一台承担对内部服务器区域的防护工作，如图 3.2所示。

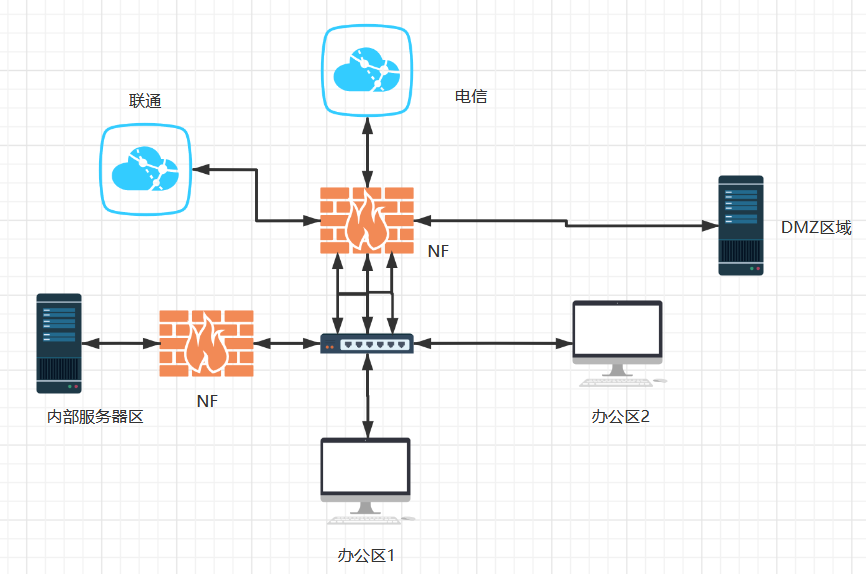


图3.2 中国移动（湖南）总公司内网网络拓扑简图（网综合防护设计）

3.2.4.1 网络出口位置

NF防火墙与核心交换机之间建立多条千兆连接，并开启LACP协议实现链路聚合，通过聚合接口与交换机进行链路转发。同时因为转发接口仅有一个逻辑接口，可以有效控制管理维护成本。

开启NAT相关功能，利用端口复用功能解决当前客户网络连接数量明显受限的问题，开启此功能后可以保证现有的公网IP的端口数量可以被最大限度复用，提高整个网络系统的对外连接数量。

开启应用管理和用户管理功能，并针对当前主要的对外业务和视频会议等对网络条件要求较高的流量设定保证策略。对企业员工设定流量限制策略，防止员工使用P2P、在线视频等应用耗尽企业网络出口带宽。同时配合URL过滤功能针对游戏、社交、在线交易、色情等应用和网站进行限制，保证员工在工作时间可以专心投入工作。

开启IPS，和防病毒功能，为企业内网提供针对入侵、蠕虫、病毒、木马等恶意攻击的防护，并能够识别WEB浏览和邮件业务中出现的恶意文件，为企业内部提供全面的安全防护

针对DMZ区域和企业内网设置严格的防护控制，对来自外部的面向非业务端口的访问进行严格限制，开启相关日志，对越权访问行为进行监控和回溯。并针对不同的内网分区设定差异化的控制策略。

