解决方案：电力企业建网的SAFE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_ti2020/170/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_170934.htm 思科SAFE解决方案助电力客户建网腾飞 当今的电力企业领导者们都非常重视盈亏问题。为了保持竞争力，他们必须想方设法提高营业收入并降低成本。建设承载现代电力营销管理体系的网络是实现这一目标的重要手段，但是病毒、黑客等等时时威胁着电力网络的安全，因而电力企业必须寻找确保网络安全的效率最高、成本最低的方法。 思科公司提供了多种不同的可帮助电力客户提高生产效率并降低各项成本的端到端SAFE解决方案。思科SAFE蓝图可确保将安全性功能内置到电力网络的每个部分之中，可将市场领先的安全产品、成熟可靠的网络安全性惯例和统一平台管理与电力客户现有的网络基础设施结合起来，进而为电力客户提供全面的网络保护。 电力行业对网络安全的需求 来源：www.examda.com 众所周知，伴随改革进程的推进，中国电力行业形成了厂、网分离和电网按区域划分的全新格局。同时计算机网络技术的发展为电力的管理和调度提供了先进的服务和支持手段，为电力新业务（如电力市场应用、电力营销业务等）的开展提供了条件。从国家电力公司到下属各电力子公司正在进行着信息网络化的推进工作，基于网络的各种业务应用（如电力调度、企业信息化管理ERP、财务信息化管理等）正在逐渐开展。 网上开展电力业务具有便捷、实时的巨大优势，同时黑客的入侵、内部人员的操作失误、怀有各种目的人对信息的侵害等问题也相伴而来。为了规避潜在的计算机网络业务风险，使网络系统能

够安全及高效运行，就必须保证网络安全隔离，随时检测各种安全隐患，同时还要兼顾网络的高效时时通畅。 另一方面，随着电力调度业务、电力营销业务、电力市场业务等越来越广泛地开展，电力企业网和Internet的联系也越来越紧密。与此同时，Internet的自由性和先天的不安全性会给电力企业网造成越来越严重的隐患，并且有可能对电力业务造成极大的破坏，网络安全成为一个不容忽视且必须解决的问题。所以当前必须把安全问题作为网络建设和网络优化的关键来抓，必须建立一套完整的网络安全机制。 具体说来，电力网络系统包括各电力公司的局域网、广域网、数据中心、虚拟专用网（VPN）、Internet接入、网络管理等，必须从网络的总体角度来考虑网络的安全问题。 思科专业的电力SAFE解决方案 来源：www.examda.com针对电力信息网络的发展现状，思科系统网络技术有限公司制定了专业的电力SAFE网络安全解决方案。 解决方案突出网络级的安全监控和预警体系，有效地提高了电力企业对计算机信息系统自身安全漏洞和内外部攻击行为的检测、管理、监控和实时处理能力，实现合理地评估信息系统安全事件、有效地实时阻断非法和违规网络活动、准确地提供违规行为的全部审计档案的目标。从用户权限的一致性、网络周边安全、数据加密、安全的监视和政策管理五个方面全面统筹电力网络的安全体系。 思科专业的电力SAFE解决方案技术特点如下： 1、针对电力网络安全的薄弱环节全方位统筹规划。解决方案注重防止非法入侵全网路由器；保护电力数据中心及其灾备？中心的网络、服务器系统不受侵犯数据中心与Internet间必须有防火墙隔离，并且制定科学的安全策略；制定权限管理这是对应用系统、操作系

统、数据库系统的安全保障；考虑网络上设备安装后仍然可能存在的安全漏洞，并制定相应策略。 2、在网络设备的安全管理方面，将所有网络设备上的Console口加设密码进行屏蔽，配置管理全部采用OUT-BAND带外方式，并对每个被管理的设备均设置相应的帐户和口令，只有网络管理员具有对网络设备访问配置和更改密码的权力。 3、在网管中心通过划分VLAN来规范管理网络和工作网络，从逻辑上把每个部门的资源独立成一个VLAN， 对VLAN的划分基于安全性策略或规则，使VLAN的划分更具安全性。网络管理员可根据用户需求，把某些共享资源分配到单独的VLAN中，并控制VLAN间的访问。 4、VPN和IPsec加密的使用。电力网络将通过MPLS VPN把跨骨干的广域网络变成自己的私有网络。为保障数据经VPN承载商传输后不会对数据的完整与安全构成潜在危险，在数据进入MPLS VPN网络之前首先经过IPsec加密，在离开VPN网络后又再进行IPsec解密。 5、通过网络设置控制网络的安全。在交换机、路由器、数据库和各种认证上，层层进行安全设置，从而确保整个网络的安全。 6、通过思科 PIX 专用网络防火墙控制网络边界的安全。PIX的NAT地址转换功能既对外部网络屏蔽了内部网络，又使内部网络用户可以有效地对外部网络进行访问，其ASA自适应算法杜绝了从外网发起的对于内网的访问，而对于内网发起的对外网的访问则可以不受限制。 7、进行黑客防范配置。通过信息检测、攻击检测、网络安全性分析和操作系统安全性分析等一系列配置，对黑客进行监控。 8、使用思科的IDS保护电力中心网络。思科的IDS实时入侵检测系统可以通过对网络流量采样，来实时地监视网络流量和进行非授权使用检

