电力系统外网一种控制个人移动设备的网络准入实现

母继元
(广元电业局,四川 广元 628000)

摘 要: 通过分析新形势下电力系统外网个人移动设备接入的特点,对传统的两类准入控制方式进行了探讨,并结合四川广元电力ASM准入平台的实例提出了一种更适合移动设备接入管理的网络准入实现方式。

关键词: 网络准入控制; 策略路由; 802.1x; web重定向; DAI

Abstract: The characteristics of BYOD (bring your own device) are analyzed when accessing to the external network of power system and two traditional network admission control (NAC) techniques are discussed. Based on the actual example of ASM NAC platform in Guangyuan power system, a more effective NAC implementation for mobile devices accessing in management is put forward.

Key words: network admission control (NAC); policy-based route (PBR); 802.1x; web redirection; dynamic ARP inspection (DAI)

中图分类号: TM732 **文献标志码:** B **文章编号:** 1003-6954(2012)04-0053-03

随着电力系统信息化建设的不断发展,其网络规模也在不断扩大,随之而来的各种安全问题也日渐突出,尤其是网络内部的接入计算机或接入设备往往成为威胁的源头。目前电力系统外网管理中较为普遍的安全问题包括:①无法发现是否有非法用户进入外网占用网络资源;②无法对入网人员进行身份验证,进而无法统计入网的员工数量和每日的来宾数量;③无法控制来宾用户的访问权限;④无法要求所有终端遵守电力系统外网管理的基本安全规范,如安装杀毒软件、必须运行某些程序,必须更新windows操作系统补丁等。

为了解决上述问题,在部分电力系统中目前采用了较为流行的网络准入控制(network access control,NAC)来防止非法用户入网。网络准入控制方案可以只允许合法的、值得信任的端点设备(例如PC、笔记本)接入网络,而不允许其它不符合要求(未通过认证、安全性不符合要求等)的设备接入。但随着消费化电子浪潮的影响,在电力系统内购买和拥有最新型的个人移动设备的趋势(bring your own device,BYOD)日益增长,包括iphone、ipad、android等各种系统都已经频繁出现在电力系统外网的日常接入中,在这样的新形势下,传统的网络准入技术由于响应速度慢或者需要安装客户端等问题已经无法满足日益发展的安全需要。通过传统准入方式与四川广元电力所采用的一种新型准入平台的比较,希望能够为电力系统外网个人移动设备的管理提供一种更具通用性、更有效的网络准入实现方法。

1 电力系统外网传统准入控制方式的弊端

目前电力系统外网中比较常见的防止非法接入的网络准入方式有如下两种。

传统技术1: DHCP结合IP-mac绑定的控制方案

由于在电力系统外网中大量采用了DHCP的IP地址分配方式,因此较多单位在初期考虑实现准入控制的时候也是以DHCP为出发点的。当网络中假设好了DHCP服务器后,可以依据入网的mac地址来自动分配IP,而为了防止私自更改IP及网络中出现非法的mac地址接入,则需要借助交换设备已有的一些安全属性如DHCP snooping和DAI(dynamic arp inspection)来实现IP-mac绑定。而采用DHCP结合IP-mac绑定的控制方式,其本质是基于mac地址也即是设备硬件地址的,对于目前电力系统外网的安全接入规范要求以及个人移动设备接入的管理而言,具有较多的安全管理弊端。

1)没有对使用设备的人员进行身份认证的步骤;

2)命令配置量过多,对技术运行维护人员的要求较高,网络中很多早期的交换设备并不支持DAI

技术，在实际使用中的适应性和可推广性较差；

3) 对于外来需要入网的移动设备，比如来宾设备或员工自带的移动设备(BYOD)，无法预先做到mac绑定，因此很难快速响应入网请求，这就极大地影响了工作业务的开展，很多电力单位因为这个原因停用了DHCP结合IP－mac绑定的准入；

4) 由于全部管理都是采用交换机静态命令行的方式进行配置的，在大量个人设备经常性移动办公或入网的情况下，无法预先灵活地设置例外设备，或依据权限或用户的变化自动调整安全策略，telnet到交换设备进行变更时响应的效率非常低。