3.2.4.2 内部服务器区域出口位置

防火墙开启用户管理和访问控制功能，针对内网用户不同分区和不同的用户组制定相应的策略限制，对重要的服务器的访问要进行严格控制。

开启IPS、防病毒、内容过滤功能，防护来自办公区域的恶意攻击，控制病毒文件在内网肆意传播，防护APT攻击借助内网用户电脑攻击关键服务器获取企业重要数据。

### 3.2.5 相关防火墙配置

边界防火墙

#基础配置

acl number 3200

rule 5 permit ip source 192.168.88.0 0.0.0.255 description 192.168.1.0 0.0.0.255

#

interface GigabitEthernet0/0/0

undo shutdown

ip binding vpn-instance default

ip address 192.168.0.1 255.255.255.0

alias GE0/METH

#

interface GigabitEthernet1/0/0

undo shutdown

ip address 1.1.1.1 255.255.255.0

service-manage ping permit

ipsec policy map1

#

interface GigabitEthernet1/0/1

undo shutdown

ip address 192.168.88.1 255.255.255.0

#配置安全区域并绑定对应安全接口

firewall zone trust

set priority 85

add interface GigabitEthernet0/0/0

add interface GigabitEthernet1/0/1

#

firewall zone untrust

set priority 5

add interface GigabitEthernet1/0/0

#

firewall zone dmz

set priority 50

#

ip route-static 0.0.0.0 0.0.0.0 1.1.1.2

ip route-static 192.168.1.0 255.255.255.0 1.1.1.2

#入侵防御

profile type ips name profile\_ips\_pc

description profile for intranet users

collect-attack-evidence enable

signature-set name filter1

target client

severity high

protocol HTTP

#

profile type ips name profile\_ips\_server

description profile for intranet servers

collect-attack-evidence enable

signature-set name filter2

target server

severity high

protocol FTP

exception ips-signature-id 74320 action block

#

security-policy

rule name policy\_sec\_1

source-zone trust

destination-zone untrust

source-address 10.3.0.0 24

profile ips profile\_ips\_pc

action permit

rule name policy\_sec\_2

source-zone trust

source-zone untrust

destination-zone dmz

destination-address 10.2.0.0 24

profile ips profile\_ips\_server

action permit

# NAT功能配置

nat address-group addressgroup1 0

mode pat

route enable

section 0 1.1.1.10 1.1.1.15

#

security-policy

rule name policy1

source-zone trust

destination-zone untrust

source-address 10.1.1.0 24

action permit

#

nat-policy

rule name policy\_nat1

source-zone trust

destination-zone untrust

source-address 10.1.1.0 24

action nat address-group addressgroup1

#流量管理

traffic-policy

profile profile\_p2p

bandwidth maximum-bandwidth whole both 30000

bandwidth connection-limit whole both 10000

profile profile\_email

bandwidth guaranteed-bandwidth whole both 60000

rule name policy\_p2p

source-zone trust

destination-zone untrust

application app BT

application app YouKu

action qos profile profile\_p2p

rule name policy\_email

source-zone trust

destination-zone untrust

application app LotusNotes

application app OWA

time-range work\_time

action qos profile profile\_email

#

内网服务器防火墙

#防病毒

profile type av name av\_http\_pop3

description http-pop3

http-detect direction download

undo ftp-detect

undo smtp-detect

undo imap-detect

undo nfs-detect

undo smb-detect

exception application name Netease\_WebMail action allow

exception av-signature-id 50000

profile type av name av\_ftp

description ftp

undo http-detect

ftp-detect direction upload

undo smtp-detect

undo pop3-detect

undo imap-detect

undo nfs-detect

undo smb-detect

#

security-policy

rule name policy\_av\_1

description Intranet-User

source-zone trust

destination-zone untrust

profile av av\_http\_pop3

action permit

rule name policy\_av\_2

description Intranet-Server

source-zone untrust

destination-zone dmz

profile av av\_ftp

action permit

#

## 3.3 网络隔离和访问控制

### 3.3.1 现状分析

中国移动（湖南）总公司企业网络如图 3.3所示，网络当中已经部署有防火墙，开启NAT功能以满足内网大量主机的上网需要，并通过防火墙规划出DMZ分区，在DMZ分区中放置有对外业务服务器。在企业内网分别规划了内部服务器区和办公区。其中办公区域为所有员工使用，内网服务器区主要存放企业重要对内业务服务器。从网络当前状况来看，提供了简单的访问控制并进行了简单的网络规划，但是网络当中仍然存在较大的安全隐患，需要对网络进行改造以提高系统安全性。

