



网络安全域自动核查分析技术及应用

刘晓峰, 谭 彬, 邱 岚, 王焕如

(中国移动通信集团广西有限公司信息安全管理中心 南宁 530022)

摘 要:通过对网络安全域自动核查分析技术的研究与应用,实现了安全域拓扑自动还原以及安全域设备互联关系、安全域边界及边界访问控制策略的自动核查。通过自动化、常态化和流程固化的方式,及时发现违反安全域规定的行为,确保边界访问控制策略最小化,确保网络安全域划分的持续合规,降低安全域管理的相关风险。

关键词:安全域;合规;访问控制策略

doi: 10.11959/j.issn.1000-0801.2015020

Automatic Verification Analysis Technology of Network Security Domain

Liu Xiaofeng, Tan Bin, Qiu Lan, Wang Huanru

(Information Security Management Center, China Mobile Group Guangxi Co., Ltd., Nanning 530022, China)

Abstract: By studying the automatic verification analysis techniques of network security domain, a secure domain topology automatically restore and security domains devices interconnected relations, security domain boundaries and border access control policy automatic verification were achieved. Through automation, normalization and processes curing methods, violations of the security domain provisions of the act were detected. It ensures border access control policy is minimized and network security domain is divided continued compliance, reduces the risks associated with the security domain management.

Key words: security domain, compliance, access control policy

1 引言

网络安全域划分和边界防护是等级防护和纵深防御框架的基本要求,也是整个网络及信息系统最基本的安全需要。电信运营商通过安全域划分和边界防护的实施,有效保障了通信网和支撑网的安全。但是,随着业务迅速发展,业务系统网络及互联关系处于持续的动态变化过程中,原有的安全域划分和边界的安全状态会被破坏,并直接导致网络和信息系统的巨大安全风险。

目前,安全域管理单纯依靠人工方式进行管理、审计、检查,难以实现精准、实时、全面地分析,无法有效限制安全域的随意调整,无法确保长期符合安全域划分标准要求,也无法对不断积累的大量边界访问控制策略的合理性进行有效判断。在全网的各类安全检查、风险评估和事件分析工作中,安全域划分问题成为常见安全风险的主要来源。

本文通过研究基于真实网络拓扑结构的安全域划分审计技术,自动分析业务系统安全域划分实际情况,准确



掌握安全域边界出口设置情况,自动发现私自部署或者调整设备行为,自动分析边界访问控制策略是否满足最小化原则。确保安全域划分的持续合规,降低安全域管理的相关风险。

2 网络安全域划分管理现状及风险

2.1 现状

目前,为满足网络边界安全防护、等级保护以及纵深防御的需要,电信运营商均遵循安全域划分及边界防护技术要求,按照业务功能和重要性划分了安全域,在安全域边界、安全域子域之间部署了防火墙等访问控制设备,进行数据流的访问控制。通过全网安全域划分,分等级对业务系统进行集中防护或者分系统防护,建立了完善的系统安全域防护体系。为通信网、业务网和网管网提供可靠边界防护能力。

在日常网络运营中,业务系统管理员根据运维和业务实际需要,对网络互联关系或者边界进行持续性调整;当网络拓扑发生变化或设备内部配置调整时,安全域逻辑结构随之发生变化。目前,安全域划分情况主要采取人工方式核查,即基于系统维护人员提供的安全域规划拓扑图,判断安全域划分是否符合要求。但由于维护人员提供的信息存在不准确情况,仅仅依靠人工记录修正拓扑图的方式,很难保证其准确性、实时性、完整性,导致误判情况经常发生,安全域的网络安全管理工作难以正常进行。

由于缺乏有效的手段准确呈现安全域划分情况,加上管理流程执行落实不到位,全网安全域管理成为目前安全管理工作中的薄弱环节,主要表现为:

- 缺乏安全域变更调整信息的准确提供和记录,维护人员无法掌握内部设备功能、互联需求等基础信息,失去了判断安全域健康状况的一手数据和判断能力;
- 缺乏有效的手段准确呈现安全域划分情况,导致安全域实际划分情况不可见,无法及时发现违反安全域规定的变更行为;
- 由于单纯依靠人工方式进行管理、检查,难以实现精准、实时、全面的安全域管理,无法确保长期符合安全域划分标准要求。

2.2 安全域划分管理风险

网络安全域是整个网络安全的基础,安全域管理的混乱直接导致如下安全风险:

