



电力 PTN 设备网管安全性

刘昀¹, 刘国军², 任建伟¹, 李坚³

(1. 国网冀北电力有限公司信息通信分公司, 北京 100053;

2. 全球能源互联网研究院, 北京 102209;

3. 国网冀北电力有限公司, 北京 100053)

摘要:为解决电力应用的 PTN 设备网管系统易受攻击与脆弱性问题, 在研究 PTN 设备网管系统体系结构的基础上, 针对电力 PTN 设备网管系统面临的风险因素, 从经济性、安全性、运维效率方面提出了基于 MPLS-VPN 电力数据通信网的设备网管系统网络部署方式, 给出省、地市、县 3 级 DCN 带内与带外相结合的 DCN 网管安全部署方案。最后, 给出了 PTN 设备网管系统与其他系统交互的边界安全防护方案。

关键词: PTN; 设备网管; 安全性; 电力通信

中图分类号: TN914

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2015382

Equipment network management security of electrical power PTN

LIU Yun¹, LIU Guojun², REN Jianwei¹, LI Jian³

1. State Grid Jibei Information and Communication Company, Beijing 100053, China

2. Global Energy Interconnection Research Institute, Beijing 102209, China

3. State Grid Jibei Electric Power Company, Beijing 100053, China

Abstract: In order to solve the problem that the power PTN equipment management system vulnerable to be attacked and vulnerability, the risk factors of electric power PTN equipment network management system were proposed based on the architecture of PTN equipment network management system. From the factors of economic, security and maintenance efficiency, the network deployment of equipment network management system based on MPLS-VPN power data communication network was proposed. The out-band and in-band DCN security deployment plan of province-level, city-level and country-level was put forward. Finally, the boundary security program was proposed for the interaction between the PTN equipment network management system and other systems.

Key words: packet transport network, equipment network management, security, power communication

收稿日期: 2015-09-08; 修回日期: 2015-12-13

基金项目: 国家电网公司科技项目“电力分组传输网安全及 IPv6 可信通信网络研究”(No.SGRITKJ[2015]406)

Foundation Item: The Science and Technology Project of State Grid Corporation of China “Research on Security of Power Packet Transport Network and IPv6 Trusted Communication Network”(No.SGRITKJ[2015]406)



1 引言

随着智能电网、云计算、大数据等技术在电网的大力推进与建设,电力通信网承载的电网业务逐渐呈现出“宽带化、网络化、IP化、多元化”的趋势。除传统的电网调度业务外,更多的电网生产、经营、电网智能化、增值业务将由电力通信网承载,这对电力通信网承载能力、业务接入的灵活性、业务差异化服务水平及电力通信网管控能力提出了更高的要求。传统的MSTP技术对数据业务突发性和灵活性的适应性越来越低,而传统的面向非连接的IP网络,由于其难以严格保证重要业务的运行质量和安全性要求。PTN技术对于IP大颗粒业务的传输弥补了原有SDH网络的不足,是SDH网络的良好补充,也使得该技术在电力行业逐步得到试点与应用。

PTN设备网管系统作为PTN系统的重要支撑,实现了PTN的实时监控、配置管理、故障管理与性能管理等功能。相对于PTN设备后门与漏洞攻击、光缆线路可靠性问题,PTN设备网管系统在DCN、主机终端、数据存储与备份等方面更易遭受攻击。本文拟重点研究PTN设备网管的DCN的网络安全、边界安全问题,其他主机终端安全、数据安全依据相关电力二次系统安全防护的相关规定。

目前在PTN与网管系统安全性方面的研究如下所示。

- 参考文献[1]针对电信DCN的需求,给出了带内、带外及双平面带外3种系统设计方案以及防火墙与网管系统的设计思路,以提高整体电信网络的安全。
- 参考文献[2]提出了一种基于信息安全和风险管理提升网管系统的安全管理及安全维护水平的方法。
- 参考文献[3]针对PTN在电力通信网中的组网策略研究,提出了采用MSTP和PTN双平面组网方式保障电力骨干四级通信网的安全可靠性。

2 PTN网管系统概述

与SDH网络管理体系结构类似,PTN管理体系结构包括PTN NMS、PTN EMS和各厂商PTN子网,如图1所示。其中,PTN子网为各厂商的PTN网元或PTN子网,PTN EMS为各设备厂商网元管理系统,PTN NMS为网络管理系统。