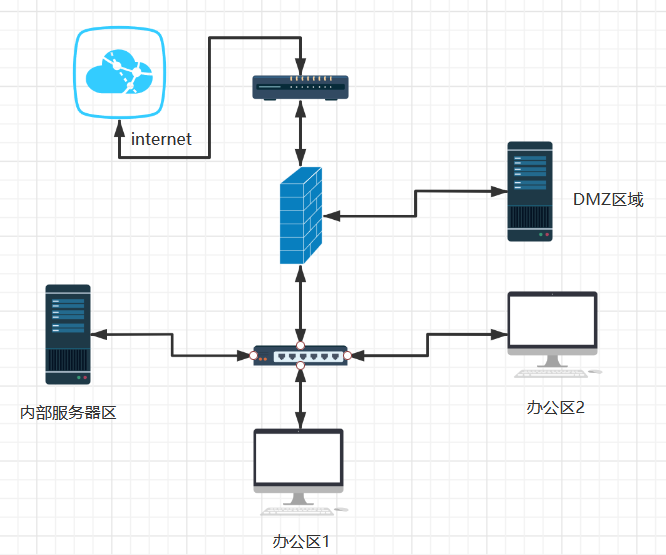


图3.3中国移动（湖南）总公司内网网络拓扑简图（网络隔离和访问控制）

### 3.3.2 安全风险分析

从当前组网来看，风险主要存在于办公区域当中，当前企业内部所有办公用PC主机都划分在同一区域当中，这虽然降低了网络维护成本，但是由于企业内部不同部门岗位所拥有的网络访问权限并不相同，不同部门用户的互联应该受到控制。但是在当前组网情况下，研发同时可以轻松连接财务部门PC主机，从而提高了跨部门重要信息泄露的可能。

而且从整个内网来看缺乏有效的病毒、恶意软件、蠕虫控制机制，攻击者在通过社会工程学或通过强行攻击的手段进入内网之后，可以在内网肆意探测、攻击、扩散，从而为企业带来重大信息安全问题。

### 3.3.3 需求分析

针对当前企业网络当中存在的问题，需要重新按照企业员工部门划分和权限规划出多个办公区域，将不同部门之间的网络进行隔离，同时还要保证各个部门都可以对企业内网共享资源进行访问。

还需要提供相应的防扫描、抗病毒和蠕虫防护机制，对网络中存在的攻击事件进行事先预警，事中防御，事后溯源的操作，保证企业内网不会发生病毒泛滥事件，并能帮助安全管理人员快速定位网络中的被攻击者利用的PC主机。

### 3.3.4 解决方案

为解决前文所述相关问题，建议重新进行网络访问权限设计。如图 3.4所示，不同区域网络共同通过一台NF防火墙进行汇聚，在NF防火墙上设定访问控制策略，严格按照权限限制各个部门之间的互访，和文件的传输。如果区域之间确实存在资源共享需求，在不违反相关规章的情况下可以在内部服务器区划分出单独服务器来实现文件的共享。

为了降低办公区与服务器区之间出现攻击扩散的可能，需要NF防火墙开启防病毒和IPS功能防护内部服务器区，同时开启用户管理功能和日志记录功能，在出现攻击后可以通过日志帮助安全管理人员迅速定位攻击发起者，并通知进行杀毒、还原等相关操作。

