NSFOCUS

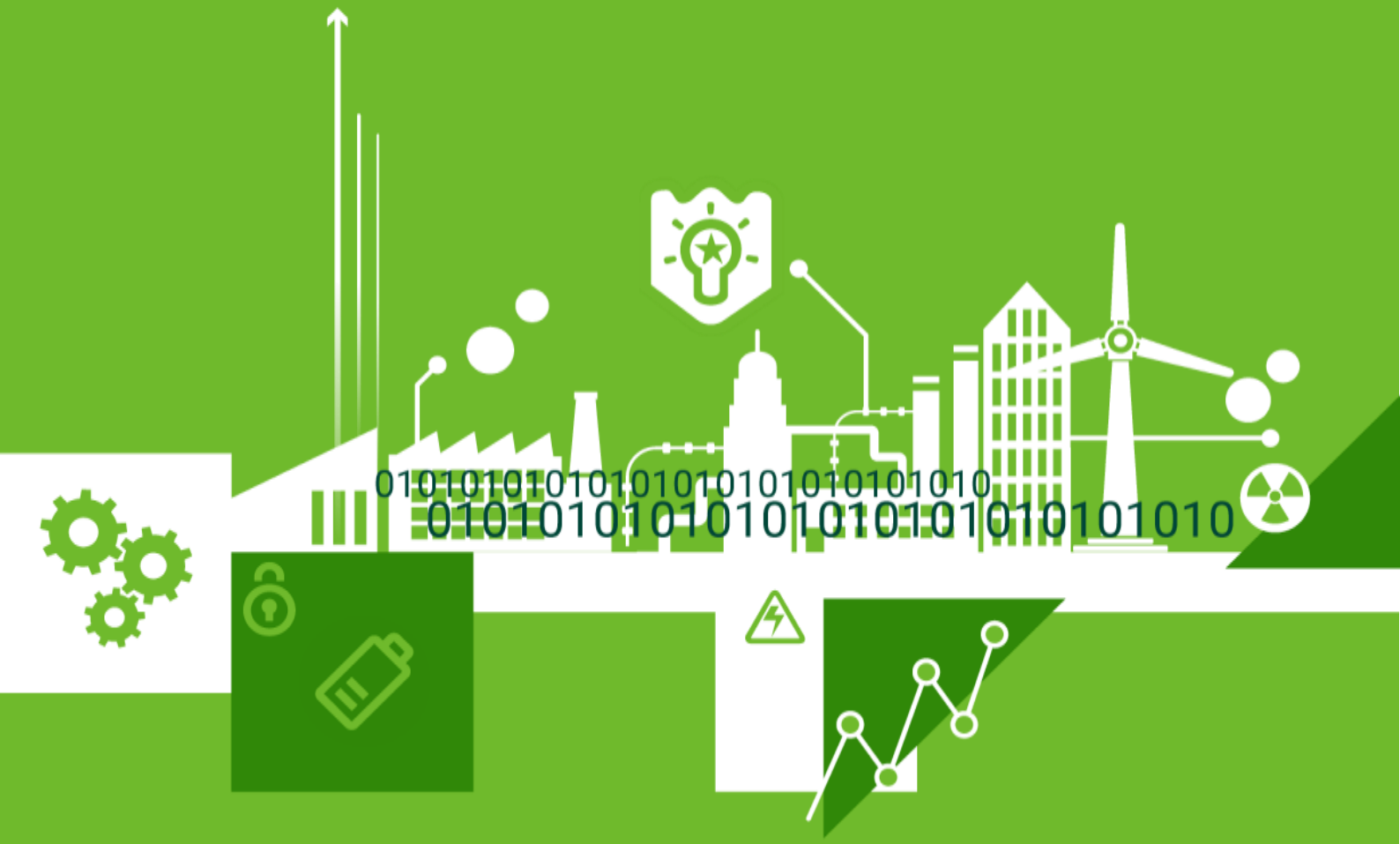
能源&企业事业部
月度安全通告

2016.12

扫码关注绿盟科技官

目录

一. 热点资讯


01010101010101010101010101010101010
01010101010101010101010101010101010

国家电网陈春霖：面向智能电网的信息安全 主动防御保障体系建设

根据《网络安全法》中对关键信息基础设施的定义，电力系统是重要行业之一。国家电网在推动智能电网建设上，落实安全管理要求，积极构建保障防御体系，多举措做好智能电网关键信息基础设施安全保障工作。

就此，国家电网公司信息通信部陈春霖主任发表《面向智能电网的信息安全 主动防御保障体系建设》一文。文章从智能电网内涵及安全挑战、电网安全防护的发展历程、智能电网信息安全风险及应对三个方面进行了详细阐述，也为国家电网“十三五”期间的信息安全建设指明了方向。文章节选如下：

安全风险分析

智能电网建设使得电网发电、输电、变电、配电、用电、调度各环节更为开放，带来大量业务结构的变化，基于互联网的社会服务和公众参与度更高，多种基于互联网的互动化业务应用发展迫切，电网侧、用户侧交互与应用更为频繁，同时，新技术的应用引入新的风险，对传统防护结构带来冲击。

国家电网智能电网信息安全主动防御保障体系建设

总体防护策略

国家电网公司贯彻落实国家和行业网络安全要求，主动适应“互联网+”、新电改等新形势业务发展以及信息化应用需求，推进电力关键信息基础实施安全防护提升，基于“可管、可控、可知、可信”的总体防护策略，打造下一代智能电网安全主动防御保障体系，全面提升信息安全监测预警、边界防护、系统保障和数据保护能力。

健全管理机制，加强内控治理

深入学习网络安全法，健全公司网络安全管理机制。进一步加强组织领导，公司舒印彪董事长担任网络安全和信息化领导小组组长。强化信息安全“三同步”，以业务全生命周期安全保障为目标，健全覆盖规划、可研、设计、开发、测试、实施、运行、下线等各个阶段的网络安全管控工作机制。建立风险报告和情报共享、研判处置和通报应急、网络安全运行、安全稽查、评价考核等网络安全工作机制。完善内控监督评价，常态开展内控达标治理工作。强化网络安全专业队伍建设，健全网络安全人才培训体系建设，完善网络安全职业认证，持续开展网络安全意识与能力建设。

全面加强网络边界安全防控

实施“安全分区、网络专用、横向隔离、纵向认证”的防护策略，分区部署、运行和管理各类电力监控系统，建设专用的电力调度数据网，生产控制大区与管理信息大区采用物理级别的横向隔离措施，同一级别的安全区纵向上落实加密认证措施。管理信息大区内网和外网通过自主研发的信息网络隔离装置进行隔离。深化互联网出口统一归集管理，提升互联网边界防护水平。按照等保要求区分系统安全域，各安全域的网络设备按该域所确定的安全域的保护要求，采用访问控制、安全加固、监控审计、身份鉴别、备份恢复、资源控制等措施。

构建全方位安全态势感知体系

开展基于大数据的信息安全事件深度分析、安全态势感知、智能预警分析、在线实时分析响应等信息安全监控预警技术研究与应用。重点从点（安全基线维度）、线（合规、预警、审计维度）、面（态势分析维度）三个功能层次，构建公司统一的网络与信息安全监控预警体系，并充分利用云计算和大数据分析技术，统筹开展信息安全情报收集、巡检、监测、预警、分析、研判与处置等工作，增强公司资产感知、脆弱性感知、安全事件感知和异常行为感知等网络与信息安全全景可视能力。

借鉴可信思想，提升应用保障能力

基于可信计算思想，加强智能电网主机、终端、应用和数据安全防护。按照国家信息安全等级保护的要求，采用相应的身份认证、访问控制等手段阻止未授权访问，采用主机防火墙、数据库审计、可信服务等技

术确保主机系统的安全。根据具体电力业务终端的类型、应用环境以及通信方式等选择适宜的防护措施，主要采取接入认证、病毒防护、安全桌面、可信芯片等防护措施保障终端安全。部署应用加密和校验、应用安全加固、应用安全审计、剩余信息保护、抗抵赖、资源控制、应用数据备份与恢复、代码安全管控等应用层安全防护措施，保障业务应用系统安全。按照涉密数据、商密数据、敏感数据、一般数据对公司数据进行分级防护。根据不同的级别，在数据的生成、传输和存储过程中做好数据加密和校验、备份与恢复等方面的数据安全控制措施。（本文刊登于《中国信息安全》）

安全管理与技术在中石化的应用

随着信息化进程加快，信息安全的重要性越来越凸显，我国已把信息安全纳入了国家安全体系，习总书记做出了“没有网络安全就没有国家安全”的重要论断，信息安全的重要性已经提升到国家战略层面。2014 年以来，中共中央网络安全和信息化领导小组的成立、首届世界互联网大会的召开、国家网络安全宣传周的开幕、网络安全法的正式颁布……，一系列信息安全举措密集出台，让大家深切感到了信息安全的重要性，安全意识得到极大的提升,信息安全已经深入到国家治理、企业经营和百姓的日常生活中，并且与国家安全息息相关。

就此中国石油化工集团公司信息化管理部 /刘远、石化盈科信息技术有限责任公司/吕浩、中国信息安全测评中心/张毅 任望，发标了《安全管理与技术在中石化的应用》一文。文章节选如下：

中国石化信息安全工作经验

经过“十一五”、“十二五”期间不懈的努力，中国石化网络和信息安全保障能力有了切实地提高，信息安全管理与信息安全防护技术并重，两手抓两手硬，信息安全管理和信息安全防护技术相辅相成，共同编织起了中国石化信息安全防护的大网。

信息安全管理以 ISO27001、ITIL 和 COBIT 等国际标准最佳实践为蓝本，借鉴企业 HSE 管理经验，结合企业实际，构筑了企业信息安全管理体系，形成了总部和企业两级信息安全组织管理构架，信息安全管理力度逐步加大，风险评估、安全测评和通报预警机制常态化运行。信息安全技术防护手段日益丰富，网络安全管控能力不断强化，形成了以应用系统为核心的纵深防御、多技术并举的防护体系。体现在一下几个方面：

1. *推动信息安全责任制，做实安全责任*
2. *严格信息安全过程管理，强化落实信息安全“三同步”要求*
3. *强化监督检查，全面开展信息安全风险评估工作*
4. *管好信息系统用户身份，全面部署统一身份管理系统*
5. *管控互联网风险，坚决推进统一互联网出口工作*
6. *提高信息安全风险综合管控能力，建设信息安全管控中心*

进一步提高思想认识，从要我安全，到我要安全

“人”是企业整个信息安全保障体系中最关键的因素。无论多么严谨的系统与体系，无论多么先进精良的设备，如果企业员工的信息安全认识不到位，信息安全意识不足，在日常工作没有形成良好的安全“习惯”，信息安全事故的发生是迟早的事情，势必会给企业带来不可估量的损失。从控制角度讲,未雨绸缪比亡羊补牢更有价值。进一步提高思想认识的目的，是要实现从要我安全，到我要安全的转变。要我安全和我要安全，两句话的重点都是“安全”，且一字不差，仅位置调换而已，但道出两种不同的思想和态度。后者表达了一种对安全的渴望，是发自内心的强烈需求；前者则恰恰相反，反映出一种对安全的消极态度，存在着一种明显的被动意识。后者符合生存的哲理，是科学的、积极而可行的；前者则违背现实，是危险的、消极而有害的。所以，培养企业信息安全意识文化，树立员工信息安全责任心，实现从要我安全，到我要安全的切实转变，

才是解决企业信息安全的关键之匙。也是中国石化信息安全工作下一步的重中之重。（本文刊登于《中国信息安全》）

明年会更糟！2017 年安全预测

从报税表诈骗到 WordPress 漏洞、勒索软件、商业电子邮件泄露、DDoS 攻击和总统大选被黑疑云——2016 简直就是网络安全地狱年，而且这还没完。

根本没理由相信 2017 会有所好转。若说有什么区别的话，那就是会变得更糟糕——因为网络罪犯会继续发动社会工程，找到投送恶意软件的新方法，破解有漏洞的数据库，利用移动技术来找出打破公司防御咬上目标人物的途径。

两位杰出的网络安全专家：安全访问软件公司 Bomgar 首席执行官马特 德克斯，安全设备管理和移动安全公司 Cyber adAPT 首席技术官斯科特 米里斯，为我们展望了一下 2017 网络安全形势。

口令“成长”