5) 整个技术本身并没有提供进行设备安全性检查的实现方法，这一点就容易导致很严重的潜在安全漏洞，对于电力系统外网用户而言，由于大部分的设备都是与公网直接相联的，尤其是在大量个人移动设备入网的情况下，安全性一旦无法得到有效评估，对于整个系统的安全管理将可能产生严重的后果。

传统技术2：标准IEEE 802.1x方案

802.1x称为基于端口的访问控制协议(port－based network access control protocol)，IEEE 802.1x技术由于是国际标准协议，因此大部分的主流厂商接入层交换机都能够予以支持，并且在目前的电力系统外网中也得到了部分应用，但随着安全趋势的不断发展，802.1x体系也逐渐显示出了无法满足个人移动设备逐渐增多的安全管理问题。

1) 安装客户端软件来实现准入控制的方式在应对个人移动设备接入时可用性差，基本上没有可操作性；

2) 电力系统外网在很多单位都存在hub接入的问题，但是由于交换机设备对802.1x支持的固有特性，大部分单位无法做到802.1x与hub接入共存；

3) 命令配置量过多，每台交换机上的配置量比前一种传统准入技术还要多，对技术运行维护人员的要求较高；

4) 无法预先灵活地设置例外设备，或临时调整安全策略。在个人移动设备经常性移动办公或入网的情况下，无法依据需要对特殊设备临时放开802.1x端口，任何人、任何设备都必须安装客户端、必须认证的管理策略在众多个人移动设备入网的环境下很难真正应用起来。

5) 与第一种传统准入技术相似的是，整个802.1x技术本身并没有提供具体的进行设备安全性检查的实现方法，同样容易导致很严重的潜在安全漏洞。

综上所述，在当前多样复杂的电力系统外网接入环境中，有必要采用更新型的网络准入实现来解决大量个人移动设备接入的问题。

2 一种新型准入控制方式在电力系统外网的应用

依据目前在四川广元电力公司外网中采用的部署实例(如图1所示)，可以提供一种更有效的新型准入控制实现，并更好地满足当下电力系统外网接入的特点。

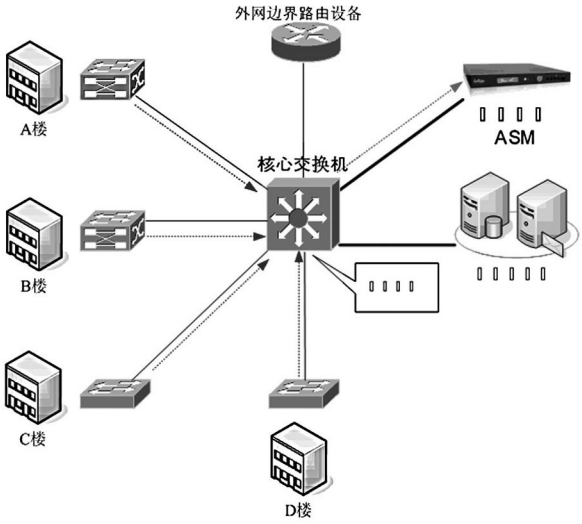

图1 四川广元电力外网准入部署示意图

在该准入部署方式中，采用了杭州盈高科技有限公司的准入平台ASM(入网规范管理系统)，准入设备ASM采用旁路方式接入到电力外网核心交换机上，并且在核心交换机上利用通用的策略路由(PBR)来实现3层引流。

(1) 广元电力外网准入方案的实现方法

策略路由PBR由于位于IP层，在做IP转发前，如果报文命中某个策略路由对应的规则，则要进行相应的策略路由的动作。在广元电力中采用的基于策略路由PBR的准入方案是在核心交换机上利用ACL捕获所有访问核心业务服务器以及外网的无差别数据流量，并通过已经配置好的route－map将捕获的流量引入网络中的ASM准入设备，最终由ASM准入设备来控制所有需要访问核心交换机后资源的数据流量，采用web重定向的方式推送认证和安全检查页面到用户的接入设备上。这种对于无差别流量的控制，其设计思路就在于各种个人移动