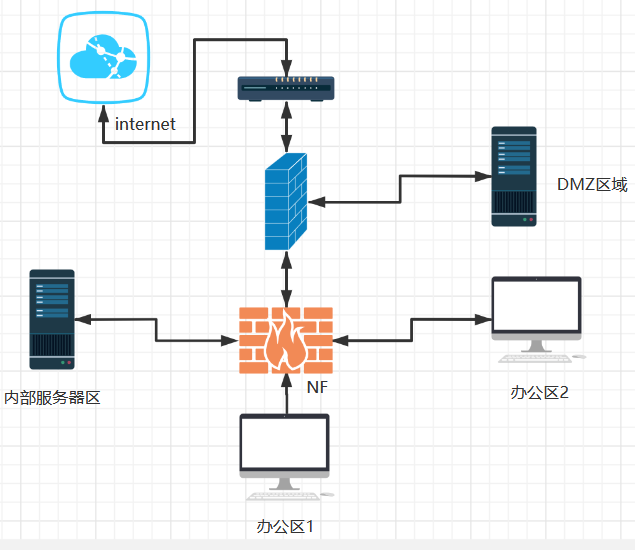


图3.4中国移动（湖南）总公司内网网络拓扑简图（网络隔离与访问控制设计）

### 3.3.5 相关防火墙配置

#ACL访问控制

acl number 3000

rule 5 permit ip source 192.168.88.0 0.0.0.255 description 192.168.1.0 0.0.0.255

#

info-center source default channel 2 log level warning

info-center loghost 10.2.0.10

#

firewall log session log-type syslog

firewall log host 1 10.2.0.10 514

firewall log source 10.2.0.1 6000

#NAT溯源

nat address-group 1

mode pat

status active

section 0 1.1.1.10 1.1.1.12

#

nat-policy

rule name trust\_untrust\_outbound

source-zone trust

destination-zone untrust

source-address 10.3.0.0 mask 255.255.255.0

action nat address-group addressgroup1

#

audit-policy

rule name trust\_untrust\_outbound

source-zone trust

destination-zone Untrust

source-address 10.3.0.0 mask 255.255.255.0

action audit profile profile\_audit

#

snmp-agent

snmp-agent local-engineid 000007DB7FFFFFFF000077D0

snmp-agent sys-info version v3

snmp-agent group v3 v3group privacy

snmp-agent target-host trap address udp-domain 10.2.0.10 params securityname %

$%$Lch\*5Z>Q0:BIj9Nv<&^W(>5,%$%$ v3 privacy private-netmanager

snmp-agent usm-user v3 v3user v3group authentication-mode sha %$%$q:JqX0VlJ,5y

kB"H'lF&kd[REPvIW\_tq`0DkZ\JN)tTE`ja\%$%$ privacy-mode aes128 %$%$.AA`F.dEUJ8Dl33

bz;0PYcZQ">eB&vh6t$]4<QJId/XV^i`[%$%$ 认证密码 Admin@123 加密密码 Admin@1234

snmp-agent trap enable

#

## 3.4分支VPN互联

### 3.5.1 现状分析

目前中国移动（湖南）总公司规模较大，在湖南省14个地级市（包含自治州）建有分支机构，并拥有一套覆盖范围较大的网络体系，其中主要网络节点如图 3. 7所示，各个网络节点通过中国移动网络实现互联。

由于各个地市之间的网络呈现分裂状态，当前尚无有效方式能够使得多个机构之间实现互连，地市子公司通过公司总部对外开放的业务服务器来获取企业运营相关信息。所有传输报文会通过明文格式进行传输。

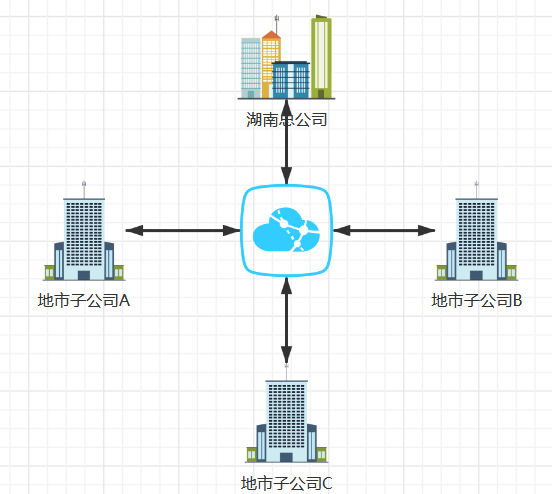


图3.7 中国移动湖南省主要网络节点简图

### 3.5.2 安全风险分析

相互分裂的组网情况将极大地降低企业运作效率，虽然通过开放部分企业服务可以向地市子公司提供部分企业信息，但同时会带来大量安全隐患。比如开放公司总部出口的访问控制权限后可能导致不受限制的外网访问，这将为攻击者提供便利条件。而企业业务数据在公网内使用明文传输将会带来数据泄密，被篡改的风险。

### 3.5.3 需求分析

由于业务发展需要并受网络发展影响，中国移动（湖南）总公司急需一套VPN系统来建立覆盖全省的内网系统。为完成此系统建设，需要满足以下需求。

需要多台防火墙设备能够支持IPSec VPN，通过设备之间建立的三层隧道加密传输网络流量，并提供完善的校验机制。

需要支持IKE密钥协商协议，使用DH密钥协商算法充分保证加密秘钥的不可猜测。需要支持3DES、AES128、AES192、AES256等加密算法和MD5、SHA2校验算法，充分保证系统的机密性和完整性。同时提供PSK预共享密钥和证书验证算法充分保证隧道两端的授权性和不可抵赖性。

要能够提供防重放攻击能力，能够对复制或伪造的加密报文进行识别和丢弃，能够针对恶意协商做到有效控制。

在企业总部需要提供必要的冗余机制增加整个系统的可靠性，能够在单一设备故障后保证企业网络不会出现瘫痪的风险。

### 3.5.4 解决方案

针对当前网络状态和具体需求，建议在全省各个地市子公司部署下一代防火墙承担IPSec VPN互联工作。

网络总体规划和隧道设计如图 3. 8所示，总部使用NF防火墙作为隧道组网和核心节点，各地市子公司均通过IPSec与总部NF防火墙进行对接。三层隧道建立后，在各个VPN网关设备及相连网络设备上设置静态路由，使得不同网络之间可以实现三层转发上的互通。