根据PTN分层结构(信道层、通路层、传输媒介层)和

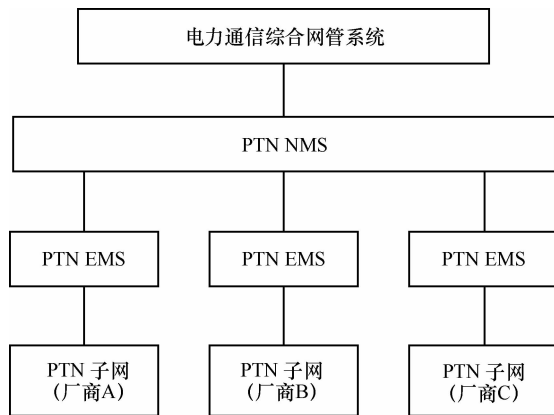


图1 PTN网络管理体系结构

设备功能,PTN设备网管系统主要功能包括拓扑管理、虚通道和虚通路管理、端到端业务管理、QoS管理、OAM管理、保护管理、同步配置管理和DCN管理功能^[4]。

3 风险分析

从PTN网管系统的安全接入、数据存储、DCN、外部互联、运维管理等方面,存在的安全风险主要包括以下几方面。

(1)DCN风险

PTN网管的DCN涉及带外DCN和带内DCN两种,其中带外DCN对网关网元的生存性要求较高,通常采用主备网关网元配置方式,否则会因网关网元的故障造成其他非网关网元无法被监控与管理。PTN的带内DCN与SDH差别较大,SDH技术在设计时就单独预留了管理开销用于网络管理(DCC专用通道),PTN的带内DCN组网需要为DCN消息数据分配唯一的VLAN,与普通业务数据区分开。此外,在带内DCN中,所有网元都需配置IP地址,网元IP地址也是DCN采用OSPF协议的基础。因此,可通过DCN通道使PTN设备免于遭受IP地址或VLAN方面的攻击。

(2)运行维护风险

PTN设备网管系统建设大多为分厂商、分期、分批建设,各子网由专属的传输设备、DCN支撑网络、服务器、客户端组成,多数采用物理隔离的方式独立成网。随着网络的日益扩大,网管系统越来越多,各支撑系统的部署没有明确的指导原则和系统防护措施,导致网络安全防护复杂、层次不清、系统管理维护困难,网络有效性、稳定性较低。

(3)违规外联

由于PTN设备网管需要外部厂商进行定期维护,所以

存在运维单位通过向网管厂商开放北向接口进行行程维护的隐患。恶意的外部厂商可以利用北向接口对设备进行非法配置和操作,进而导致电力通信网的运行失控。

(4) 互联风险

在生产控制大区,PTN 设备网管系统通过北向接口与电力通信综合网管系统的采集控制系统互联,如果系统互联缺乏安全措施或安全策略不当,采集控制系统的安全风险(如感染病毒木马、错误指令、配置不当等)将直接对设备网管系统造成威胁。

(5) 主机设备入侵

组成通信设备网管的主机设备(包括控制台、应用服务器和数据库服务器),如果未能部署主机防火墙等组件进行主机网络层面的访问控制以及主机入侵检测或入侵防护手段检测对服务器的入侵行为,将存在攻击者利用系统漏洞对通信设备网管攻击的风险。

4 安全防护方案

4.1 设备网管系统网络部署方式

针对电力通信设备网管系统,其网络部署方案如下所示。

(1) 局域网或直连方式

这是当前的常用方案,以 SDH 网管系统为例,当网关网元与服务器不在同一站点时,则每个网关与网元服务器之间均开通一条 2 Mbit/s 通道传输数据信息;若网关与服务器在同一站点,则直接通过局域网互联。远程维护终端与网管服务器之间采用一条 2 Mbit/s 通道传输信息。该方案虽安全性较高,但网络拓展性和运维灵活性较差,需占用过多的网络资源,不利于网络的集中监控与配置。

(2) 构建与调度数据网、数据通信网相互独立的网管网

从安全性角度来看,这种方式满足了专业设备网管系统与其他网络(尤其是数据通信网与互联网存在接口)的物理隔离要求,通过加强对人员和设备的安管理工作,可达到较高的安全防护强度。但从经济性角度看,这种方案需要较大的资金投入。

(3) 数据通信网中划分网管 VPN,并对各设备网管系统进行分域

该方案实现了通道层面的逻辑隔离和系统层面的强逻辑隔离,形成了虚拟网管网,基本满足了专业设备网管系统与其他网络(尤其是数据通信网与互联网存在接口)

的隔离要求。该方案具有较高的运维效率与经济性,不需要在基础网络中重复部署网络设备实现组网,同时也不会对通信专业人员带来额外的运维成本。但从业务重要性及安全等级要求来看,专业设备网管系统均高于数据通信网的其他应用系统,因此这种部署方式将专业设备网管暴露于安全等级较低的网络中,需要对网管系统边界加强防护措施,防止其他应用系统对专业设备网管系统的直接访问。

综合安全性、运维效率、经济性等方面因素,本文建议在电力数据通信网构建独立的网管 VPN,将 PTN 设备网管系统部署于网管 VPN,并划分独立的 PTN 设备网管系统管理域,增强 PTN 网管系统各边界的防护要求。

