解决方案：电信行业混合型病毒和垃圾邮件解决方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/227/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_227206.htm 从“ 主动防御、主动反应 ”这一观点出发，协助运营商建立适用电信业务、可伸缩、抗打击的防病毒网络。 各种信息技术的不断发展为电信运营商带来了广阔的商机，同时也带来了新的威胁和新的风险。在传统电信网络上，大多数网络捆绑单一业务： 电话网提供电话业务以及部分补充业务； DDN 网络提供点到点数据专线业务； 帧中继网络提供数据专线以及虚拟专用网业务； 同步网提供网络同步服务； 信令网为电话网提供信令服务； 即使是号称多媒体网络的ATM 也基本用作数据专线以及虚拟专用网。大多数用户终端智能性较低并且与网络信令隔离，因此一般不会影响网络安全。 然而随着新业务的出现和基础带宽的不断提高，新兴运营商已不满足于每个业务建一张网的思路： 网络不但需要承载多种业务，还必须在用户使用同一个接入线路的条件下提供多种业务。为此，网络为识别统一接入线路上的多种业务，不可避免地将部分智能性转移到终端，IP 网络成为承载多业务网络的重要选择。恶意用户可以使用计算机系统干扰业务流程，甚至发起黑客攻击使网络瘫痪，这样的模式严重影响了IP 网络安全。由于当前分组语音的大量使用，IP 网络需要与传统电话网络互通，IP 网络的安全隐患进而会影响传统电话网络的安全。 电信业安全威胁分析 作为基础网络提供商的电信企业，影响最大、威胁最大的风险就是那些消耗基础带宽、影响网络性能的威胁，主要包括混合型威胁和各种垃圾邮件。 现在互联网面临的威胁

已经由传统的病毒威胁转化为现在的包括了蠕虫、木马和恶意代码等与传统病毒截然不同的新类型。这些新类型的威胁被业界称为混合型威胁。混合型威胁整合了病毒传播和黑客攻击的技术，以多种方式进行传播和攻击。不需要人工干预，能够自动发现和利用系统漏洞，并自动对有系统漏洞的计算机进行传播和攻击。同时，混合型威胁传播速度极快，通常在几个小时甚至几分钟就可以导致整个网络瘫痪。攻击程序的破坏性更强，受感染的系统通常伴随着木马程序种植除了破坏被感染的机器，在传播过程中会形成DDoS攻击，阻塞网络。混合型威胁正是近几年电信行业所面临的主要威胁。而垃圾邮件则泛指未经请求而发送的电子邮件，如未经发件人请求而发送的商业广告或非法的电子邮件，甚至一些不存在的产品和服务。垃圾邮件是某些想利用 Internet致富的人藉以散播广告或色情的媒介，传送邮件者只需极少的花费，即可造成收件者严重的损失： CPU及服务器硬盘、终端机用户硬盘都极有可能因垃圾邮件影响速度和空间 ； 除了使网络陷入动弹不得的境地外，更令人忧心的便是其夹带的病毒，将同时危害企业网络。 方案介绍 赛门铁克安全方案借鉴最新的安全思想，从 “ 主动防御、主动反应 ” 这一观点出发，协助运营商建立适用电信业务、可伸缩、抗打击的防病毒网络。相对于被动式病毒响应技术而言，主动式反应技术可在最新的混合型威胁没有出现之前就形成防御墙，静侯威胁的到来而避免威胁带来的损失。 通用漏洞利用阻截技术 通用漏洞利用阻截技术的思想是： 正如只有形状正确的钥匙才能打开锁一样，只有 “ 形状 ” 相符的混合型病毒才能利用该漏洞进行攻击。如果对一把锁的内部锁齿进行研究，便可以立即了解

到能够打开这把锁的钥匙必需具备的特征甚至不需要查看实际的钥匙。类似地，当新漏洞发布时，研究人员可以总结该漏洞的“ 形状 ”特征，也就是说，可以描述经过网络到达漏洞计算机并利用该漏洞实施入侵的数据的特征。对照该“ 形状 ”特征，就可以检测并阻截具有该明显“ 形状 ”的任何攻击（例如蠕虫）。 行为阻截技术 行为阻截的思想就是： 在系统中实时监控各种程序行为，一旦出现与预定的恶意行为相同的行为就立即进行阻截。使用了带行为阻截技术的赛门铁克防病毒软件之后，防病毒软件将监视计算机上的所有外发电子邮件。每当发送电子邮件时，防病毒软件都要检查该邮件是否有附件。如果该电子邮件有附件，则将对附件进行解码，并将其代码与计算机中启动此次电子邮件传输的应用程序相比较。常见的电子邮件程序，如 Outlook，可以发送文件附件，但绝不会在邮件中附加一份自身程序的可执行文件副本。只有蠕虫才会在电子邮件中发送自己的副本。因此，如果检测到电子邮件附件与计算机上的发送程序非常相似时，防病毒软件将终止此次传输，从而中断蠕虫的生命周期。 多层过滤反垃圾邮件技术 没有一种技术能完全彻底地解决垃圾邮件问题，赛门铁克通过采用全面的、多层级的过滤技术来防御垃圾邮件。通过为电信运营商设计智能、多层的混合型威胁和垃圾邮件防护架构，优化全系统内混合型威胁和垃圾邮件事件的全面监控、及早发现、及时通报、快速处理等环节，缩短响应时间，有效降低病毒可能造成的损失。建立多层、分布式的混合威胁和垃圾邮件防御架构既与电信运营商现有行政管理模式相匹配（总部指导省公司，省公司指导下级公司），有效提高管理效率，同时又能体现“ 统一规划，

分级管理”的思想，让各省级单位分担总部，地市级单位分担省公司的运行维护负担。 功能逻辑 图中英文缩写分别表示如下产品：SESA-Symantec Enterprise Security Architecture、SSC-Symantec System Center、SCS-Symantec Client Security、SNS-Symantec Network Security Appliance 图 推荐产品在电信运营商混合威胁和垃圾邮件防护体系中功能逻辑图 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com