在IKE proposal和IPSec proposal方面，建议使用AES 256加密算法、SHA2校验算法、预共享密钥验证方式、DH-1 group密钥协商算法。如此配置可以满足系统机密性、完整性、授权性、不可抵赖性的需要。

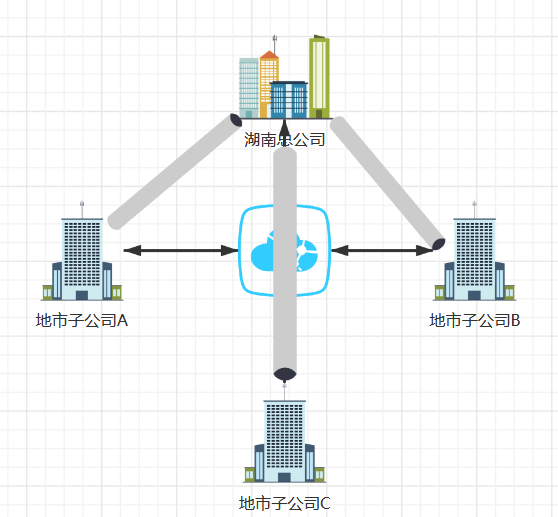


图3.8 中国移动湖南省分支VPN互联设计

在详细部署方面，建议在企业总部使用图 3. 9方式进行组网设计，使用两台NF防火墙旁路接入企业总部出口路由器，两台NF防火墙呈双机主备工作状态，两台设备间通过多条千兆链路捆绑形成高可靠心跳线。在两台设备出接口使用子接口划分公网和内网区域，分别开启VRRP功能，并在路由器之间以及路由器和防火墙之间打通二层转发通路，保证VRRP报文可以正常转发。在公网VRRP虚接口上配置公网IP，作为IKE协商和IPSec隧道IP地址，在私网VRRP虚接口上配置内网IP，承担明文转发工作。在路由器上起三层交换虚接口承担流量三层转发功能。

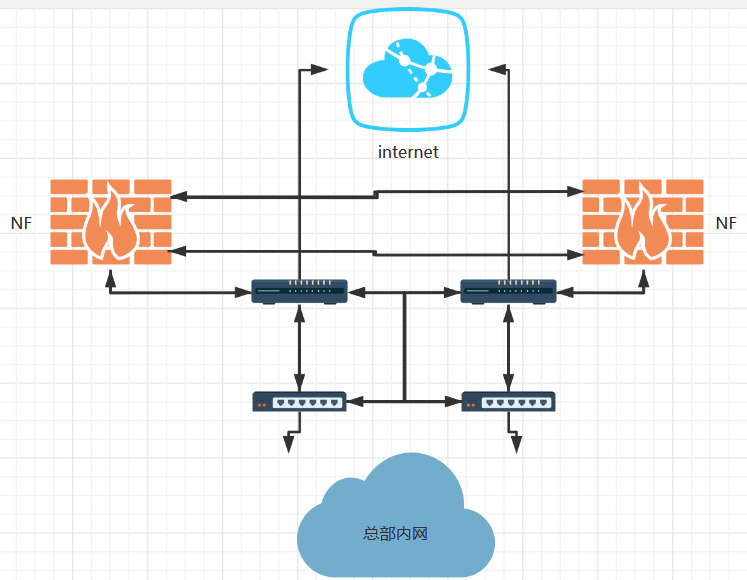


图3.9 中国移动（湖南）总部VPN互联组网设计

在分支机构，由于网络规模较小，并未使用双机组网方式，此时可以使用单台NF防火墙旁路部署于出口设备处，配置公网和私网两个子接口，使用公网接口对外建立IPSec隧道，使用私网接口对内转发明文报文。组网如图 3. 10所示。