10 月 21 日造成互联网大面积掉线的 DDoS 攻击，至少有部分是因 IoT 设备上未修改的默认口令被黑客利用而发起的。别觉得自己能幸免，有多少用户用的是简单、常见、过时的口令？2017 年，更好的口令管理服务，会随着企业意识到自己防护有多差而引起重视。

有太多特定用途的“哑”设备了，就像前面说过的助力 DDoS 攻击的那些路由器，这让黑客们的工作变得十分容易。

弱口令依然一统江湖的时候，网络安全人员面对关键基础设施、联网系统和远程访问系统及设备防护任务简直一筹莫展，而且问题还不只是外部威胁一种。

内部威胁缓解也可以通过更好的口令管理来完成。最佳方式，是实现用户未知口令安全存储的解决方案，并定期验证和轮转这些口令以确保安全。

这里指的，其实就是凭证保险柜。理想状况下，用户不会知道自己的口令，口令由保险柜自动填充，并且每周轮转和改变。黑客本质上是很懒的，他们也有自己的时间需求。如果你让他们的破解工作更难，他们就会转移目标而不是投入时间精力来跟你死磕。

权限受到重视

黑客想要高权限，他们通过瞄准 IT 员工、CEO 和供应商之类的特权用户来获得高权限。虽然公司对重要系统、应用和数据采取了安全措施，这些预防性措施显然已不再足够。2017 年，懂行的公司最终会严肃对待特权用户保护问题，而不仅仅是系统防护，他们会识别、监视特权用户的访问，关闭他们不需要的权限。

有人说“我的用户和外部供应商都只能用 VPN 来连接，挺好的。”但其实他们根本不知道这些外部人士到底都在读取些什么！权限管理就像电梯间，根据角色，乘客只能进入某些特定楼层，切实地限制了用户行为，尤其是在用户怀有恶意的情况下。即便手握有效口令，只要权限限制了只能访问第 1 和第 7 层，任何试图闯入第 6 层的做法都会触发警报并锁定电梯。

解决权限问题，同样需要公司愿意提供关于潜在危险的扩展教育和培训，尤其是在越来越多的移动办公人员太喜欢牺牲隐私和个人数据来换取访问权，而且天真地以为自己的安全会被第三方服务提供商和 App 作者保护好的情况下。

尤其是最近几代数字原住民，太愿意给出自己的个人数据来换取 App、联网、信息等等的访问权了——利用这一点简直不要太容易！他们几乎默认这些 App 开发者、服务提供商会确保他们的安全。天真！危险！综合考虑如今的网络安全技术缺口、人才短缺、移动办公、App 为中心的环境、更高级的黑客活动，我们面对的根本就是一场完美风暴。只会更坏，不会更好。

安全责任推卸升温

现在，安全公司的客户倾向于连“假如”发生网络攻击事件都不提了，直接就问“什么时候”被攻击？情况会有多糟？这种自己撒手不管，完全依赖安全公司服务的思潮，是十分恐怖的。

IoT 和对安全解决方案提供商越来越重的依赖度，意味着公司企业可能在数据泄露发生时推卸其所有权和事件源头的责任。谁应该对保护、维护和修复各种技术负责？更糟的是，有没有产品被接入根本无法打上补丁的内部系统？很多 IoT 设备经常因为不在 IT 传统管辖范围内而被无视掉，但这确实造成了对威胁的暴露面。

IoT、自动化和云在不断集成整合，但似乎没人完全确定到底谁该对维护所有这些不同技术的安全负责：IoT 设备制造商？安全服务提供商？内部 IT 团队？个人用户？在安全上，木桶理论完全适用——取决于最不安全的设备或关系。

当数据泄露发生，即便有层次化的安全措施，谁负责、谁有权响应的问题，也将引发激烈的争执和相互指责。

通过确保 IT 与业务部门之间的开放沟通，理解潜在威胁、安全选项、公司内部的挑战和限制，此类责任推卸游戏便可有效杜绝。

部分问题在于：作为 CSO、CISO 甚或 CIO 之类安全相关责任人，如果你工作做得超棒，那么你基本上毫无存在感；否则，你将如坐针毡。如果你定出了不错的策略、规程和安全措施，通常也得交给 IT 来实施。但如果因为你没能理解业务需求、预算、各种要求而导致这些措施没起到效果，那你就真的可有可无了。

勒索软件将失去控制

自 2016 年 1 月起，赛门铁克安全响应小组见证了每天平均 4000+勒索软件攻击：比 2015 年的数据增加了 300%。

大多数公司依赖低开销预防技术来缓解此类威胁，比如防火墙、反病毒解决方案或入侵预防。然而，这些工具并不足以起到完全预防作用，被泄露的数据大军赤裸裸地昭示着这些检测和事件响应方法必须改善。

随着攻击者继续使用社会工程和社交网络来锁定敏感角色或公司内部人士，全面安全教育的需求变得比以往更加紧迫。

如果安全策略和技术不将此类攻击方法纳入考虑，勒索软件将持续渗入。还有检测问题。有些攻击者能在公司环境中畅游数月之久，而网络、边界、终端和数据安全系统及过程之间的隔绝却限制了公司预防、检测和响应高级攻击的能力。

最后，新的攻击界面，比如说：IaaS、SaaS 和 IoT。这些东西太新了，公司企业还没弄清保护它们安全的最佳方法。

驻留时间看不到多大改善

驻留时间——从攻击成功到被受害者发现的时间间隔，在 2017 年不会看到任何改善。某些极端案例中，驻留时间甚至能达 2 年之久，给公司造成数每次泄露百万美元的损失。

为什么会这么久？原因令人无奈的简单——几乎没有对真正攻击活动检测的关注。随着恶意软件时代的到来，公司、厂商和个人都绷紧了‘把坏人拦在门外’的弦，整个行业快速成长，专注于两个基本主题：“深度防御”——用层次化预防战术让从外部渗透变得更难；以及“恶意软件识别”——已证明自身是朝向 100%检测率的军备竞赛。

响应技术和修复能力都有了进步，受害者可以快速隔离和修复攻击所造成的损害。但是，问题在于，这些技术对减少驻留时间没什么卵用；除非响应团队偶然遇到了某些恶意事件，或者意外发现了某个异常。

时至今日，安全人员使用网络设备日志文件来搜索攻击是否发生或已成功的线索，但存储和分析这大量数据是花费巨大且低效的。

大量数据存储和大规模分析引擎的需求，驱动了新安全信息和事件管理(SIEM)产业。但是，尽管 SIEM 是个很好的事后鉴证工具，却依然对发现实时进行中的攻击毫无效果。分析原始网络流量以发现攻击指征或许会有所帮助。在黑客攻击边界或设备防护层时，或者在他们作为无辜/恶意内部人士完全绕过防护措施后尽快发现他们，将大幅缩短他们的驻留时间。

手机作为切入点的数据泄露将持续上升

2017 年，至少会有 1 起(大概会更多)重大企业数据泄露事件由手机导致。波耐蒙研究所一份报告发现，对一家企业而言，手机数据泄露的经济风险可高达 2640 万美元。该项调查中 67%的受访企业报告称，曾因员工使用手机访问公司的敏感和机密信息而导致数据泄露。

当今世界的人员及其手机都流动得太快太频繁了，老一套网络安全策略很难起效。而且，随着用户对其所选手机权利意识的增长，漏洞利用形势堪称成熟。

很多用户觉得自己能在对公司和个人服务的持续访问中保护好自身隐私。还有很多人丝毫不觉得自己是安全事件责任人；如果他们能规避“安全”以改善用户体验，他们会的。CISO、CIO 和 CEO 将之视为实现企业安全策略的复杂挑战，而且是不能用通过 SSL 发送电子邮件和日程安排到单一指定 OS 能解决的。

手机支付，也将成为安全责任的一方面。MasterCard 的“自拍支付”和英特尔的人脸识别解锁软件 True Key 只是冰山一角。个人应当明白，自身生物特征数据应像其他财务和私密数据一样得到妥善保护。而这，又落到了教育和培训的身上。

公共 WiFi 接入提供商像香烟盒上印制“吸烟有害健康”标语一样竖起互联网安全警示牌或许会比较好。比如说，“警告：本公共接入连接不安全，您收发的信息有可能被罪犯偷看、收集并用以盗取您的资产、身份或私密信息。”

IoT = 威胁网？

IoT 漏洞和攻击还会继续增长，对各类安全措施的标准化需求亦然——今年 DefCon 上的黑客展示了 47 个新漏洞，影响 21 个厂家的 23 种设备。

还有，今年 10 月让包含推特、Netflix、Reddit 和英国政府网站在内世界主要站点掉线的大规模 DDoS 攻击，据说也是由不安全 IoT 设备组成的 Mirai 僵尸网络造成的。

投放到“智能设备”上的大量关注正好印证了 IoT 日益扩张的影响力。现实却是，联网设备未必是智能设备。联网的“东西”，通常因其简单性而是“即发即弃”没有后续维护的，或者干脆就是我们根本不知道的一些内置功能或工具——就像 Mirai 僵尸网络中使用的那些路由器。这导致了一种无视这些“哑”设备的思维，根本没注意到这些设备虽然“闷不吭声”，却是连接到联通全球的互联网上的。

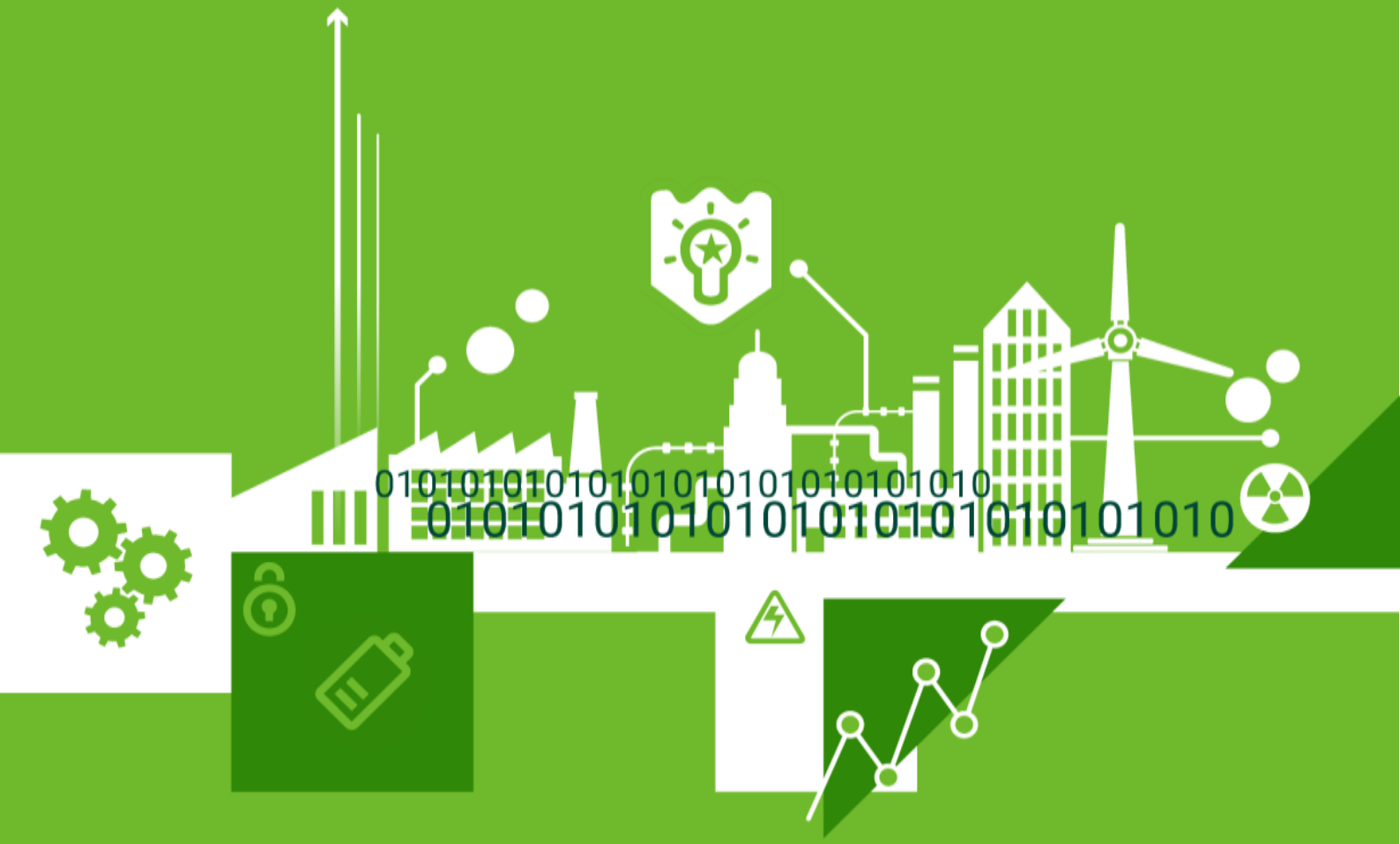
这还不仅仅是小型消费级设备，甚或智慧家居或智慧汽车的问题。更令人不安的，是对广泛使用的大型基础设施系统的攻击，比如电网、航空电子设备或铁路系统。

