企业网络信息安全系统方案

前言

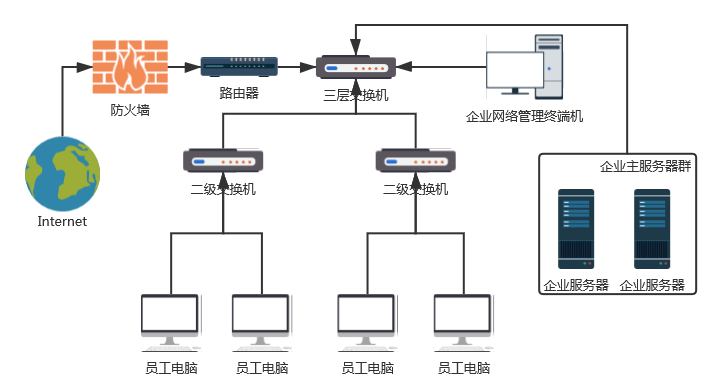
随着计算机技术的飞速发展，在计算机上处理的业务也由基于单机的任务发展成为基于局域网或互联网的企业级信息共享与处理和全球范围内的信息系统。在计算机从网络世界获得诸多受益的同时，网络安全问题也逐渐突出。为了能够更加高效且安全地使用计算机网络，我们需要结合实际的生产需求，完善和优化企业内部的网络结构，构建更加安全的数据保护系统，同时建立稳定的容灾体系，然后建立防火墙和一系列防入侵方案，来进一步提高企业网络系统的安全性，从而达到提高网络效率、稳定保护企业内部数据的目的。

1. 优化企业内部的网络结构

在设计企业内部的总体网络结构时，应当综合企业规模、性能需求、资金预算等多方面的因素，同时还要考虑网络结构的可维护性和可扩展性。由于该企业规模大于10w人，所以在建立总体的网络模型时应当首要考虑的就是网络的性能和稳定性。对于传统的二层交换技术的网络架构，在只有数百台工作站的情况下，性能表现较为理想，但是当网络规模增大到上千台时，这种网络结构的性能劣势就被体现出来了，同时，在大规模的网络中，这种网络结构的稳定性也会大大下降。所以对于该企业，在网络结构的总体设计上应当采用三层交换技术，即“二层交换技术+路由转发”，这种网络结构既能够大幅提高网络的性能，同时也能提供较高的稳定性。

如下为三层交换结构的网络结构图。

在该网络结构中，通过企业内部总防火墙和总路由器来和外部互联网进行连通，然后经由三层交换机和二层交换机将网络分发给各个员工的工作机。在网络中，企业内部的服务器和三层交换机连通，通过三层交换机将企业内部的服务分发到员工的工作机上，同时，使用企业网络管理终端机与三层交换机进行直连，使其拥有对整个网络的管理权限。



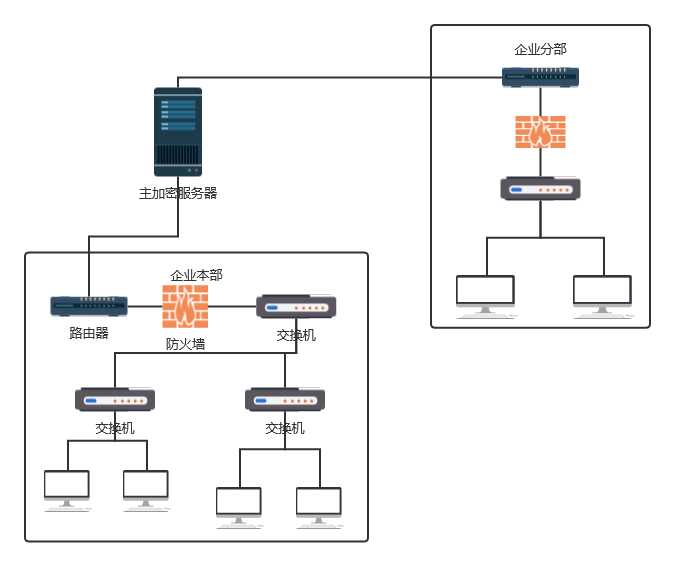
企业内部网络拓扑总计结构

1. 企业分部网络结构

考虑到该企业存在异地分支机构，且要求能够进行远程的内部事务处理，所以应当设计企业分部和企业本部进行网络通信的结构，同时还应当兼顾到企业内部事务的保密需求。

如下为企业分部网络结构设计。

在该网络结构中，主加密服务器架设在互联网上，该服务器能够接收来自企业分部的请求并将请求加密后转发给企业本部，反之亦然。



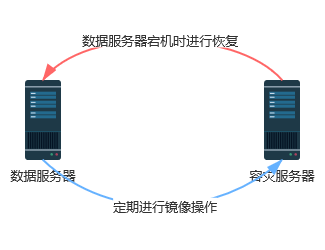
企业分部网络结构

1. 企业内部容灾结构

因为要求企业能够具有高可用性，所以应当在设计网络结构时考虑企业服务的容灾性。

如下为企业内部数据服务器的容灾架构。

在该网络结构中，为每一台企业内部数据服务器配备一台容灾服务器，该容灾服务器定时对数据服务器上的数据进行镜像备份，当数据服务器宕机时，使用容灾服务器上的镜像对数据服务器进行恢复。



企业内部数据容灾结构

对于企业内部的其他服务器，采用集群的方式进行部署，即每一个服务都部署在多台服务器上，然后经由一个反向代理服务器对外提供服务接口。在反向代理服务器上配置负载均衡策略，一方面能够提高整体网络的性能，另一方面又能够提高网络的容灾能力。

1. 企业内部数据的保密处理

为了防止企业内部数据被员工拷出或者通过mail发送而泄漏，应当在网络内部设计防护机制。在文档保密的安全机制中，使用文件的加密和解密系统，将企业内部涉密文件进行加密处理，同时设置权限系统，给不同的企业用户分配不同的权限，只有拥有对应权限的用户得到文件后才能进行文件的解密操作。同时设置文件的审计系统，即将用户对文件的操作进行记录，方便日后审查和追溯。

1. 企业员工行为管理

为了满足对企业员工的行为监控和限制，采用限制终端带宽的方式。带宽的限制可在交换机和路由器上进行设置，首先对ip进行分段，将这些分段的ip按照不同的用户类别进行分配，然后通过设置对这些分段的ip分配不同的带宽，从而到达限制用户带宽的目的。对于限制员工工作时间聊天、打游戏和看电影的需求，可采用在防火墙设置可访问域名的方式来实现，例如只对新闻部门开放新闻类域名的访问权限，将对其他域名的请求作为非法请求进行拦截。