测。同时，它可以通过封锁网络访问或终止非法对话来主动响应非法活动。另外，它还能够检测各种攻击并提供高级的IP碎片重组功能和“扫除”反IDS检测的能力。 9、思科的CSPM(Cisco Security Policy Manager)网络安全管理软件可统一的定制管理网络安全策略，并从集中的图形化界面管理Cisco PIX防火墙、Cisco IDS入侵检测系统探头(Sensor)等重要的网络安全元素，并可监控网络当前或历史上发生的安全事件。 10、对操作系统和数据库管理系统的安全配置。操作系统/数据库系统是网络应用系统运行的基本支撑平台，其安全指根据具体的操作系统/数据库管理系统的选型，利用其本身提供的安全机制，通过系统配置实现规划的安全业务，避免攻击者绕过应用系统直接操作敏感数据。 针对电力行业的模块化实施策略 来源：www.examda.com安全基础设施的建设是一个不断随技术进步而更新的长期过程。思科在总结企业网设计与实施经验的基础上，提出的SAFE体系架构是层次化、模块结构的模型。网络安全模块化有两种主要优势。首先，它允许体系结构实现网络各功能块间的安全关系，其次，它让网管人员可逐个模块地评估并实施安全性策略，而非试图在一个阶段就完成整个体系结构。如下图所示，对每个电力企业网的功能区模块进行了展示，这些模块在网络中扮演特定角色，有特定的安全需求。 一、在企业园区网中的模块的具体分析如下： 1、管理安全模块。在管理安全模块中通过思科IOS防火墙、SNMP 、NIDS、系统日志、系统管理、（带专用VLAN支持）的接入交换机、控制一次性口令（OTP）等手段组合完成安全策略实施。管理模块的主要目标是实现电力企业网中所有设备和主机的安全管理。记录和报告信

息从设备流向管理主机，而内容、配置和新软件从管理主机流向设备。 企业管理网络一般有两个作为防火墙和VPN端接设备的IOS路由器分开的两个网段。防火墙外的网段连接到所有需要管理的设备。防火墙内的网段包括管理主机本身以及作为终端服务器的IOS路由器。其余接口连接到生产网络，但仅用于来自预定义主机 、受IPSec保护的管理信息流。这样就可以管理没有足够物理接口来支持普通管理连接的思科设备。 2、核心和服务器模块。电力网络中的核心模块几乎与其它任意网络体系结构的核心模块一样。它主要是将信息流尽可能快速地从一个网络传送和交换至另一网络。服务器模块的主要目标是向最终用户和设备提供应用服务。服务器模块上的信息流由第3层交换机中的主板入侵检测进行检查。 服务器模块通常从安全角度会被忽略。在检查大多数员工对其所连服务器的接入水平时，服务器通常会成为内部攻击的主要目标。仅依靠有效口令不能提供全面的攻击缓解策略。使用基于主机和网络的IDS、专用VLAN、访问控制和出色的系统管理惯例（如使系统保持与最新补丁同步等），可实现对攻击的更全面响应。 3、大楼分布模块。此模块的目标是向构建交换机提供分布层服务，这其中包括路由、服务质量（QoS）和访问控制。数据请求流入这些交换机再传至核心，响应则以相反途径进行。 构建分布模块提供了针对内部发起的攻击的第一线防御。通过使用访问控制，它可减少一个部门访问另一部门服务器上保密信息的机会。例如，包含营销和财务的网络可以将财务的服务器分配到一个特定VLAN并过滤对其的访问，以确保只有财务人员能访问它。出于性能原因，重要的是，此访问控制应在能以近乎线速提供过滤