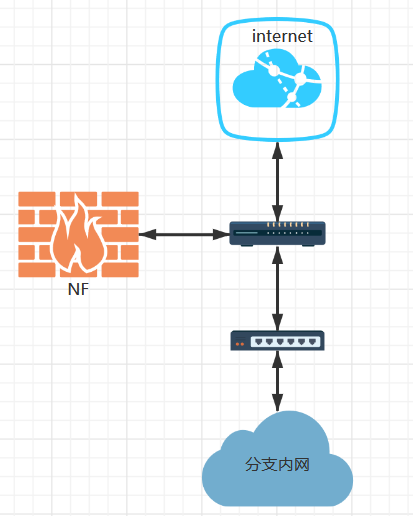


图3.10 中国移动（湖南）地市子公司VPN互联组网设计

### 3.5.5 相关防火墙配置

总部防火墙VPN网关配置

#

ike proposal 10

encryption-algorithm aes-256

dh group2

authentication-algorithm sha2-256

authentication-method pre-share

integrity-algorithm hmac-sha2-256

prf hmac-sha2-256

#

ike peer b

ike-proposal 10

remote-address 2.2.2.2

pre-shared-key %$%$SP!UWlu=$B7`~B!@iRn+jvmd%$%$ 预共享密钥 Test!1234

#

ipsec proposal tran1

esp authentication-algorithm sha2-256

esp encryption-algorithm aes-256

#

ipsec policy map1 10 isakmp

security acl 3000

ike-peer b

proposal tran1

#

ipsec policy map2 10 isakmp

security acl 3001

ike-peer b

proposal tran1

地市子公司防火墙VPN网关配置

#

ike proposal 10

encryption-algorithm aes-256

dh group2

authentication-algorithm sha2-256

authentication-method pre-share

integrity-algorithm hmac-sha2-256

prf hmac-sha2-256

#

ike peer a1

ike-proposal 10

remote-address 1.1.3.1

pre-shared-key %$%$SP!UWlu=$B7`~B!@iRn+jvmd%$%$ 预共享密钥 Test!1234

#

ike peer a2

ike-proposal 10

remote-address 1.1.4.1

pre-shared-key %$%$SP!UWlu=$B7`~B!@iRn+jvmd%$%$

#

ipsec proposal tran1

esp authentication-algorithm sha2-256

esp encryption-algorithm aes-256

#

ipsec policy map1 10 isakmp

security acl 3000

proposal tran1

ike-peer a1

#

ipsec policy map2 10 isakmp

security acl 3001

proposal tran1

ike-peer a2

#

interface tunnel 1

ip address unnumbered interface GigabitEthernet1/0/1

tunnel-protocol ipsec

ipsec policy map1

interface tunnel 2

ip address unnumbered interface GigabitEthernet1/0/1

tunnel-protocol ipsec

ipsec policy map2

#

## 3.5 安全防护加固

### 3.6.1 现状分析

中国移动（湖南）总公司企业内网如图 3. 11所示，内部网络按照办公区域不同划分为多个分区，将内网服务器单独分区管理以向公司内网提供相关服务，同时将部分对外服务置于DMZ区域当中。网络出口位置部署有一台防火墙设备，主要承担访问控制及NAT功能。

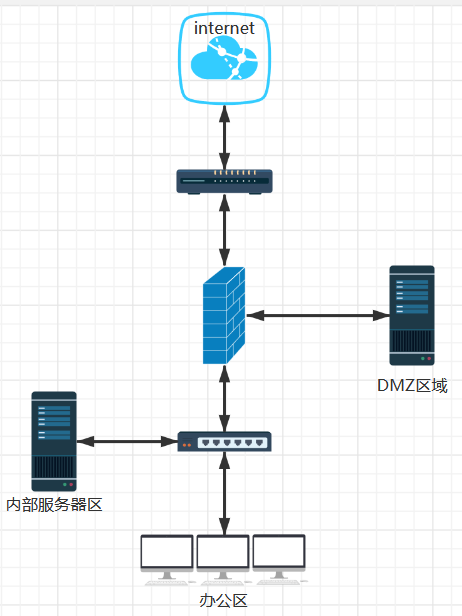


图3.11 中国移动（湖南）总公司内网网络拓扑图（安全防护加固）

### 3.6.2 安全风险分析

1、当前企业网络虽然部署有传统防火墙，对从外网至内网及DMZ区域的访问行为作出了一定的限制，但是由于内网办公区域存在大量地向外网的网络访问需求，这势必导致大量的办公主机会在网络访问当中面临众多安全威胁。

（1）遭遇恶意站点

在员工进行互联网访问的过程中，或多或少会进入部分遭到黑客攻击利用的站点，此时很有可能感染病毒、木马等恶意程序，导致主机被控制。而且当前APT攻击盛行，企业内部关键人员很有可能受到有目的性的攻击，需要额外注意。