- 无法保证长期符合标准安全域结构要求,各类设备

安全需求不能得到正常保障;

- 无合理互联需求的子域之间互通,引起攻击或者恶意代码流量的广泛传播,导致网络瘫痪;
- 互联网或者其他网络用户利用混乱的边界设置,直接攻击该安全域,或者以该安全域作为跳板攻击其他核心子域,导致“一点攻破、全网皆失”的后果。

电信运营商的网络系统是一个庞大、复杂的系统,在业务不断发展的前提下,如何保证安全域划分和边界防护的持续合规,是一个巨大的挑战。

基于上述风险,本文设计一种针对电信运营商安全域的自动化核查和分析系统,实现在网设备准确发现、真实的安全域拓扑审计、子域之间和安全域之间边界访问控制策略自动核查,为安全域管理提供一体化的技术支撑手段,实现安全域划分和管理的透明性,保障安全域划分和防护控制的持续合规,降低安全域管理的风险。

3 安全域合规自动核查系统的设计及实现

本应用设计面向支撑整个安全域的管理工作,立足于全面解决上述主要问题,为安全域拓扑自动还原和展现、设备变更管理、安全域划分合规检查、各类边界策略核查提供一体化支撑能力。

3.1 安全域管理模型和功能架构设计

如图1所示,笔者基于PDCA循环理念设计了安全管理模型,通过plan阶段的策略管理、do阶段的现网数据收集、check阶段的综合分析和action阶段的响应处理,进行闭环和循环管理,实现安全管理问题的及时发现和整改,保持安全域的持续合规。

如图2所示,笔者基于安全管理模型,采用分层低耦合架构设计安全域合规自动核查系统的功能框架。

网络安全域自动核查系统按照采集层、分析层和展现层进行设计。

- 采集层:实现网络设备和主机设备信息的自动采集。
- 分析层:通过信息标准化处理,实现安全域拓扑还原、安全域划分核查、防火墙策略核查和在网设备自动发现。
- 展现层:提供安全域信息管理、安全域核查结果展现,并提供安全域合规问题闭环整改。