信息流的硬件平台上实施。这一般是需使用第3层交换而非更多的传统专用路由设备。通过使用RFC2827过滤，同一访问控制也可防止源地址电子欺骗。最后，子网分隔可将IP语音（VoIP）信息路由到呼叫管理器（Call Manager）及其相关语音网关。这可阻止VoIP信息穿过其它数据流穿过的网段，降低了窃听语音通信的可能性，可更平稳地实现QoS。 4、大楼接入模块。SAFE将构建模块定义为包括最终用户工作站、电话及其相关第2层接入点的扩展网络部分。其主要目的是向最终用户提供服务。 因为用户设备一般来说是网络中的最大规模组成，以简洁、有效的方式实现安全性是极具挑战性的。从安全角度来说，是在分布模块而不是在大楼接入模块中对最终用户实施的访问控制。这是因为工作站和电话与其相连的第2层交换机没有第3层访问控制功能。基于主机的病毒搜索在工作站级实施。 二、边缘分布模块。此模块的目标是在边缘集中来自各元素的连接。信息流从边缘模块过滤和路由并送至核心。 边缘分布模块在整体功能方面与大楼分布模块有些类似。这两个模块都采用接入控制来过滤信息流，但边缘分布模块在一定程度上可依赖整个边缘功能区域来执行附加安全功能。这两个模块均使用第3层交换来获得高性能，但边缘分布模块可添加附加安全功能，这是因为其性能要求不高的缘故。边缘分布模块为从边缘模块发送到园区网模块的所有信息流提供了最后一道防线。这可以减少电子欺骗分组、错误路由升级和对网络层访问控制的配置。 三、对企业边缘中包含的模块的具体分析如下： 1、公司互联网模块。公司互联网模块为内部用户提供了到互联网服务的连接并使互联网用户访问公共服务器上的信息。信息也可从此模块流

向VPN和远程接入模块（VPN在这两个模块终结）。 通过SMTP、 DNS、 FTP/HTTP、防火墙、NIDS应用和URL过滤等手段实现体系的安全。 本模块的核心是一对高可用的防火墙，它们为互联网公共服务和内部用户提供保护。状态检查会检验所有方向的信息流，从而确保只有合法信息流穿过防火墙。除模块中的第2层和第3层的高可用以及防火墙的状态故障转换功能，所有其它设计考虑也都围绕安全性和攻击缓解进行。 2、VPN和远程接入模块。此模块的主要目标有三个：从远程用户处端接VPN信息流、为从远程站点端点VPN信息流提供一个集中器，以及端接传统拨号接入用户。所有传送至边缘分布的信息流来自于远程公司用户，他们在被认可进入防火墙之前以某种方式进行了验证。 设计指南 除了高可用以外，此模块的核心要求是拥有三个独立外部用户服务验证和端接。因为信息流来自于企业网络外的不同来源，故此应决定为这三种服务的每一种提供防火墙上的独立接口。 3、WAN模块。此模块并不是潜在WAN设计的完全专用部分，它为WAN端接提供了高可用和安全性。采用帧中继封装，信息流可在远程站点和中央站点间传输。电信服务供应商的双连接通过路由器向边缘分布模块提供了高可用性。安全性由IOS安全特性提供。输入访问列表可用于阻塞来自远程分支机构的所有不必要的信息流。 电力行业青睐思科的理由 来源：www.examda.com众多电力行业用户选择思科安全解决方案的根本原因在于提高自身竞争优势的真实保障： 思科公司在全球技术支持方面是行业领导者，因此可帮助客户极大地节省总体拥有成本。思科公司的获奖服务包括了快速安装、维护和提升思科安全产品所必须的工具、专业技术和资源。 尽

管思科公司提供了PIX防火墙、入侵检测系统(IDS)、访问控制列表(ACL)和VPN集中器等产品并籍此成为安全性市场中的领导者，但必须认识到，行业目前所面对的全球安全性问题只能通过政府与企业间的合作才能得到解决。所以，思科公司与其他主要网络提供商及政府领导者开展了密切协作，目的就是要开发和提供能解决这一全行业难题的联合解决方案。 思科认为网络安全是一个复杂的问题，要考虑安全层次、技术难度及经费支出等因素，因此在设计方案时遵循了如下设计思想：尽可能地提高系统的安全性和可靠性；保持网络原有的性能特点，即对网络的协议和传输具有很好的透明性；易于操作、维护，并便于自动化管理，而不增加或少增加附加操作；尽量不影响原网络拓扑结构，便于系统结构及系统功能的扩展；安全保密系统应具有较好的性能价格比，一次性投资，可以长期使用。 安全护航 面向未来 来源：www.examda.com安全不是产品的堆砌。思科公司制定的面向电力企业网络的安全蓝图（SAFE）的主要目标是，为用户提供有关设计和实施安全网络的最佳实践信息。SAFE可作为正考虑其网络安全性要求的网络设计人员的指南。SAFE在网络安全设计方面采用了深入防御的方式。这类设计的重点在于所预测出的威胁及减轻威胁的方法，而不是单纯地“将防火墙放在这儿，将入侵检测系统放在那儿”等。该策略带来了一种安全分层方式，这样，一个安全系统的故障就不大可能引发对整个网络资源的损坏。 对于企业家来讲，面向未来的网络建设充满了一系列性能权衡。可以根据具体的资金情况来进行灵活的设计选择。无论是将分布模块拆分到核心模块中，还是将VPN和远程接入模块的功能与公司互联网模块

的功能合并，或者根据您的威胁响应策略的不同，合理配置NIDS应用，都需要一个科学的规划。