4.2 DCN 安全部署方案

PTN 技术在电网应用中,为满足多种业务的接入需求,通常应用于电力四级骨干通信网、县域通信网中。如图2所示,以构建基于 PTN 的县域通信网为例,依据设备网管系统网络部署方案分析结果,PTN 网管系统的带外 DCN 采用数据通信网来承载,各地市主备两台 PTN 网管服务器放在地调中心通信机房,同时接入地调数据通信网核心路由器;省公司网管客户端直接接入省数据通信网;各县公司网管客户端接入地区数据通信网,县局和第二汇聚点核心 PTN 设备(网管业务)通过 GE 光口接入地区数据通信网。为保障全省范围内 PTN 网管业务的传输安全,全省 PTN 网管业务通过数据通信网的独立网管 VPN 承载。

针对 PTN 带内 DCN 组网,为保障 DCN 带内网络安全,各个县域的 PTN 的 DCN 单独组网,每个县域各设两个网关网元,网关网元与网管服务器之间采用数据通信网的链路实现互联互通。为保障 PTN 带内 DCN 的组网安全,还应满足以下要求。

- 网关网元作为接入数据通信网的重要设备,为保证通信的稳定性,尽量选择 DCN 处理能力强的 PTN 设备作为网关网元。
- 为保证网管服务器与网关网元管理的网络连接的可靠性,应采用主备网关网元配置方式,保证所有非网关网元能通过不同路由连接到备用网关网元上。
- 为了区分在相同物理通道上传送的普通业务数据和 DCN 消息数据,需要为 DCN 消息数据分配唯一的 VLAN,带内 DCN 使用的 VLAN 标签缺省值为 4 094,业务的 VLAN 标签不能使用该 VLAN 值。

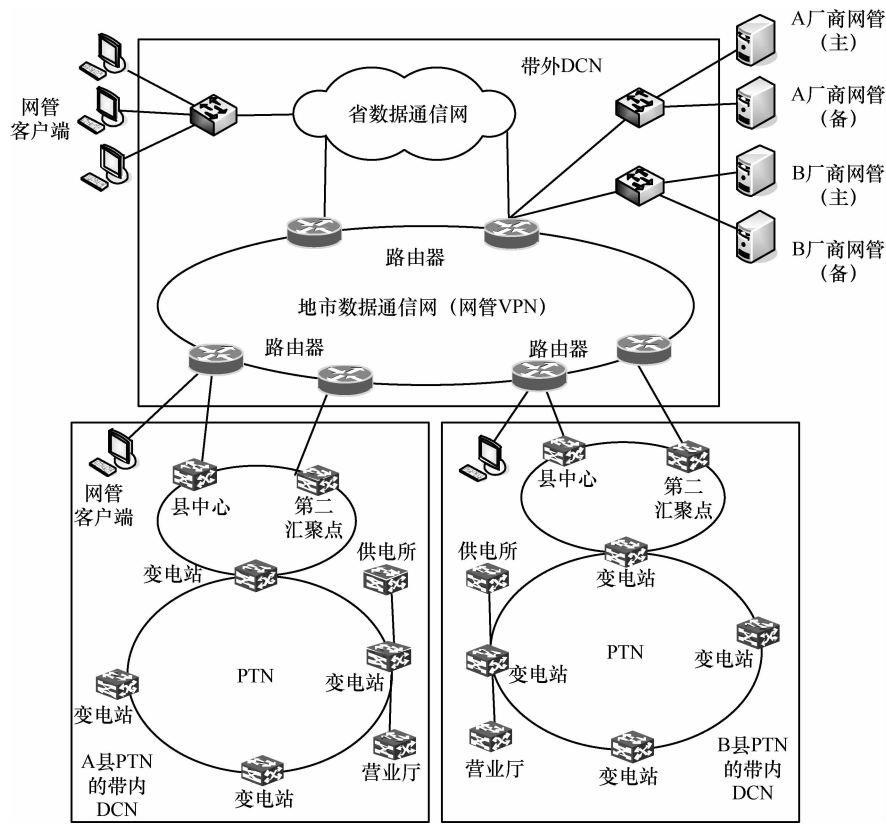


图 2 DCN 安全部署方案

- 考虑到网络限制，同一带内 DCN 子网的网元数不宜超过 64 个，否则导致网络管理结构复杂，主控板负载过大，影响路由计算。
- 网元的 IP 地址必须全网唯一，不能使用广播地址。