联网喷头忽冷忽热都是小问题，2017 年遭遇电网或交通系统大型黑客事件的极高可能性才令人担忧。这些来自 50 或 60 年代的技术依然在为关键基础设施系统服务，而且几乎完全没有防护，这才是实实在在一点就爆的“哑”IoT。

其实这是个认知问题。普罗大众似乎不认为这些系统与他们日益频繁使用的 IoT 设备类似——甚至手机都能落入该分类范畴。

就像之前的智能手机，IoT 设备被认为是新的、独立的一类东西，不属于老一代技术范畴，不受过往技术的限制。但这种想法很是荒谬：智能手机根本是最常见最广泛的互联网设备。IoT 则是下一个大规模风行的东西。有些公司这次稍微前瞻了一点点，试图摒除掉 IoT 上类似手机当前面临的那些安全问题。目前为止，采取的行动还是又落回了预防上，但每个设备/连接都是可被攻击的。缩短驻留时间和保护 IoT 安全，取决于能否尽快以最高置信度报出这些不可避免的攻击所发生的时间。

二. 警钟长鸣


01010101010101010101010101010101010
01010101010101010101010101010101010

重大安全事件

NTI 绿盟科技威胁情报中心、绿盟科技威胁响应中心、绿盟科技 DDoS 攻防研究实验室、高级安全研究部等组成的协作小组，随时关注重大安全事件的进展情况，针对影响面大、危害严重、行业关系紧密的安全事件给出深度分析报告。

京东千万条账户数据泄露？京东回应称系 2013 年的漏洞所致

12 月 11 日消息，有媒体报道称一个 12G 的数据包在黑市上开始流通，其中包括用户名、密码、邮箱、QQ 号、电话号码、身份证等多个维度，数据多达数千万条。而黑市买卖双方皆称，这些数据来自京东。

对此，京东方面紧急发布声明，并未否认这些数据来自京东，同时京东在声明中强调，这些数据初步判断源于 2013 年 Struts 2 的安全漏洞问题，当时国内几乎所有互联网公司及大量银行、政府机构都受到了影响，导致大量数据泄露。

同时，京东方面建议用户高度重视信息安全和隐私保护，在涉及到财产的电商、支付类系统中使用独特的用户名和登录密码，开启手机验证和支付密码，并将登录密码和支付密码设为高强度的复杂密码，提高账户安全等级。

事实上，电商平台一直是数据泄露的重灾区之一，据一本财经统计，京东在 2015 年就曾被曝出大量用户隐私信息泄露，用户共损失数百万。一年后，京东公布调查结果，称因“内鬼”——3 位京东物流人员，通过物流流程，掌握了用户姓名、电话、地址、何时下单、所购货物等信息，总数据达到 9313 条。

而 2014 年初，支付宝也曾被曝 20G 用户资料泄漏，包括用户个人的实名、手机、电子邮箱、家庭住址、消费记录等，相当精准。后经调查，此次泄漏同样是“内部作案”：支付宝前技术员工李明和两位同伙，利用职务之便，多次在公司后台下载用户资料，将用户资料按条数出售，价格不等，价值较高的，一条可卖数十元；也有人以 500 元的代价，购买了 3 万条用户信息。

此外，2014 年底，中国铁路购票网站 12306 的 6 个子网站存在高危漏洞，致数十万条用户数据外泄，包括用户账号、明文密码、身份证、邮箱等敏感信息在内的数据被贩售。12306 宣布悬赏、号召网友查找漏洞；2012 年 1 号店被曝网上商城员工与离职、外部人员内外勾结，90 万用户资料泄露，价格只需 500 元。

乌克兰再次发生断电 疑为网络攻击所致

据乌克兰能源公司 UKrenergo 消息，上周六半夜，乌克兰首都基辅北部及周边地区发生断电，电力公司专家采用人工操作，30 分钟后开始逐渐恢复供电，75 分钟后已全面恢复。

UKrenergo 公司主管 Vsevolod Kovalchuk 在 Facebook 上发文称，发生本次事故的原因可能是设备失灵，或者也可能是网络攻击；推测此次事故的原因为“通过数据网络的外部干预”，公司专家及执法部门已发起调查，并称将在不久后发布事故报告。

此次事故不由让人想起去年 12 月乌克兰电网遭遇攻击事件，当时许多安全专家认为是俄罗斯黑客组织，利用 BlackEnergy 和 KillDisk 恶意软件，向乌克兰的电力公司发起了 DDoS 攻击，并延缓其修复过程。

2015 年的那次事件发生后，电力公司专家用了 3-6 小时才修复问题。

值得一提的是，前几天 ESET 的博客文章提到，攻击乌克兰电网并致其停运的 BlackEnergy 黑客组织现如今似已更名 TeleBots，目前该黑客组织已经将目标转移到了乌克兰银行。

据说攻击所用恶意程序中的不少恶意代码和 BlackEnergy 先前所用的具有较大相似性，所以 ESET 推测 BlackEnergy 组织也就是现如今的 TeleBots。

不知本次乌克兰停电事故是否与之相关。

重大安全漏洞

绿盟科技威胁响应中心 NS-SRC 每天都在关注重大漏洞的发展动态，制定了完善的闭环应急响应流程，指导安全事件紧急响应服务操作人员按照该流程，保证实施进度和质量的可控，在规定的时间内完成应急响应服务。通过多部门、多平台的合作，实现全面的安全事件检测、预警与防护方案。

Firefox 远程代码执行漏洞

2016 年 11 月 30 日，Mozilla Firefox 官网发布了一个紧急更新，修补了编号为 CVE-2016-9079 的漏洞。该漏洞是一个存在于 SVG 动画模块中的释放后重用(UAF)漏洞，当用户使用 Firefox 浏览包含恶意 Javascript 和 SVG 代码的页面时，会允许攻击者在用户的机器上远程执行代码。受该漏洞影响的平台包括 Windows，Mac OS 以及 Linux。

影响的版本：Firefox version < 50.0.2、Firefox ESR version < 45.5.1、Thunderbird version < 45.5.1

官方已经发布了版本更新，建议用户升级到最新版本。在火狐浏览器中勾选自动更新后，浏览器会自动更新到该最新版；或者手动下载最新版本安装，下载页面如下：

Firefox 50.0.2

https://www.mozilla.org/en-US/firefox/50.0.2/releasenotes/

Firefox ESR 45.5.1

https://www.mozilla.org/en-US/firefox/organizations/all/

Thunderbird 45.5.1

https://www.mozilla.org/en-US/thunderbird/

红帽 JBoss Fuse 及 JBoss A-MQ 所用 Karaf 远程代码执行漏洞

2016 年 11 月 25 日（当地时间），bugzilla.redhat.com 对编号为 CVE-2016-8648 的漏洞信息进行了更新。该漏洞存在于红帽 Red Hat JBoss Fuse 和 Red Hat JBoss A-MQ 所使用的 Karaf 包中，漏洞发生于通过 JMX 操作向 MBeans 传递的对象被反序列化的过程中。一个远程攻击者可在运行 JAVA 虚拟机且在 MBean 的类路径中包含反序列化组件的机器上利用该漏洞，从而造成远程代码执行。

受影响的版本：Red Hat JBoss Fuse 6、Red Hat Jboss A-MQ 6.3.0

规避方案：官方目前暂未发布针对该漏洞的版本更新，由于利用该漏洞需要“admin”的用户身份，所以作为临时的缓解策略，使用 Red Hat JBoss Fuse 或 Red Hat JBoss AM-Q 的用户可以在“etc/users.properties”文件中为“admin”用户设置一个强口令。

Apache HTTPD 拒绝服务漏洞

2016 年 12 月 5 日（当地时间），seclists.org 网站发布了一条关于 Apache 网页服务器拒绝服务漏洞的消息，漏洞编号为 CNNVD-201612-069。该漏洞存在于 mod_http2 模块中，这是从 Apache HTTPD 2.4.17 版本开始引入的关于 HTTP/2 协议的模块。然而该模块在默认情况下不被编译，且默认不启用，该漏洞只影响使用 HTTP/2 协议的用户。在使用 HTTP/2 协议的服务器上，攻击者可以通过发送精心构造的请求，导致服务器内存耗尽，造成拒绝服务。

受影响的版本:Apache HTTPD version 2.4.17、Apache HTTPD version 2.4.18、Apache HTTPD version 2.4.20、Apache HTTPD version 2.4.23。

规避方案：Apache 官方尚未发布版本更新，然而 github 上已经对该漏洞进行了源代码修复，建议用户下载最新的源码编译安装。github 链接地址如下：https://github.com/apache/httpd。作为临时的缓解策略，已经启用 HTTP/2 的用户也可以从配置文件的“Protocols”行中删除“h2”和“h2c”从而禁用 HTTP/2 。

OpenSSH 远程代码执行漏洞

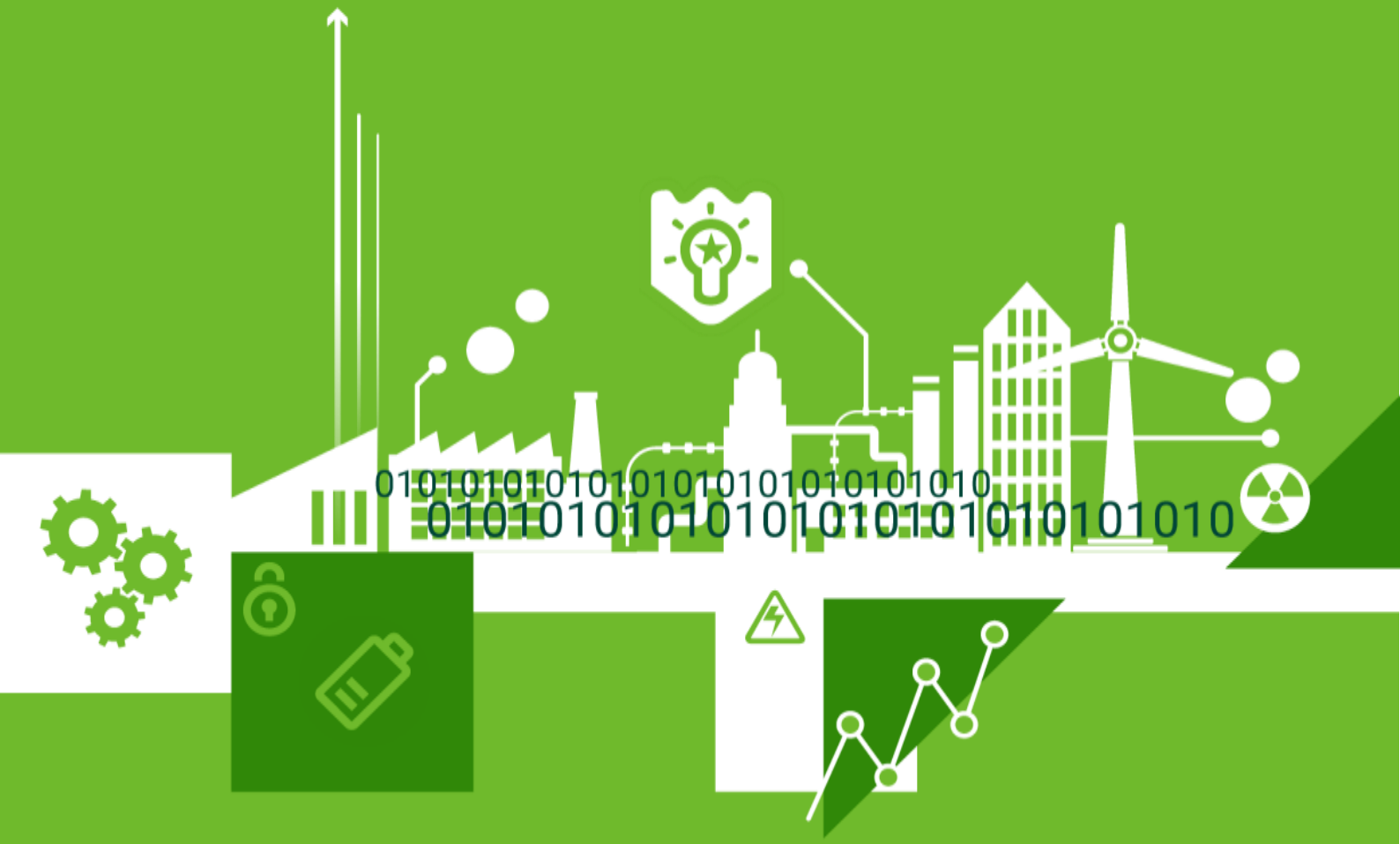
2016 年 12 月 19 日，OpenSSH 官网发布了一个 OpenSSH 的版本更新，在新版本中修复了编号为 CVE-2016-10009 的漏洞。该漏洞允许攻击者在运行 ssh-agent(该程序通常运行在客户端)的机器上加载一个恶意模块 PKCS#11 从而使攻击者有机会执行远程代码。

