解决方案：电信网络安全，从内到外的解决方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/233/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_233018.htm 近年来，随着中国电信行业的快速发展，以“ 用户至上，用心服务 ”为核心的服务理念逐渐深入到电信运营商内部的服务系统中。建设安全、高效、快捷的信息系统，是目前国内电信运营商信息化建设的重要目标。 作为电信行业信息化建设具有代表性的电信运营商，其自身的信息化建设已经走在全国的前列。目前各大运营商都已经建设有OA、ERP等信息系统，并在此基础上开发部署了统一的电信信息管理系统。下属各市县的OA和ERP等通过该平台统一进行管理和操作，改善了各地的信息系统不集中、分散管理等问题，并为今后的业务扩展提供了统一的扩展接口。 随着统一的电信信息管理系统的不断丰富，使用人数的不断增加，迫切需要对电信的信息管理系统进行有效管理。从另一个角度来说，由于电信业对整个社会的发展影响是至关重要的，保护整个电信网络信息管理平台的安全，成为不容怠慢的一项重要使命。 电信安全应用，势在必行！ 目前网络安全形势越来越严重，网络攻击的手段也越来越多，如基于网络传播的病毒、蠕虫，含有恶意代码的网页，以及日益严重的间谍软件等。传统的解决方式在面对这些新的安全威胁已经显的力不从心。各种入侵和攻击开始从原来的针对TCP/IP协议本身的漏洞攻击，转向针对特点系统和应用漏洞的攻击，传统的单一防火墙无法抵御。因而，作为国内网络重中之重的电信网络，需要一种新的有效安全管理方式来面对新的安全威胁。电信网络安全管理和应用，

势在必行！针对应用系统众多、人员管理复杂等电信网络的特点，深信服科技推出的电信级UTM网络安全－SINFOR M5400-AC安全网关，针对电信网络的特点，从内网安全管理，到外部安全防范以及远程接入安全访问等多种角度，进行统一管理和部署，保证了电信网络和各种核心信息资源的安全性。 安全管理分内外 一、 内部安全管理： 对拥有众多内网用户的电信网络而言，对内网用户实行严格的安全认证管理以避免安全隐患是及其重要的。深信服科技的UTM 安全网关基于Web的用户认证功能，使得管理员对上网用户的管理变得十分灵活方便。用户启用了Web认证功能以后，除了对客户端的本地身份（如：用户名密码认证，LDAP，RADIUS等认证）进行常规性认证以外，还将启用Web认证。当客户端在浏览器中输入任意网址时，SINFOR M5400-AC会要求用户输入用户名和密码进行认证。只有当用户输入了正确的帐号，该用户才能够访问Internet.用户帐号、Web认证、IP MAC地址绑定等多种认证方式灵活绑定，更为方便地对电信网络众多的内网用户进行有效管理。 为保证电信网络内部员工合理使用Internet资源，防止用户访问不安全的网络站点，深信服科技的电信级UTM安全网关－SINFOR M5400-AC提供了完善的访问控制功能。通过合理设置访问权限和URL过滤规则，杜绝了电信网络内部员工对不良网站和危险资源的访问，防止了木马、病毒、间谍软件等对电信网络带来的安全风险。通过深度内容检测技术，M5400-AC能及时封堵QQ、MSN、BT等P2P软件，并且能够针对MSN或者QQ中所传送的文件进行扫描，有效防止电信网络内网用户对Internet资源的滥用。同时，深信服科技电信级UTM安全网关M5400-AC独特的