（2）收到邮件攻击

企业邮箱对外公开，很有可能收到来自外网的不明邮件，此时如果员工安全意识薄弱，点击附带有恶意软件的邮件附件或按照邮件指导连接到恶意站点，就很有可能被攻击者攻陷，进而导致攻击者进入内网。

2、同时，办公人员的上网行为还有可能降低企业办公效率，影响网络正常转发，为企业运营增加法务风险。这些上网行为主要包括：

（1）带宽滥用

办公人员可能使用P2P，在线视频等消耗大量，此部分功能将导致公司仅有的出口链路被大量与工作无关的业务占据，此时出口设备上并无专业的流量控制和管理方案将导致正常业务流量无法得到保证，进而影响到正常的办公。

（2）违规外联

微博、在线视频、在线游戏、在线炒股、访问非法网站、访问不良网站等操作将对企业员工的工作效率造成不良影响，同时会增加企业面临潜在安全风险的可能。此时如果不加以限制将提高公司的管理成本。

（3）敏感信息泄露

办公区域内部，员工会在本地使用大量内部使用级、机密级甚至是绝密级文档和企业运营数据，这部分信息是严禁外泄的，但是受限于当前的网络安全管理情况，企业尚无有效手段限制员工外发相关文档，这将导致公司大量信息资产的外泄。

（4）违禁内容发送

员工在正常上网当中，可能会在论坛等公共网络场景流量相关内容，此部分可能在不加控制的情况下可能会包括企业内部的一些敏感信息、非法言论内容、代表公司的错误观点、公司员工岗位分配等信息，这些信息将会对公司的运营造成不良影响。

### 3.6.3 需求分析

从当前网络情况来看，由于有防火墙的存在，可以对外部的非授权访问做到较好的屏蔽，但是当前防火墙功能单一，缺乏对外进行IPS和防病毒防护功能，这将导致外网的恶意攻击可以轻易进入内网，对企业信息财产造成损害。所以企业当前需要增加安全防护设备来对外部攻击进行有效防护。而且大量员工上网行为对网络的正常工作产生了一定冲击，所以需要应用安全类设备对当前网络中的多种应用流量和上网行为作出有效管控，保证企业的正常运作。具体需求如下：

1、防入侵攻击

能够有效防御入侵攻击，防止来自外网攻击者和内网被控制主机的攻击，保护关键服务器上的信息财产安全。并提供相应的日志记录和告警信息，能够帮助进行攻击行为的审查。

2、恶意软件防护

能够有效防护内网办公区域不受外网潜在威胁侵害，能够有效识别病毒、木马和恶意软件，同时能够防止内网不同区域间的病毒、蠕虫扩散，将安全威胁控制在一定区域。能够对邮件、HTTP等应用中附带的文件进行扫描，对恶意文件进行屏蔽并做出相应提示。

3、URL、内容过滤

有效控制企业内网办公区向外网发送非法言论，防止包含公司机密内容的相关留言信息出现在论坛等公开系统。同时能够防止员工浏览包含非法或不良网站的相关内容。

4、防钓鱼，防恶意站点

当企业员工浏览钓鱼网站，被挂马站点等存在较大安全风险的网站时，需要能够提供相应安全提示或直接进行屏蔽。

5、应用管理

能够根据流量数据有效识别网络应用，可以针对应用制定限制，屏蔽，放行等相关操作，并可以根据应用流量信息生成详细报表，帮助企业管理人员审视网络健康状况，为网络流量优化提供相关建议。

### 3.6.4 解决方案

结合企业当前网络状况和具体需求，建议在企业防火墙和核心交换机间增加下一代防火墙设备，以提供对内网的防护和管控功能。如图 3. 12所示。

为减少对网络的改造并提高网络可靠性，建议将NF防火墙以虚拟线模式接入网络当中，按此设计无需改动原有组网的地址规划，同时在设备故障或电源意外中断的情况下可以直接提供内置Bypass能力，保障网络无故障运行。