受影响的版本: OpenSSH version < 7.4

规避方案：官方已经发布了该漏洞的版本更新，建议用户升级到不受影响的最新版本，下载页面如下：

http://www.openssh.com/portable.html

三． 安全技术焦点


0101010101010101010101010101010
0101010101010101010101010101010

漏网之鱼——无线安全迫在眉睫

近年来大量遭受无线攻击而造成经济损失的事件被报道，政府、社会、媒体也都在高声疾呼无线安全的重要性，要提高网络安全意识。但是针对个人防范无线攻击的方法或是教育多入牛毛，反而企业无线安全却被忽视了，针对个人的防范手段对企业来讲很难起效，事前预防和事中防御就变得尤为重要。

2013 年全球顶尖娱乐软件公司-育碧（Ubisoft Entertainment）发布了一部重磅作品《看门狗》，玩家扮演一名名为 Aiden Pearce 的顶级黑客在美国芝加哥‘惩奸除恶’，利用一台功能强大的智能手机随意游走在城市中任何相互连接的电脑系统，轻松获得任何人的个人信息，潜入中央系统安装后门程序，操纵整个城市。

这种超人般的存在如果搬到现实社会中会是什么样子，可以肯定这将会是一场灾难。试想一个手持移动设备在你附近游走，分分钟攻破你的无线网络，干扰网络、安装后门程序，窃取重要数据会是什么样的情形。

不要觉得这不现实，类似的安全事件已经发生：

1. 美国史上最大信用卡 WiFi 窃案主犯 28 岁的 Albert Gonzalez 通过驾车搜寻存在安全隐患的无线网络，并对其进行攻击，窃取酒店、超市、支付系统等用户的信用卡账号，偷盗贩卖 4100 万个信用卡和提款卡号。

2. 上海地铁 10 号线，因 WiFi 无线列控系统故障导致“开错方向”事故。同年，再次由于无线列控系统故障，在切换成人工驾驶后，操作失误，导致列车追尾；

就在今年年初 WIFI 联盟正式发布 802.11ah WIFI 标准，这项新技术功耗更低，覆盖范围更远，穿墙能力强。你是不是觉得这很 Cool，以后无线生活会更加便利，美好？不要太乐观，这一新技术覆盖的范围可以达到 1 公里。1 公里意味着黑客可坐在附近的民宅喝着咖啡轻松绕过你的传统安全设备，拿走他想要的东西，留下你不想要的隐患。你觉得你的安全防护已经固若金汤，现在看来其实还有漏网之鱼。而且随着无线技术的不断发展，无线安全风险会愈演愈烈，企业及个人在享受科技带来的红利的同时，也承受着等价的安全威胁。

目前我们所面临的无线安全风险大致分为这么几种：

1.流氓 AP

使用 360 随身 WIFI 等工具创建临时无线热点，引狼入室。

2.非法外联；

私自通过 WIFI 万能钥匙或是找没有密码的无线信号，蹭‘别人’的网，反遭泄密。

3.非法内联；

攻击人使用非法 AP 嗅探公司无线网络，随即进行密码破解，直接进入内部进行数据下载或安装后门。

4.钓鱼 AP；

攻击人伪造公司无线网络，被攻击人诱使登录后，利用社会工程学方式诱骗获得公司 wifi 密码，邮件、内网账号等信息。

5.WLAN 中间人攻击；

攻击人伪造公司无线网络，被攻击人诱使登录后，攻击者再以终端身份连接到合法接入点，在中间中转被攻击人跟合法接入点之间的流量，从而进行数据的明文监听和更高级的攻击。

6.WLAN 拒绝服务攻击；

无线 DoS 攻击，造成无线接入点瘫痪。

近几年有大量遭受无线攻击而造成经济损失的事件被报道，政府、社会、媒体也都在高声疾呼无线安全的重要性，要提高网络安全意识。但是针对个人防范无线攻击的方法或是教育多入牛毛，反而企业无线安全却被忽视了，那些针对个人的防范手段对企业这种人数众多的经济组织来讲很难起效。事前预防和事中防御就尤为重要，要想进行良好的无线防护自身就必须满足以下几点：

1.具备无线防火墙能力，结合射频信号及 802.11 特点，提供无线防火墙安全策略，能根据 AP 或 Station 的安全属性定制无线网络准入规则，通过射频信号阻止非法用户接入，支持建立射频安全区，提供具有物理安全、可信的无线网络。

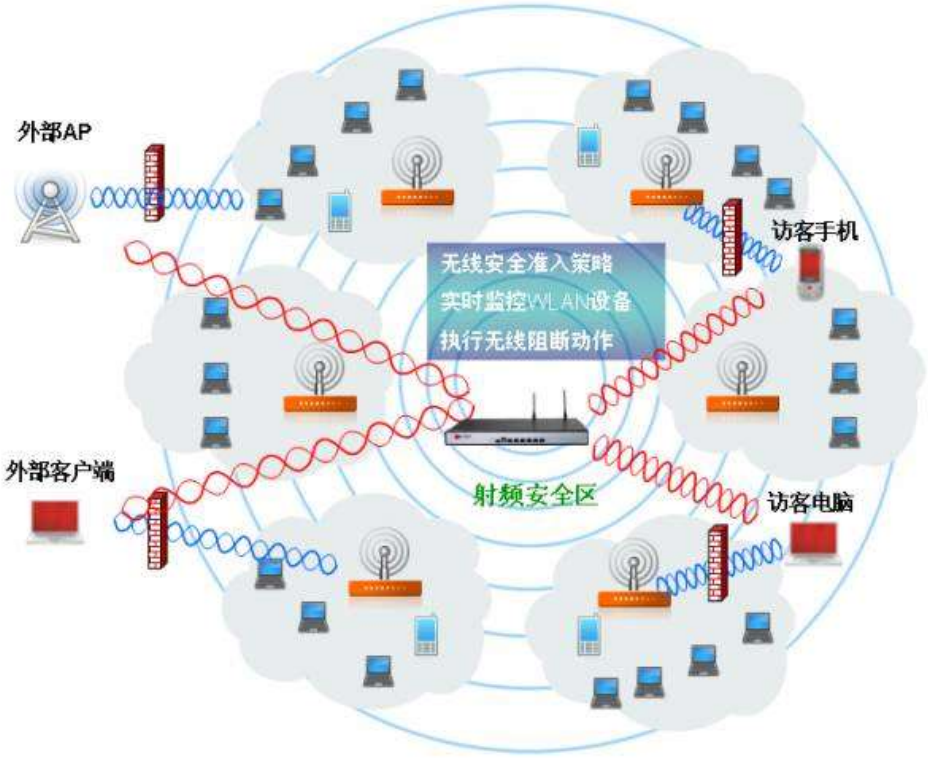
2.具备包括无线扫描、欺骗、DoS、破解等多类性无线攻击的检测规则，以及告警、阻断能力，同时还需要有多种类型流氓 AP 的检测与阻断能力。

3.具备丰富的报表统计，能够提供无线网络实时拓扑、雷达图、柱状图、饼状图、攻击排名等多种丰富统计，一目了然的了解无线安全状态。

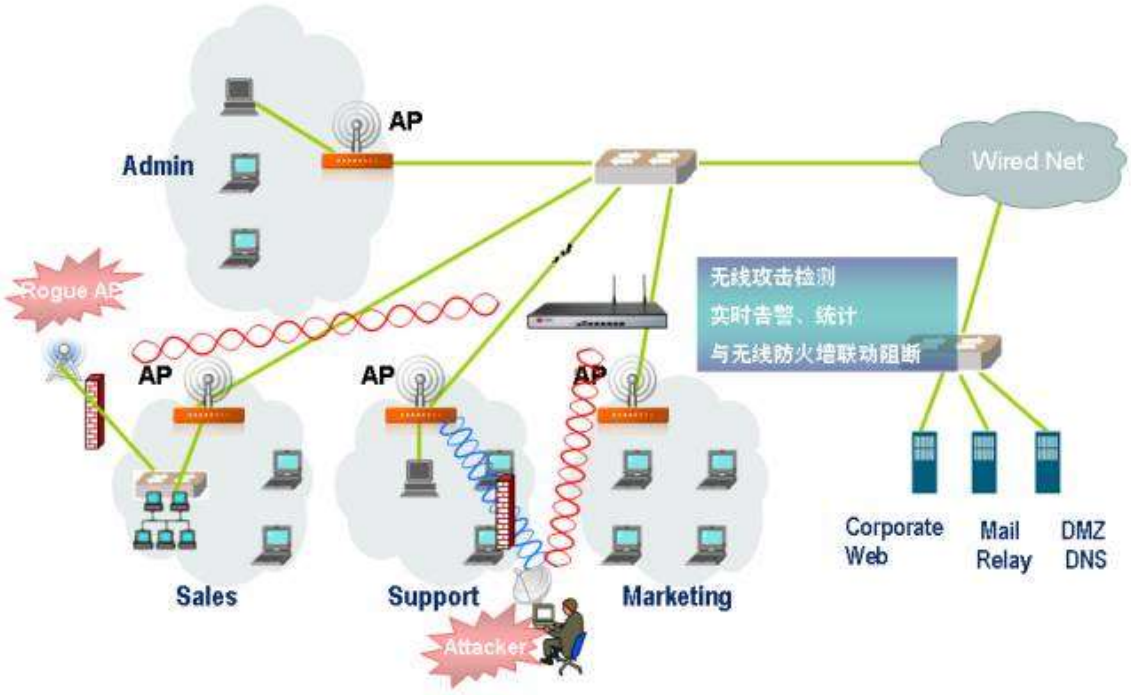
其中最能检验无线安全产品专业性的重要标准是，自身具备多少检测规则。为什么这么说？由于无线攻击的特殊性，传统的攻击检测规则无法适用，所以就要求安全厂商必须非常了解无线传输技术以及无线攻击的方式和手段，有针对性的制定出适用于无线攻击的检测规则。所以有没有专业的检测规则，就可以评判是不是一个真正的无线安全产品。而检测规则越多产品的专业性就越强。

同时无线安全类产品的实现基础应该是这样的：

1.事前预防



2.事中防御



在具备以上几个重要能力和实现基础之下，才能称之为支撑企业无线网络安全的坚实后盾。

无线网络安全任重道远，我们还有很长的的路要走，正所谓魔高一尺道高一丈，构建出安全、良性的无线网络环境才能使我们的生活生产得到保障，在享受无线网络带来的红利的同时免去一些侵扰和风险。

你的云安全吗？

近年来，随着虚拟化技术的不断发展与完善，云计算得到了广泛的认可与接受，许多组织已经或者计划进行云平台建设。因此，一大批云计算服务提供商也涌现了出来，包括知名的 Amazon AWS、Google GCE 以及 Microsoft Azure；同时，国内也出现了像阿里云、腾讯云、移动云、云杉网络等一批优秀的云服务提供商。