敏感内容拦截和安全审计功能更为防止重要信息泄漏提供了最有效的保证。 目前电子邮件已经成为人们最重要沟的方式。电信内部大量的信息都通过电子邮件方式发送到外部，也极可能成为泄漏电信网络重要信息的途径之一。SINFOR M5400-AC安全网关独创的邮件延迟审计功能，可以对经由M5400-AC的所有邮件进行延迟审计。对于从电信网络内部向外发送的邮件，M5400-AC安全网关会对其进行延迟缓存，只有等待管理员审计后才能发出，确保了电信信息资产不外泄，保证了电信网络的信息安全。 二、外部安全防御 SINFOR M5400-AC集成了全球领先的防病毒厂商“ F-PROT ”的杀毒引擎。可以有效地对所有电信网络内部用户接收的邮件和下载的文件进行病毒过滤，大大降低了电信网络内部机器感染病毒的风险。 同时，SINFOR M5400-AC强大的杀毒功能支持HTTP、SMTP、POP3、FTP、NETBIOS等多种协议的数据流，不仅可以查杀普通病毒邮件，还可以检查出各种压缩包（zip，rar，gzip等）内部隐藏的病毒。面对层出不穷、千变万化的病毒，SINFOR M5400-AC防病毒功能所使用的病毒库，可自定义每天在线升级，有效地保护电信网络免受病毒侵袭，把病毒阻挡在电信网络之外。 电信网络的信息资产是不言而喻的，因而也成为了众多黑客的攻击目标，如何有效防止来自外网的攻击？SINFOR M5400-AC集成了高效的IPS（入侵防御系统）系统，有效识别和抵御20，000多种攻击，更大范围的保护了电信网络连接到Internet的安全。 伴随着日益严重的垃圾邮件，SINFOR M5400-AC采用了关键字和权重、智能应答确认技术、黑白名单过滤、指纹识别、RBL等反垃圾邮件技术保证了电信网络免受垃圾邮件的侵扰。 因而，

深信服科技针对电信网络内部安全管理和外部安全防范等角度，构建起符合电信运营商自身需求和特色的安全管理平台，如图1.1所示： 移动办公安全接入 目前，电信企业自身应用环境纷乱复杂，既有内部的应用如：内部OA系统、文件共享、Email等应用服务，又有众多面向电信增值应用商、合作伙伴、VIP客户等对外的应用。如何地有效解决远程用户安全访问电信网络内部资源？深信服科技的移动办公解决方案，是电信移动用户远程访问的一种最佳方案。 深信服科技的移动办公方案最大的特点是在一台设备内同时提供两套VPN系统，完美地解决了单一VPN系统存在的缺点。移动用户在便捷地实现远程接入的同时，更安全地保证了数据在公网上的传输。 因而，电信众多的移动用户通过深信服科技的移动办公解决方案，在选择安全的接入方式时，可选择IPSEC VPN的方式接入电信网络的内部资源，也可以利用SSL的易用性，无需安装客户端即可实现安全接入。 传统的IPSEC VPN需要在客户端进行复杂的配置，深信服科技的移动办公解决方案，集成了先进的DKEY技术，可以将移动用户的安全策略存储在类似U盘的USB Key（又名DKEY）中。这样移动用户随身携带标识自己身份和存储了对应安全策略配置信息的DKEY，可以在任何一台电脑安全的接入到总部。对于使用IPSEC VPN的移动客户端，安装好客户端软件后，只需要插入DKEY，输入自己的密码就可以完成接入，完美解决了IPSEC VPN客户端配置难的问题，实现了IPSEC VPN的零配置，如同使用银行取款机一样安全方便。 而相比IPSEC VPN，SSL VPN的最大优势就在于无需安全客户端。对于电信移动办公人员，只要通过标准的浏览器，包括智能手机、PDA终端等，就可以

通过SSL VPN远程访问电信信息管理系统，极大地提高了电信运营商的工作效率。由于工作在应用层，SSL VPN更容易提供细致的访问权限控制，可以为每一个移动用户提供不同的访问权限，预先设置用户所能够访问的资源。SSL VPN移动用户也可以使用USB DKEY技术进行身份认证。一个KEY，可同时支持两套VPN系统。 深信服科技的移动办公解决方案，为电信的远程接入提供了多种安全接入方案。目前深信服科技是国内唯一能够提供此IPSEC和SSL一体化解决方案的研发厂商。 作为国内领先的VPN以及网络安全研发，深信服科技长期专注VPN以及安全领域的研发，拥有多项发明专利，产品及功能应用于众多行业。深信服科技提供的解决方案，不仅可以应用于电信自身的移动办公，还可以作为电信运营商增值服务进行运营。2005年，SINFOR VPN电信互联增值业务运营平台，被国家科学技术部列入“ 2005年国家级火炬计划项目 ”。深信服科技的电信解决方案，必将不断提高我国电信行业的综合竞争力。 