设备，不管是 iphone、ipad 还是 android 等非 windows 系统都自带了 web 浏览器，能够支持 http 协议，因此实现了既不需要安装客户端，又能够保证身份认证和安全检查的双重保护目的。

(2) 广元电力外网准入方案的管理流程

①各种个人移动设备及内部台式机在接入外网时，自动在 web 页面上获得入网的提示，并且必须通过管理员的审核；

②各种个人移动设备及内部台式机在 web 页面上进行身份认证，可以设置来宾设备或特殊设备不需要进行身份认证，但只授予有限访问区；

③可以在接入设备入网前检查其是否安装杀毒软件、是否运行了必须的程序，以及是否更新了系统补丁(windows 设备)；

④入网后能够依据用户的认证角色派发其访问权限，例如只能访问特定服务器，非管理员允许不能访问其他网络资源。

(3) 广元电力外网准入方案的应用效果

广元电力中利用 ASM 平台实现的准入控制方案，能够很好地区分外网中来自不同部门的终端设备及来宾设备，并能够针对 iphone、ipad、android 等非 windows 系统实现全面的身份认证和访问权限控制，禁止所有非法外来设备接入内部网络，使电力系统外网的安全管理制度得到了有效落实。同时，外网的管理员能够及时了解新设备的入网情况，并控制各个部门以及来宾用户的访问权限，有效落实了电力系统外网的安全管理规范，对网络中的许多安全风险都进行了预防和告警，对网络的正常运行提供了十分有效的安全支撑。

(4) 新技术在电力系统外网接入中的应用优势

依据对广元电力外网准入方案的分析，可以看到该新型准入控制方案对其他电力系统外网移动设备接入管理的建设具有很高的参考价值，有如下优势。

①完全不需要安装客户端软件。由于该方案中的认证是通过 web 重定向实现的，因此全部的认证过程都只需要接入设备有支持 http 协议的浏览器即可，在这种情况下，目前电力系统外网中接入的 iphone、ipad、android 等非 windows 系统都可以有效地利用自带的各种浏览器来自动实现认证，入网快速，完全不需要管理员额外的干预，能够节约外网管理员的大量时间和人力成本，更符合新形势下电力系统外网个人移动设备接入管理的需要；

②由于策略路由技术是基于三层交换的，因此不会与接入层的 hub 连接产生冲突，电力系统外网中已有的 hub 设备可以与准入平台共存，更有利于准入管理的推广，整个技术实现也更贴近实际情况，在目前的网络环境下更为实用；

③命令配置量极少，只需要在核心交换机上配置策略路由即可。对于目前电力系统分布较为广泛的外部网络而言，可以节省大量的配置和实施工作量。

④在该方案中，可以非常灵活的通过 ACL 来控制哪些终端需要受管理，哪些终端是可以例外的，外网管理员可以实现非常灵活的管理效果，比如对内部员工机器进行较为严格的限制，而对部分特殊机器放开网络；

⑤可以灵活地在 web 页面就实现对设备的安全状况检查，这一点完全弥补了电力系统中已有的传统准入技术重认证轻安检的缺陷，能够迅速收集外网中全部个人移动设备的安全信息，并依据管理员预先制定的安全策略自动下发到个人移动设备上，实现权限的有效分配，并自动将高危设备置于外网预先设定的有限访问区内，从而实现了入网安全和主动防御的措施。

3 总 结

总体来看，目前电力系统外网新形势下个人移动设备接入管理的需要决定了必须改变传统思路，采用更新型更有效的准入管理方式，针对个人移动设备轻便、灵活、快速的特点提供响应速度更快、策略更灵活和更高效的准入控制功能，这样才能够为电力系统的信息安全管理提供更具可操作性的解决方案。

参考文献

[1] Tanenbaum A. S. 计算机网络[M]. 北京：机械工业出版社，2011.

[2] Yusuf Bhaiji. 网络安全技术与解决方案(修订版)[J]. 北京：人民邮电出版社，2010.

[3] 何俊. NAC 准入控制指南[R]. 盈高科技，2012.

(收稿日期：2012－05－29)