云平台的发展与普及加大了数据泄露和网络攻击的风险。一方面，虚拟化系统本身就存在一定的安全威胁。比如，作为当前全球最大的商业和开源虚拟化系统，VMware 和 OpenStack 曾分别出现了 222 和 68 个漏洞，其中不乏高危漏洞。如果攻击者通过 Hypervisor 漏洞从虚拟机逃逸到宿主机，那么攻击者就可能读到宿主机上所有虚拟机的内存，进而控制这台宿主机上的所有虚拟机。

另一方面，在当前广泛为大家所接受的云平台中，它的虚拟化环境很少提供专门的安全防护机制或者部署专门的安全设备来防护租户的资源。因此一旦攻击者对租户的计算、网络或者存储资源进行攻击，无论是租户还是云平台，对此将无能为力。

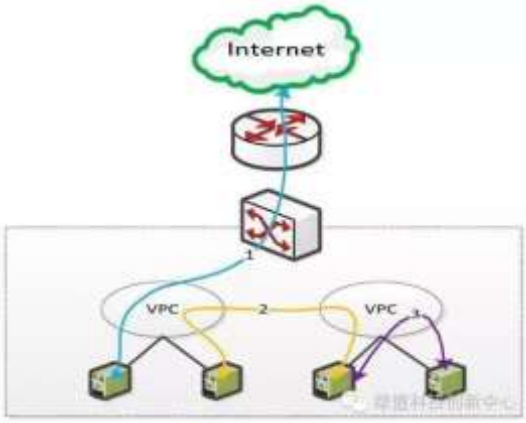
众所周知，在传统的数据中心中，安全防护通常是通过在安全域入口部署专用的安全设备来实现的，比如防火墙、IDS、IPS 等。那么在云计算这种新型的计算模式下，传统的“一劳永逸”的防护方案就不那么奏效了。一方面，各租户的业务和流量存在很大的差异，如果单纯的在入口进行安全防护，既难做到租户之间的区分，同时也会在一定程度上加大安全设备的负载，增大网络故障的风险。另一方面，云环境使得网络的边界变得不像物理数据中心那么清晰，很难进行固定安全域的划分，同时东西向流量又占据了很大比重，因此机房内部的流量攻击是传统入口部署方式防护不了的。

云环境防护需求

从传统数据中心的安全防护来看，通常安全设备所提供的防护能力，包括扫描类（比如系统漏扫、Web 漏扫、配置核查等）的安全服务和网关类（比如防火墙、入侵防御、入侵检测等）的安全服务。那么对于云计算等虚拟化环境下业务的安全防护，其防护需求是否发生了新的变化？虚拟化环境的安全防护又和传统数据中心的安全防护有什么区别？

其实，无论是针对传统数据中心的安全防护还是基于云计算的虚拟化安全防护，业务对于安全防护的需求，在本质上并没有发生变化。换句话说，安全防护的手段也没有发生实质性的变化。其不同之处在于虚拟化环境下，业务的流量更复杂，防护的方式更加的多元化、复杂化。

从大多数的云环境业务网络部署规划来看，用户在将其业务部署云化之后，其流量主要包括三个方面：（1）公网访问云平台内部业务的流量，也就是通常所提到的南北向流量；（2）同一个租户不同子网之间的访问流量；（3）租户同一个子网不同虚拟主机之间的访问流量，也就是所说的东西向流量。因此，基于云环境的安全防护，通常也基于这三种不同类型流量进行应对。



云环境防护思路

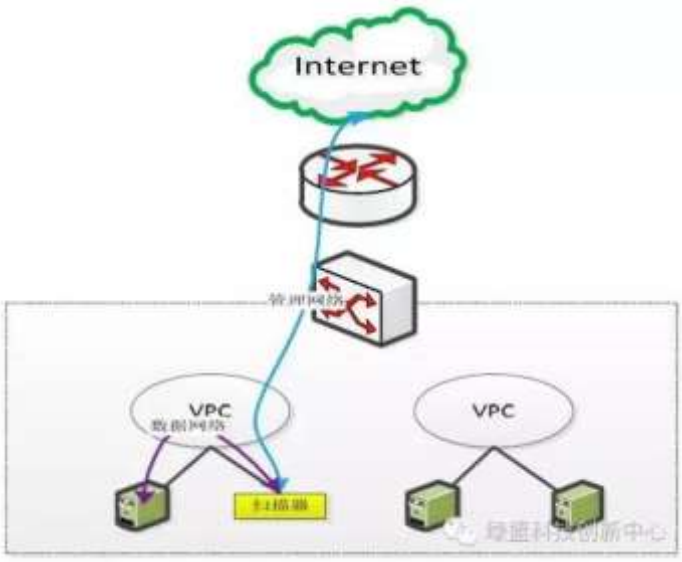
上文提到，通常安全防护的服务包括扫描类和网关类两种，那么如何在云环境中有效的应用这两种类型的安全防护，使我们的云更安全呢？

扫描类服务

扫描类防护服务，其核心的问题在于，安全服务需要与被防护对象网络可达。从这个角度来看，云上业务的扫描类安全防护可以分为两类。一种是拥有外网访问权限的业务；另一种是外网无法访问的业务。

拥有外网访问权限的业务，比如我们的 Web 服务器、邮件服务器等。对其进行扫描类安全防护通常比较简单，可以直接采用云端的扫描服务，比如绿盟云的极光自助扫描。用户只需按需的申请扫描应用，而无需购买、部署任何类别的扫描设备，就可以实现业务的安全扫描。

而另一种业务类型，则是不允许外网访问的，仅允许业务集群中的网络进行访问，比如数据库系统、ERP 系统等。这种类型业务的扫描类防护，其核心难点也就是如何保证扫描类安全设备如何与业务能够网络互通。通常可以采用两种方式来实现。（1）将虚拟化的安全设备实例与待防护系统部署在同一个虚拟的子网中，提供一个专属的管理网络，供安全运维人员对扫描器进行操作控制；（2）基于云平台内的虚拟网络，利用 VLAN、隧道或 SDN 技术，将部署在云上业务的网络与扫描器的网络实现互通。关于这一点，将在后文中做更为详细的介绍。



网关类服务

对于网关类的安全防护，如何有效的应对上述提到的三种不同层面访问流量的防护，成为了云安全设计的重要参考依据。

对于第（1）种流量类型。这种南北向的流量防护，在安全防护部署时相对简单，通常可以参照传统数据中心的安全防护部署方式，将安全设备部署在数据中心的入口，进行公网与内网之间的访问控制等防护。这里的安全设备既可以是传统的“硬件盒子”，也可以是虚拟化的安全设备虚拟机。

对于第（2）种和第（3）种流量类型，也就是东西向流量，传统的硬件盒子设备很难部署进用户的云平台内部，因此其对于东西向流量的防护显得有些吃力。通常东西向的流量防护有两种思路：一种是把安全设备放进云平台进行防护；另一种则是把云平台内部的业务流量导出来，经过安全设备的清洗后，再回注到云平台。

针对第一种防护思路，可以采用 NFV 的方式，将传统的安全设备进行虚拟化，把硬件盒子虚拟化为软件的安全设备虚机，将其与用户云平台内的业务统一部署在云平台中，通过云平台的网络规划，实现业务流量东西向的防护；

针对第二种防护思路，通常实现为安全资源池化的方式，将传统的硬件安全设备或者虚拟化的安全设备，组织成安全资源池，将用户云平台内的流量通过一定的技术手段，牵引到安全资源池内，安全资源池完成对其进行的安全防护之后，将流量再回注给云平台。

上述两种思路各有其利弊，很难说哪种方式更好，第一种思路将安全设备部署在了用户业务网络内部，与传统的部署方式很像，实现起来相对简单。但是其存在的问题在于，传统的硬件安全设备盒子无法继续使用，而且虚拟化的安全设备也要对各种各样的云平台进行适配，方案落地难度大，实现代价较大。而第二种思路，则有效的利用了传统的硬件安全设备，并且其部署方式也与云平台进行充分的解耦，降低了方案部署落地的难度。但是它存在的问题是，如何高效的将云平台内的流量进行动态的牵引，并且准确的进行回注。

弹性安全云

从上文的描述可以看出，无论是对于扫描类的安全防护还是网关类的安全防护，都可以采用独立于云平台的安全资源池技术来进行实现。这种池化的安全服务方式，我们将其称作一朵弹性的安全云。

安全云分布式的部署在用户云平台所在的每一个数据中心内部，实现安全防护的就近选择。这种弹性的安全云其好处主要在于：

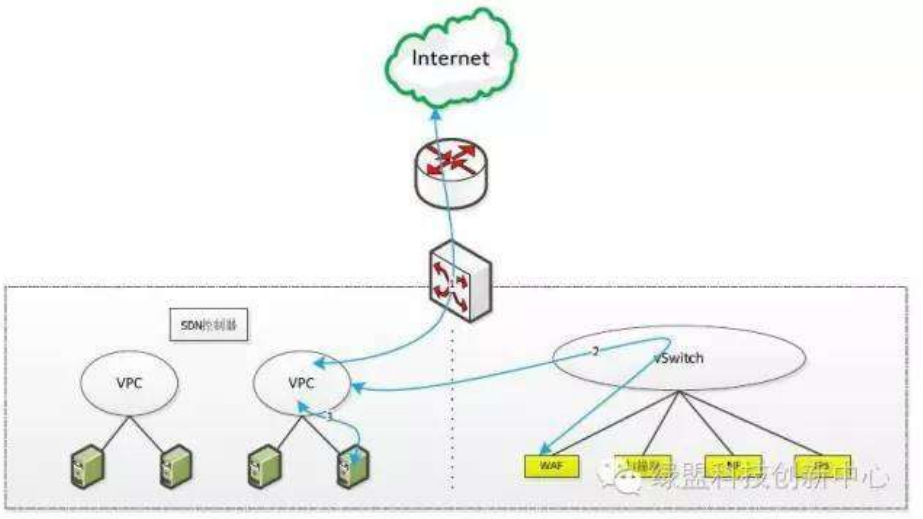
（1） 流量处理灵活。用户既可以实现南北向流量的安全防护，又可以实现东西向流量的防护。

（2） 与云平台解耦。安全设备的形态既可以是传统的硬件盒子，也可以是虚拟化的安全设备实例。设备部署不依赖于云平台，并且可以集成众多厂商设备，共同组成这朵安全云。

（3） 弹性扩充和收缩。由于安全云内部拥有众多的虚拟化安全设备实例，因此，可以根据用户防护任务的压力大小，动态的实现安全云朵的扩张与收缩。既满足的防护需求，同时又可以做到绿色环保。

（4） 负载均衡与高可用。弹性的安全云根据各安全设备负载大小，动态的对安全防护任务分布进行负载均衡，保证每一项防护任务的防护性能和防护效果。同时还可以据此实现防护服务的高可用。

（5） 安全服务编排。由于用户流量的安全防护均在安全云内进行，因此可以针对不同的流量特性，对其进行自动化的服务编排，实现多种安全防护的智能组合。使得防护更加精准与安全。