4.3 边界安全防护方案

边界安全防护方案如图 3 所示。

当 PTN 设备网管系统部署于网管 VPN 中，需要在以下边界进行安全防护。

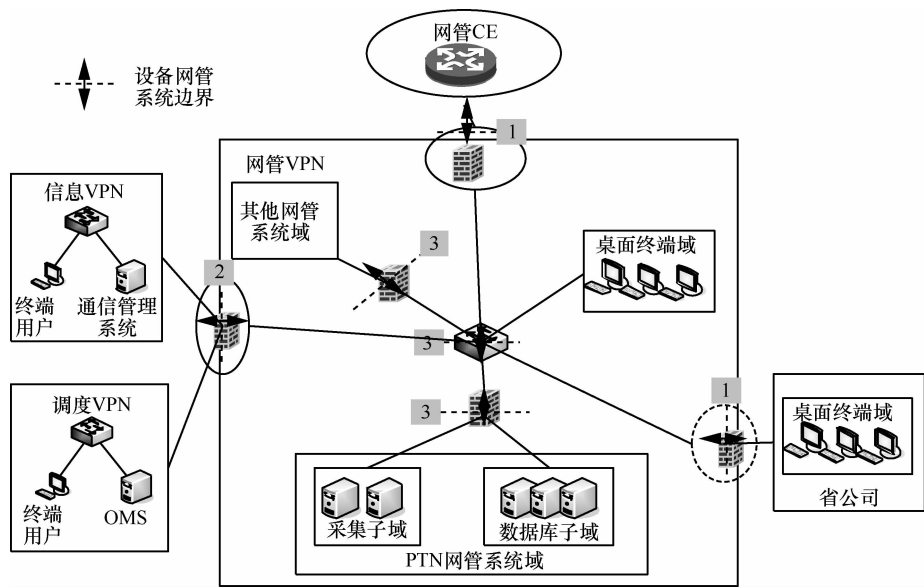


图 3 边界安全防护方案

(1)网管 VPN 纵向互联边界安全防护

包括省电力公司与地市电力公司互联边界,各边界需要部署硬件防火墙设备、网络入侵检测/防护设备、安全审计设备。

(2)网管 VPN 与信息 VPN、调度 VPN 互联边界安全防护

需要部署硬件防火墙网关设备,配置网络地址转换规则,将需要互联访问应用服务器的 IP 地址转换为对方网络指定的 IP 地址,并严格限制网络访问的地址。

(3)设备网管系统域间边界安全防护

可部署硬件防火墙设备或通过交换机划分 VLAN 隔离。

5 结束语

本文针对电力应用的 PTN 网管系统的 DCN 脆弱性、违规外联、系统互联等风险因素,结合安全性、运维效率、经济性等因素,建议在电力数据通信网中构建独立的网管 VPN,用于承载 PTN 网管业务。在此基础上,构建以省、地市带外 DCN 与县带内 DCN 相结合的三层 DCN 部署方案,从 PTN 网关网元生存性、防 VLAN 与 IP 地址攻击、子网的网元限制数量等方面提出 DCN 防护要求。针对纵向互联边界、横向互联边界、域间边界问题,应部署硬件防火墙设备、网络入侵检测/防护设备、安全审计设备或划分 VLAN 隔离,保障 PTN 设备网管系统的边界安全。本文提出的 DCN 部署方案与边界安全防护方案有利于指导电力 PTN 设备网管系统的 DCN 规划与设计,保障电力 PTN 设备网管系统安全稳定运行。

参考文献:

- [1] 罗红艳. 电信级传输双平面 DCN 带外网管系统研究[J]. 信息技术, 2013(2): 83-86.
LUO H Y. Network management system for dual-plane DCN band of telecommunication transmission [J]. Information Technology, 2013(2): 83-86.
- [2] 谭彬, 邱岚, 梁业裕, 等. 基于风险管理提升网管系统安全维护水平的方法[J]. 计算技术安全, 2011(6): 25-28.
TAN B, QIU L, LIANG Y Y, et al. Network management system

for risk management to enhance the security maintenance [J]. Computer Security, 2011(6): 25-28.

- [3] 王羿. PTN 在电力通信网中的组网策略研究 [J]. 电力信息与通信技术, 2014, 12(11): 52-57.
WANG Y. Research on PTN networking strategy in electric power communication network [J]. Electric Power Information and Communication Technology, 2014, 12(11): 52-57.
- [4] CCSA YD/T 2374-2011[S/OL]. [2011-12-20]. <http://www.tsinfo.js.cn/inquiry/gbtdetails.aspx A100=YD/T%202374-2011>.

[作者简介]



刘昀(1980-),女,博士,国网冀北电力有限公司信息通信分公司高级工程师,主要从事电力市场、信息通信安全等工作。



刘国军(1983-),男,全球能源互联网研究院高级工程师,主要从事电力通信安全、网络评估等工作。



任建伟(1980-),男,国网冀北电力有限公司信息通信分公司高级工程师,主要从事电力通信安全研究与运维工作。



李坚(1987-),男,国网冀北电力有限公司工程师,主要从事电力信息安全研究与管理工作。