开启IPS功能和防病毒功能，对外网发起的恶意扫描、渗透攻击、木马、蠕虫、恶意软件等攻击可以进行有效防护。

开启URL过滤和WEB信誉功能，对员工网页浏览行为作出限制，将上网行为控制在公司规章制度允许的范围内，同时屏蔽可能存在安全风险的站点。

开启应用管理和流量控制功能，对每个员工的流量做出限制，并对P2P流量、在线游戏、在线视频流量（如优酷等）制定阻断策略，为视频会议等应用制定流量保证策略。

按照公司规章设定内容关键字，控制企业员工对外传输可能对公司财产或信誉造成损害的信息，严格控制网页流量、文件传输、电子邮件、网络论坛等网络访问形式传播公司机密文件。

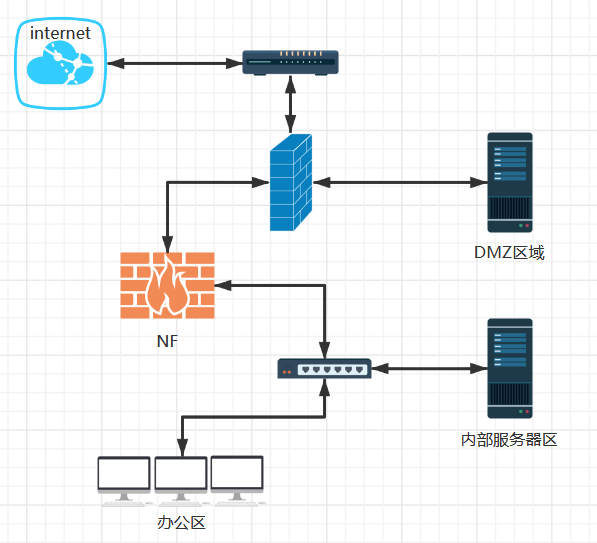


图3.12 中国移动（湖南）总公司内网网络拓扑图（安全防护加固设计）

### 3.6.5 相关防火墙配置

#防病毒保护

profile type av name av\_http\_pop3

description http-pop3

http-detect direction download

undo ftp-detect

undo smtp-detect

undo imap-detect

undo nfs-detect

undo smb-detect

exception application name Netease\_WebMail action allow

exception av-signature-id 50000

profile type av name av\_ftp

description ftp

undo http-detect

ftp-detect direction upload

undo smtp-detect

undo pop3-detect

undo imap-detect

undo nfs-detect

undo smb-detect

#

security-policy

rule name policy\_av\_1

description Intranet-User

source-zone trust

destination-zone untrust

profile av av\_http\_pop3

action permit

rule name policy\_av\_2

description Intranet-Server

source-zone untrust

destination-zone dmz

profile av av\_ftp

action permit

#应用管理、流量限制

traffic-policy

profile profile\_p2p

bandwidth maximum-bandwidth whole both 30000

bandwidth connection-limit whole both 10000

profile profile\_email

bandwidth guaranteed-bandwidth whole both 60000

rule name policy\_p2p

source-zone trust

destination-zone untrust

application app BT

application app YouKu

action qos profile profile\_p2p

rule name policy\_email

source-zone trust

destination-zone untrust

application app LotusNotes

application app OWA

time-range work\_time

action qos profile profile\_email

#

# **总 结**

党和国家领导人一贯高度重视网络和信息安全。习近平总书记2014年2月27日下午主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话。他强调：“没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国”。

信息化时代的背景下，网络的安全对于企业来说至关重要，信息资源的数据得到安全保障才可以保证企业顺利运行和参与企业竞争。企业网络需要加强防火墙安全系统的建设，搭建一个稳定、安全的网络环境，维护企业信息和数据安全，提高企业的市场竞争力。

企业网络安全防护的发展越来越依赖防火墙，可以说是信息安全领域最成熟的产品之一。日益增长的安全要求对信息安全产品提出了更高的要求。 未来，防火墙产品可能会因为功能的扩展、应用的日益丰富以及流量的复杂性的增加而呈现出更加严格的处理要求。

很多防火墙技术都在不断革新，除了对既有的基础功能上做出增加，还在反向追踪、反向定位、逆向侵袭等方面作出努力，既要保障企业网络安全防护的进步，又要在源头上对威胁彻底解决。防火墙技术是比较灵活的技术手段，单一层面的防火墙建立在防护内容上比较少，所以对企业网络安全防护的考虑，大部分情况下是使用多层防火墙来完成的，尽量让防火墙的功能进一步健全，由此在各类问题的集中解决方面能够取得更好的成绩，在企业网络安全防护的可靠性、可行性方面也可以得到不错的成果。