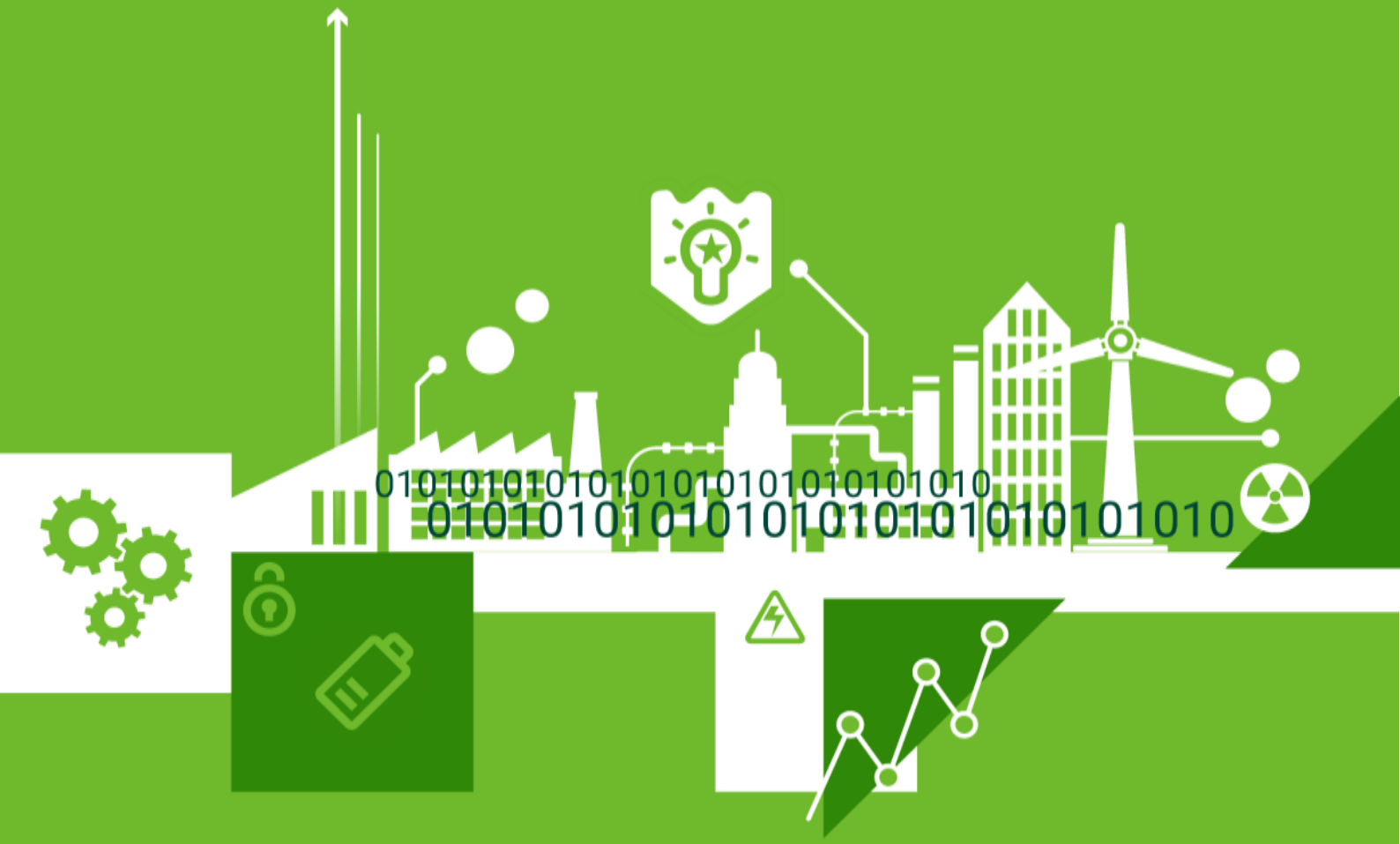


那么如何将安全云与用户的业务云进行整合联动，成为了这朵安全云存在价值的关键之所在。近年来，SDN 技术快速的发展与成熟，尤其是在云网络的管理和应用上，更是越来越普遍。SDN 的这种控制与转发相分离的网络架构，使得云平台内网络流量的管理变得更加的灵活。那么依托 SDN 这种天然的优势，可以动

态的将待防护流量牵引到安全云，安全云对其进行清洗完毕后，会将流量再送回至 SDN 网络，保证业务的正常运行。

如果云平台的网络没有 SDN，那安全云的防护方式是不是就不可用了呢。答案当然是否定的。如果没有 SDN，我们可以在云平台部署一个专属的引流代理，根据用户特定的防护需求，通过 VLAN 或隧道等方式将其牵引至安全云上进行防护。甚至可以将这个引流代理预先部署在用户云平台每一个虚拟机内。

四. 解决方案

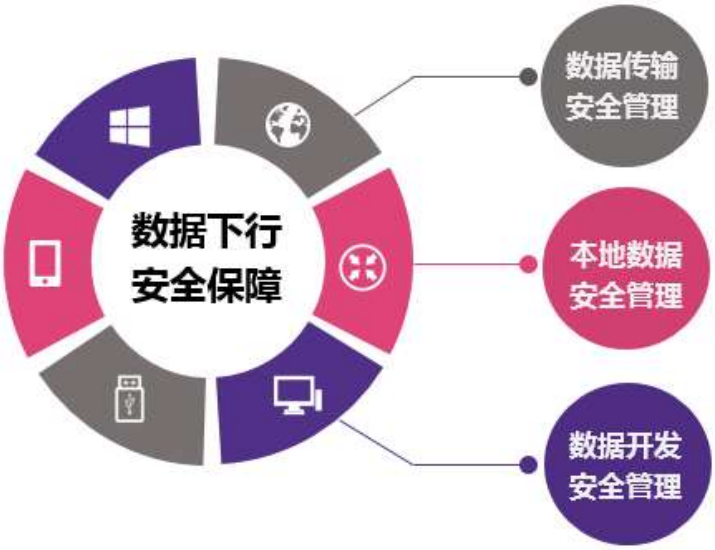


绿盟科技烟草行业数据下行和数据应用安全防护思路

国家烟草专卖局自 2013 年以来，开展面向全行业的行业卷烟生产经营数据下行服务，有力地支撑了行业的生产经营和决策管理。由于行业数据库级数据下行服务对于行业生产经营的重要性，因此对于数据下行安全保障的要求也越来越高，并逐步加强对下行数据安全管控的要求。

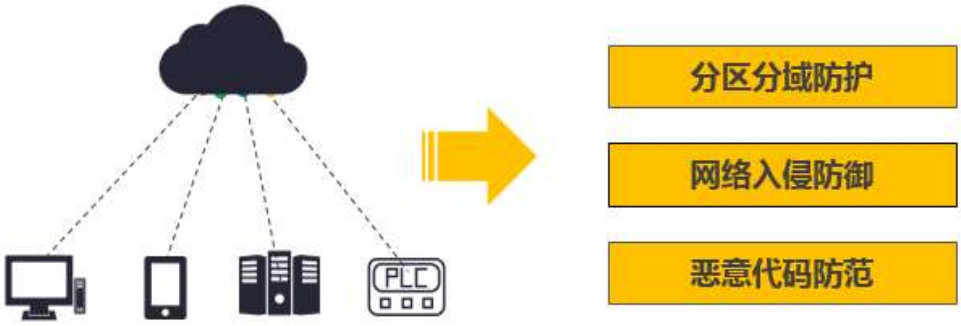
为确保行业生产经营数据安全可控，国家烟草专卖局发布了《关于进一步加强数据下行和数据应用安全的通知》（国烟信综〔2015〕35 号），要求行业各单位加强数据下行过程的安全管理，对网络环境采取入侵防护和实时监控措施，对接收数据库服务器配置安全防护策略，对下行数据做好本地安全管理和审计，对二次开发做好安全管理，并有针对数据下行的安全运维管理方案，确保数据下行过程中的数据安全。

针对行业提出的安全防护原则和防护要求，绿盟科技从数据下行过程安全管理、数据下行本地安全管理、下行数据应用开发安全管理等三方面进行分析解读，提出了针对每个阶段的安全防护方案。



数据下行过程安全管理

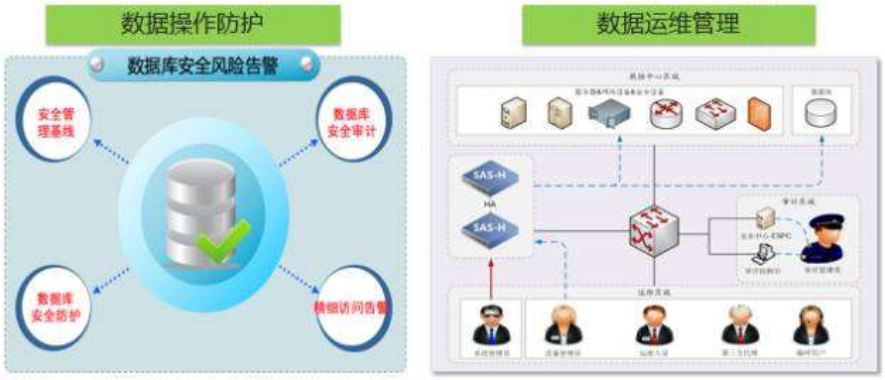
数据下行过程安全管理主要采用分区分域、网络入侵防御、恶意代码防御等防护手段。分区分域防护是数据库级数据下行过程安全防护的基础，可以将跟下行数据相关的业务系统，按行业要求划分单独安全域，并在安全域边界采取入侵防范措施，在发生入侵事件时能及时告警并实时阻断；同时加强网络恶意代码防范措施，做到对恶意代码及时检测和清除。



数据下行本地安全管理

数据下行本地安全管理主要通过安全管理基线、数据库操作防护、安全运维管理等方式进行。安全管理基线从端口、进程、账号、文件等维度对业务系统的正常工作进行检查；数据库操作可从审计和防护两方面

进行考虑；安全运维审计终端计算机的登录操作行为，对登录服务器的账户、操作行为进行记录，对审计进程进行保护，对审计记录进行保存。



下行数据应用开发生命周期管理

烟草行业数据库级数据下行服务的应用开发，特别是移动应用（移动 APP）等新型业务模式，在提升了业务便捷性的同时，也存在着下行数据泄密、开发应用系统安全性不足等安全风险，所以在对下行数据进行应用开发时，需要针对下行数据应用系统开发生命周期全过程进行安全评估，主要分为需求分析、设计阶段、实施开发、验证测试、发布阶段和维护阶段几个部分。

方案收益

综上，烟草行业数据库级数据下行安全防护方案旨在从数据下行过程安全管理、数据下行本地安全管理和下行数据应用开发生命周期管理三部分，通过分区分域、安全审计、安全运维、应用开发各阶段安全管理等途径，实现整体的针对数据库级数据下行安全立体防护效果。

获取详细的防护方案，请联系绿盟科技能源&企业事业部烟草销售部 68438880-6988

绿盟科技能源行业安全日志审计平台

作为一名能源行业的信息安全管理人员，你有没有被各种安全设备、服务器、网络设备的安全日志搞得焦头烂额？无论是要从各种日志中进行问题分析和定位，还是从日志中提取有用的信息，是不是都像大海捞针一样忙得筋疲力尽收获却总是寥寥？

而且，而且，你们单位里只有你一个安全管理员有木有？

单位这么多安全日志、设备日志，每天就好几万条怎么分析？

可是，今天集团总部又要安全检查了，重点要求设备安全日志检查，怎么办？

那么在日常工作中，信息安全管理员究竟会面临哪些安全日志审计的问题呢？

日志分散在各地

随着信息化技术的逐渐深入，企业往往采购了多种安全设备，软件、硬件、数据库等。这些设备和系统会分别分布在不同的网络位置，并各自产生日志，且每种安全设备，或网络设备，或者每个厂商都会有各自的控制台进行日志查看，无法集中；

日志格式不统一

每个厂商，尤其是安全设备厂商的每种日志类型的格式都不相同，并且表达着各自不同的意思。相同或相近的意义，会有千差万别的表述方式和格式，这使得管理起来，费时又费力；

日志量巨大

每个企业的核心业务都不同，导致保护核心业务的安全设备也多种多样，且为了保证从日志中发现威胁，安全设备往往会产生大量日志，且十分巨大。如今大型的能源企业，日志量是可观的，已经达到 TB 级或更高。对于审计人员来说，如此大量的日志，是无法有效运维的；

日志无法有效查询

如今的企业，日志审计产品大多以应对等保检查为主，但是上级单位在发现安全威胁和异常时，要求企业进行审计或者追踪威胁时，传统的日志审计系统却无法有效查询或者追溯；

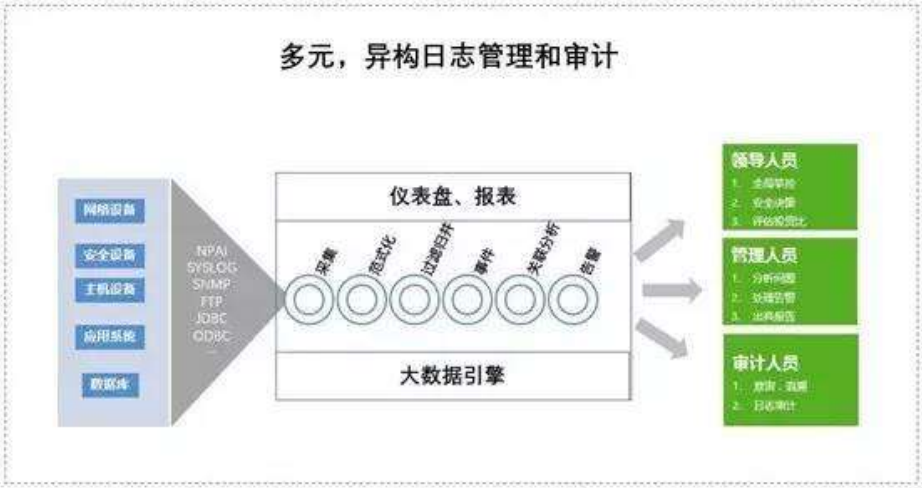
管理职责不明确

日志应该被哪个部门管理？告警由谁来负责和处理？这是个无法界定的难题。网络设备日志应由运维部门监管，但是信息安全部门在进行安全分析时，需要一定的网络设备支持，更不用说服务器和应用系统日志了；

如果想解决以上问题，需要一个具有处理海量日志的平台或系统来为安全追溯和审计工作提供技术上的支撑。它要能够应对分布在多个网络的日志进行统一收集和管理。对日志格式不仅范式化描述，为了便于安全分析，对一些日志进行强化处理，增强日志的健壮性。还要能对存下来的日志进行有效查询。另外，能够按照用户的角色进行职责界定。最终实现对企业日志的集中化存储、分析、审计和展示。

为解决以上问题，绿盟科技推出多元，异构日志治理整体解决方案（以下简称 NESP），犹如一把利器，让你管理日志游刃有余。

该方案基于成熟的大数据技术，通过主动与被动相结合的方法，实时地采集用户网络中各种不同厂商的网络设备、安全设备、主机、操作系统、以及各类应用系统产生的日志，并将这些信息汇集到安全中心，进行集中化存储、备份、查询、分析、告警和审计，并出具丰富的报告，实现企业日志的全生命周期管理。



- ***超高性能的技术架构***

未来应对企业产生的海量日志，NESP 采用了大数据架构，使得系统在日志采集，存储，分析等方面得到了极大的提升，足以应对 PB 级的日志量。

恰到好处的日志范式化与分类

NESP 对收集的各种日志进行范式化处理，将来自不同设备和系统的各种不同的表述的日志进行规范化描述，范式化字段不超过 60 个，既能满足复杂分析和存储的要求，又极大的提升了查询性能。

集中化的日志查询和审计

NESP 为客户提供了监视仪表盘，可以在一个屏幕中查看不同类型的日志，并以折线图、占比图，统计图等。用户可以自定义仪表盘，按需设计布局，可以为不同角色的用户建立不同维度的仪表盘。

系统提供了日志查询功能，用户可以制定查询策略，针对范式化后的日志或者原始日志进行综合条件查询和模糊查询。

系统提供了规则关联引擎，可根据业务要求自定义安全分析模型，极大的提升了日志的分析深度与安全事件的识别度。

丰富灵活的报表

报表是日志审计系统的必备功能之一。基于 NESP 的报表引擎，可以生成各种报表，客户可根据自身需要生成日报、月报、季报等，并支持邮件方式传递。支持 PDF、WORD、HTML 等格式的报表。

完备的安全性设计

NESP 系统具有良好的自身的安全等级设计。系统的自身安全性体现在：

日志采集器与分析中心之间支持加密通讯

日志采集器支持存储转发

浏览器访问支持 HTTPS 协议

采用基于角色的访问控制机制

用户身份三权分立，内置系统管理员、审计管理员、用户管理员

灵活的业务扩展

平台在日志管理的基础上可以进行无缝扩展，如：资产管理、脆弱性管理、威胁管理、安全态势感知、攻击链条分析、安全运维管理等。根据业务需要进行安全业务拓展，最终实现企业安全管理的最终目标。

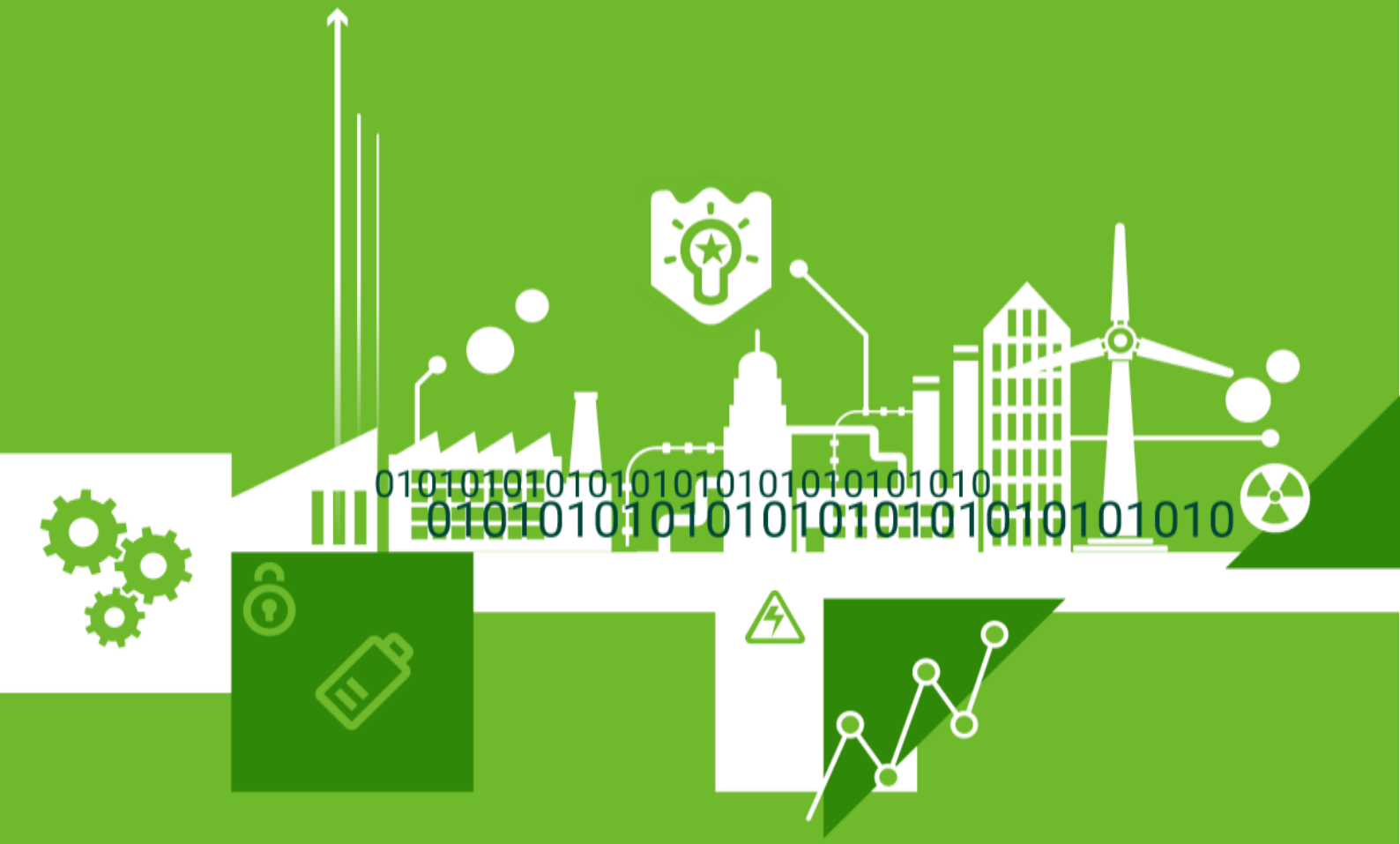
全自动的日志审计平台让你轻松完成安全日志存储、查询、展现的工作；

单位再多安全日志、设备日志，也轻松处理了；

领导再也不用担心日志审计这一项会扣分了~

获取详细方案请联系绿盟科技能源&企业事业部，联系方式：010-68438880-6964

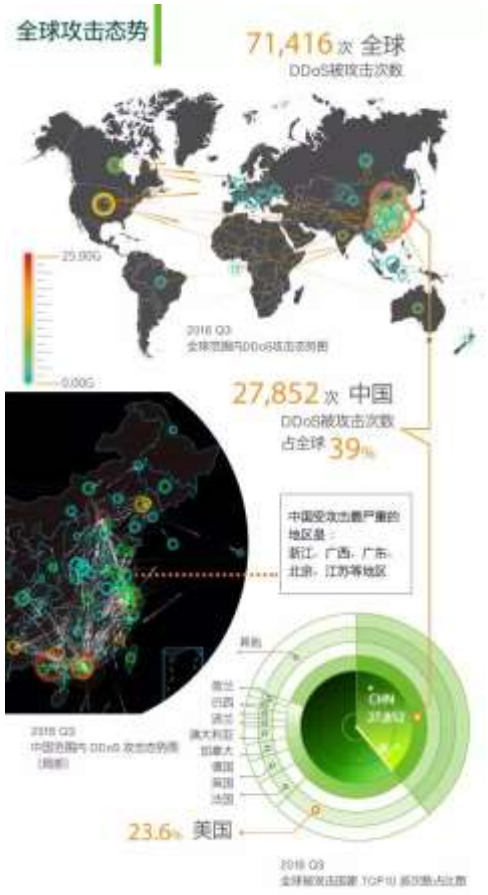
五． 绿盟科技动态



产品及服务动态

绿盟科技 2016 Q3 DDoS 态势报告

DDoS 攻击是在众多网络攻击中一种简单有效并且具有很大危害性的攻击方式。据绿盟科技全球 DDoS 态势感知平台监控数据分析显示，Q3 发生 DDoS 攻击事件明显上升，平均攻击峰值达到 19.4G，物联网设备成为黑客僵尸网络的新宠，总体攻击态势十分严峻。



绿盟科技工业防火墙--专注工控系统边界防护 精准助力能源安全

随着工信部有关《工业控制系统信息安全防护指南》的发布，工控安全又被提升到了一个新的高度。指南指出工业控制系统应用企业应从十一个方面做好工控安全防护工作，作为工控安全防护重要环节的边界安全在指南的第三大点进行了重点阐述，特别指出工业控制网络与企业网或互联网之间的边界应通过工业控制网络边界防护设备进行安全防护，通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。可以看出，作为边界防护的重要安全设备工业防火墙，在企业工控安全防护中起到了至关重要的作用。

作为工控安全先行官的能源行业早在 14 年就由国家发改委发布了《电力监控系统安全防护规定》对电力企业工控系统的安全防护进行了规范，15 年初国家能源局又发布了国能安全 36 号文进一步对电力企业工控安全进行了合规性阐述，提出了针对省调、地调、配电网、发电厂、变电站的安全防护方案和安全评估规范。无论是 14 号令还是 36 号文都对电力企业的工控安全防护起到了较强的推进作用，发文在“安全分区、网络专

用、横向隔离、纵向加密”的十六字方针的基础上对边界安全进行了强化，在控制区与非控制区边界安全子项中规定安全Ⅰ区与安全Ⅱ区之间应当采用具有访问控制功能的网络设备、安全可靠的硬件防火墙或者相当功能的设备来实现逻辑隔离、报文过滤、访问控制等功能；在系统间安全防护子项中规定同属于安全Ⅰ区或安全Ⅱ区内部的不同系统之间，根据需要可以采取一定强度的逻辑访问控制措施，如防火墙、VLAN 等进行逻辑隔离。这些安全防护场景均可以通过工业防火墙的部署来满足安全防护要求，从合规性与刚需两个方面做好电力企业工控系统的安全防护。

在石油石化领域，中石油、中石化发布的“十三五”发展规划中也明确了工控安全的重要性。比如油化行业的油田工业控制网络是覆盖油田生产现场（井口、站库、管线等），用于生产数据实时采集和进行远程控制、自动控制的网络。其覆盖范围广，很多设备部署在野外，并采用光缆、无线等多种组网方式，因此容易受到来自外部的搭线攻击。确保工业系统运转安全是油田工业控制网络安全的根本，因此如何防范针对业务信息，特别是指令信息的窃取、破坏、篡改，防止恶意代码或黑客从远程设备和内部局域网终端对油田工业控制网络的其他设备进行攻击，是油田工业控制网络安全需要重点解决的问题。这些迫在眉睫的信息基础设施存在的安全隐患也都可以通过工业防火墙的部署来进行安全保障，确保油田工业控制网络安全平稳高效的运行。

那么什么是工业防火墙，工业防火墙的应用场景都有哪些呢？下面小编就为大家简单介绍一下吧。

什么是工业防火墙？

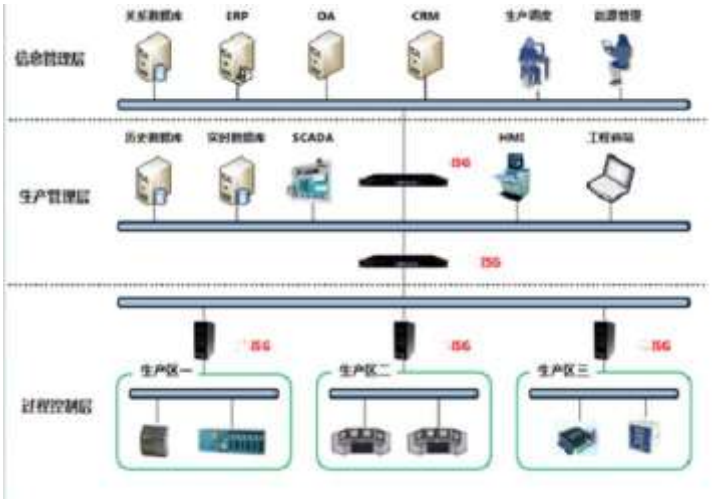
为了提高安全防护能力，传统防火墙在发展过程中不断的添加新的功能，但是防火墙的安全性与其速度、功能成反比。防火墙的安全性要求越高，需要对数据包检查的项目（即防火墙的功能）就越繁杂越精细，对 CPU 和内存的消耗也就越大，从而导致防火墙的性能下降，这一点与工业网络对于实时性的要求是相背离的。

绿盟科技的全新产品工业防火墙定位于帮助工业企业用户对来自网络的病毒传播、黑客攻击等攻击行为进行过滤和防护，避免其对工业控制网络的影响和对生产流程的破坏。不但支持传统防火墙的基础访问控制功能，更重要的是它提供针对工业协议的深度过滤，实现了对 Modbus、OPC 等主流工业协议和规约的高细粒度的过滤，针对工业网络协议的内容和数据进行细致的合规性检查。例如：绿盟工业防火墙的 Modbus 协议管控模块可以针对 Modbus 协议的设备地址、寄存器类型、寄存器范围和读写属性等进行检查。通过类似的管控模块能有效的防范各种非法的操作和数据进入现场控制网络，最大限度地保护控制系统的安全。

工业防火墙都用在哪？

安全区域之间的访问控制和安全防护

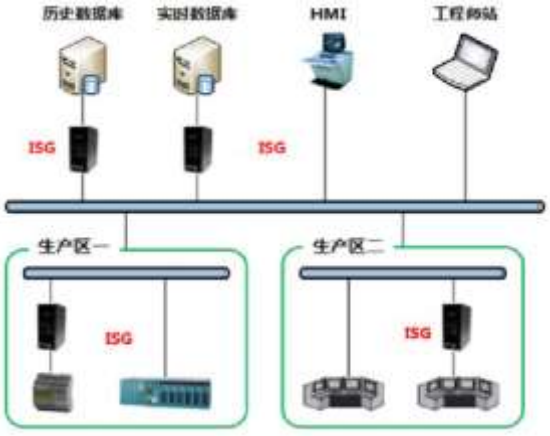
在纵向不同层次网络之间部署防火墙，控制跨层访问并对层间数据交换进行深度过滤，防止攻击者通过上层网络向下层网络的渗透和攻击。



在同层次中平行的厂区、工艺流程和业务子系统之间部署防火墙，将它们分割成不同的安全区域，控制不同安全区域之间的访问，并对区域间数据交换进行深度过滤，减少区域之间安全问题的扩散和影响。

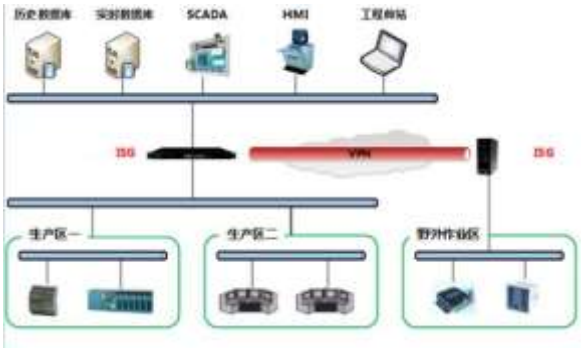
重点设备的安全防护

在重点设备的前端部署防火墙，限制可以访问它的 IP 地址、屏蔽非业务端口访问、过滤非法的操作指令、记录所有的访问和操作，对其进行全面的安全防护和审计。



分散工业网络的安全互联

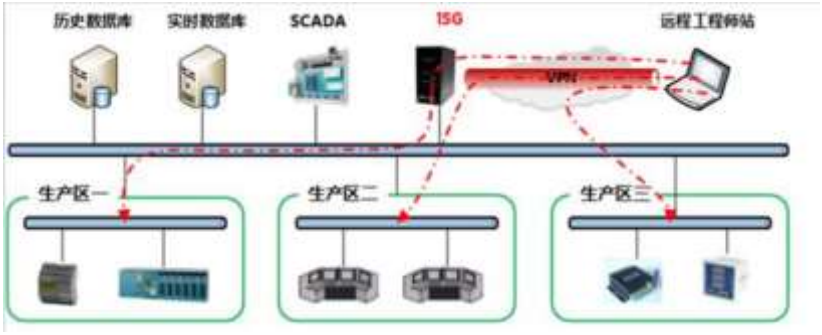
对作业区内部的工业网络进行安全保护，阻断来自公用网络的攻击，实现作业区网络的边界安全防护。



使用 VPN 对作业区与调度中心之间的数据传输进行加密和保护，搭建安全的数据交换通道，解决两者之间的数据传输安全问题。

安全的远程维护

在工业网络与公用网络接口处部署防火墙，并启用 VPN 功能，将其作为远程维护的堡垒设备。远程维护人员使用 VPN 连接到防火墙上，一方面进行身份认证，另一方面对通过公用网络完成的远程维护操作进行加密保护，实现安全的远程维护。



总结

随着网络信息时代的到来，我国工业模式发生了翻天覆地的变化，未来将彻底打破了“信息孤岛”模式，能源相关企业全面联网，生产数据轻松实现汇总分析，不但提高了生产效率，还达到了节能减排的目的。信息化给能源企业带来的有利变化显而易见，但随之而来的网络安全问题又使人为之惊慌。

在能源企业的工业网络中，运行着 DCS、PLC、SCADA 等各种过程控制系统，它们往往是生产系统的核心，负责完成基本的生产控制。工业防火墙可以切实保障核心生产控制系统的网络安全，在不影响工业生产实时性的同时保护工业网络数据的安全传输。避免过程控制系统遭受入侵破坏对工业生产造成的影响。

获取详细方案请联系绿盟科技能源&企业事业部，联系方式 010-68438880-6071 或 前台转接能源&企业事业部。

市场活动动态

绿盟科技专家现场“解密运维保障之道”

2016 年 11 月 26 日，绿盟科技受邀参加广州的互联网技术沙龙，绿盟科技专家做了主题为“解密互联网抗 DDoS 攻防之道”的演讲，并指出利用抗 D 混合清洗方案，进行本地及云端清洗的无缝协同，是互联网抗 D 的关键。来自网易、腾讯、唯品会、魅族等企业在内的互联网客户也发表了各自的见解。

伴随着互联网时代的到来，各类网络安全问题愈发引起各行各业的关注。当受到流量大、频次高、可持续的 DDoS 攻击时，缺少专业安全运维人员的企业客户都面临着极大的安全挑战。为此，可靠的安全设备和专业的安全运维人员成为网络安全保障必不可少的因素。此次技术沙龙邀请到了来自广州和深圳区域的网易、腾讯、唯品会、魅族等企业在内的互联网客户，针对网络安全和运维保障，各家都发表了自己的见解。

会上，绿盟科技专家阐述了 DDoS 攻击近年来流量变大、频次高发、情况复杂化，且形成产业化的趋势，分析了行业客户在抗 D 方面面临着的重重困难。对此，绿盟科技的抗 D 混合清洗方案将本地清洗和云清洗连接起来，有效应对 DDoS 攻击，切实解决客户难题。多年来，绿盟科技信息安全产品及服务在市场上始终一枝独秀，在 2014 年亚太区 DDoS 市场份额排名中，绿盟科技以国内第一，亚太区第四的成绩向客户交出了满意答卷。专家指出：云清洗是应对大流量 DDoS 攻击的关键手段，联合抗 D 才是最行之有效的方法。

绿盟科技作为信息安全领域的领军企业，不仅重视技术创新，更加注重与各行业间的沟通与交流。在快节奏的互联网时代浪潮中，把握客户的真正需求，切实解决客户难题，提供优质可靠的安全运维服务，是绿盟科技 16 年来不懈追寻的目标。面对新的挑战，绿盟科技会秉承“专攻术业成就所托”的愿景，为互联网安全做出新的贡献。

加强安全监控平台建设 推进智慧企业创新管理

12 月 12 日，以“推进管理创新，打造智慧企业”为主题的“首届智慧企业创新发展峰会”在成都世纪城国际会议中心圆满召开。大会吸引了来自政、商、学、研、企等不同领域的 500+代表参与，更有专家学者、行业领袖、企业家代现身说法，探讨和分享“智慧企业”建设理论和实践经验。绿盟科技做为国内安全行业领军企业积极参与了本次大会，绿盟科技安全专家在会上发表了题为“加强安全监控平台建设，推进智慧企业创新管理”的主题分享。

本次活动由四川省企业联合会、四川省企业家协会联合主办，旨在激励传统企业向智慧型企业转型，并围绕智慧企业建设理论与实践以及企业提质增效、自主创新的转型升级路径等热门话题进行了深入探讨。峰会还特别邀请到中国工程院 3 位院士莅临会场作精彩演讲，为推动“智慧企业”建设，促进企业管理创新指点迷津、出谋划策。

中国工程院院士潘云鹤指出，我国企业正处于信息化和工业化相融合阶段，需要通过创新来引领企业的发展。因此，要借鉴“智慧城市”已经确定的理论和实践成都，在智慧企业建设的“智能”上下功夫，沿着“管理数字化-信息网络化-决策智能化“的进程不断发展。

而健全的网络安全环境不仅为进一步推动“智慧企业”建设工作提供了有力保障，更像是一剂强心剂，为促进企业可持续发展创造了必要条件。

最近几年，伴随物联网、大数据、云计算等新技术广泛应用，全国乃至全世界都掀起了一波智慧创新的浪潮，与此同时，安全行业发生了深刻的变化。

绿盟科技安全专家指出，企业目前面临的威胁不仅传播速度更快，其所利用的攻击面也越来越宽广，覆盖移动、桌面、网络、Web 和各种应用、社交网络等。在这一态势下，一方面企业应急响应的时间窗口越来越小，另一方面企业应急响应所需的知识、专业技能、技术手段等却不断增加。基于此，专业化、系统化、自动化等安全平台特性显得尤为重要，大规模的安全情报系统和专家社会网络系统相互融合，“云地人机”协同作战将会成为网络安全应急响应的新常态。

云

绿盟科技云端安全能力，通过云端预警，7×24 小时云监测等服务，可对监测站点进行平稳度、敏感内容、篡改情况、网速、关键字的监测 ，并通过结合运营商云平台抗 DDoS 集群组对来自互联网大流量的攻击进行牵引清洗。

地

绿盟科技独有的攻防平台，结合企业安全中心 ESPC 和大数据态势感知平台 BSA，对各种资源进行态势感知和信息采集，综合分析用户即时的网络安全态势。

人

绿盟科技专业技术服务团队，绿盟科技通过绿盟云专家、绿盟本地专家及值守运维人员的专业服务，对网站运行情况及设备的运维情况进行实时的监控，并在网站上线前，对网站进行了充分的渗透测试。

机

客户部署的安全设备，主要负责防护网站的安全，充分保障客户网站的正常运行。

绿盟科技安全专家强调，为了切实保障物联网安全，需要国家、企业、安全服务提供方的通力协作。国家层面，已经出台相关法律法规对互联网管理、应用设备的生产标准等进行一定的安全规范；从企业层面，应当强化安全监控平台建设、及时升级安全保护技术与机制；像绿盟科技这样从事安全服务提供方层面，应当强化风险监控体系、风险防御机制以及风控技术建设，帮助企业建立起 “即时、快速、有效”的应急响应体系。