通过技术手段,结合配套管理流程,实现安全管理工作的闭环和持续管理。下文对安全域合规自动核查系统的关键设计进行说明。

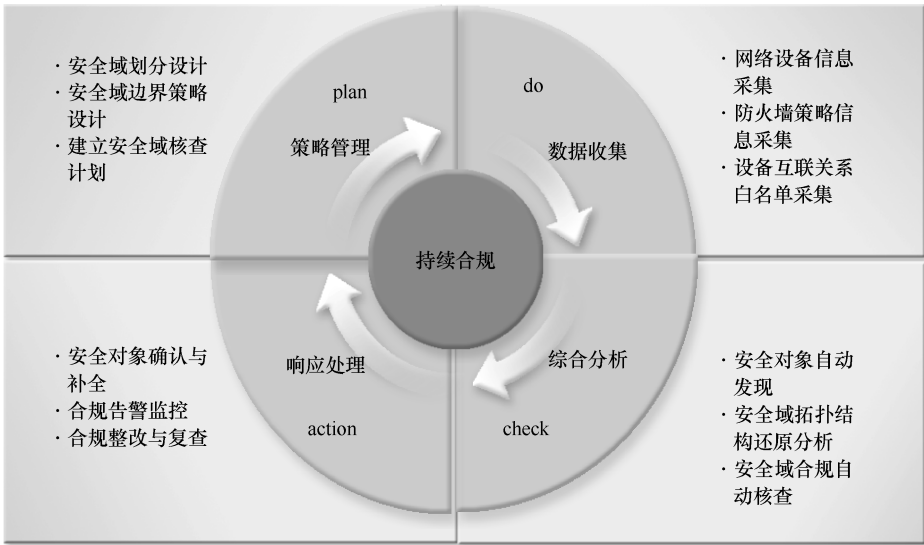


图 1 安全域合规管理模型示意

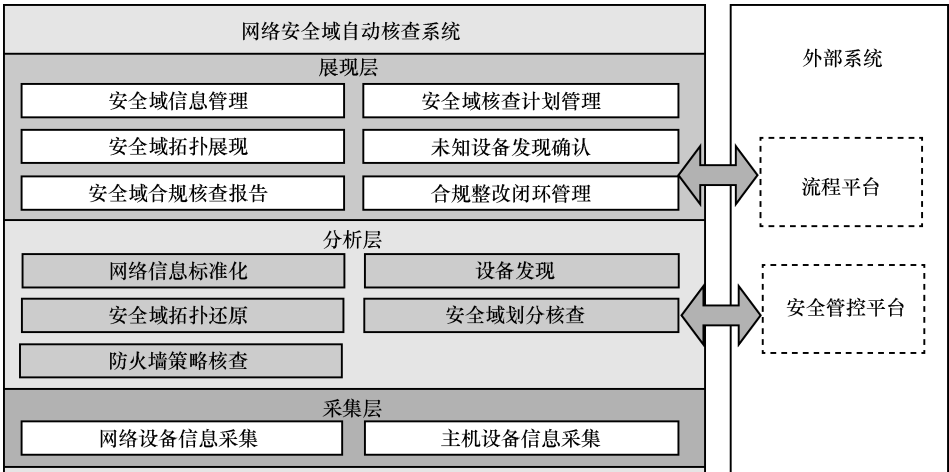


图 2 安全域合规自动核查系统功能架构

3.2 网络信息采集设计

网络信息采集模块利用 Telnet、SSH 等手段,通过登录交换机、路由器、防火墙和主机等设备采集如下信息。

- 采集与设备发现和网络拓扑还原相关的信息:包括设备 ARP 信息、设备 MAC 地址信息、设备路由信息、设备接口信息、设备配置信息等。
- 采集防火墙、交换机上有关边界访问控制策略的信息。
- 采集各安全域、各边界设备互联关系白名单。

由于涉及不同设备类型、设备厂商,采集模块对于采集到的原始信息进行标准化处理,生成标准化的资产信息表、与拓扑逻辑分析有关的网络设备互联关系表、路由表、防火墙策略表等列表,为上层的分析功能提供归一化数据。

3.3 安全域合规分析与展现设计

3.3.1 安全对象核查与确认

安全对象核查是从现网环境中发现所有存在的设备 IP 地址信息,与安全管控平台已接入的资产对象进行比对,核查现网内是否有未接入安全管控平台的设备。

对于未知的在网设备,触发用户确认、更新、完善安全对象信息的流程,实现对各安全对象入网、变更、退网等业务状态的监控,支撑安全域管理办法规定的管理要求。图3 为安全对象自动发现与处理流程示意。

3.3.2 安全域拓扑结构还原及展现

安全域拓扑还原通过对现网中的网络设备和主机的 ARP MAC 地址、路由信息、接口信息等配置信息,分析出设备之间的互联关系,分析内容主要包括设备间连接关

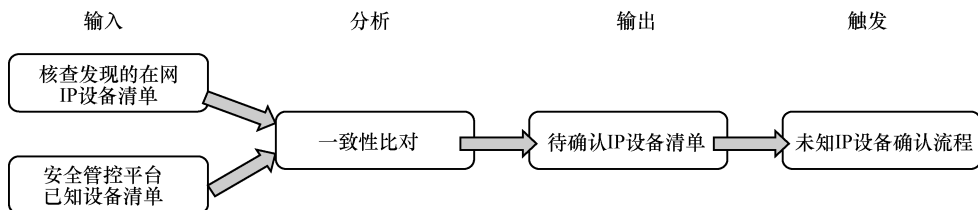


图3 安全对象自动发现与处理流程

系、设备上下联位置关系、服务器 VLAN 归属、双机互联关系、二层交换机分析、边界设备和边界出口。基于此,实现安全域逻辑的网络拓扑的还原。通过对安全域拓扑进行版本保存,实现拓扑图的版本管理和版本间拓扑变化情况对比。图4为安全域拓扑还原效果示意。

基于安全域逻辑的网络拓扑,不同于网管系统中的网络拓扑概念,主要体现各类系统安全域划分的子域和边界概念,体现主机、网络设备之间的互联关系。

3.3.3 安全域合规自动核查

根据安全域管理办法进行安全域自动核查设计,自动核查内容包括安全域设备互联关系变更核查、业务系统 VLAN 核查、安全域边界出口变动核查、安全域划分合规核查、边界访问控制策略核查。

- 安全域设备互联关系变更核查内容:资产使用端口数目变更、端口(接口)IP 地址变更、VLAN 所拥有端口和 IP 地址变更、资产之间互联关系变更。
- 业务系统 VLAN 核查内容:业务系统 VLAN 变更、业务系统未划分为独立 VLAN。
- 安全域边界出口变动核查内容:边界出口数量变化、边界出口 IP 地址变化。
- 安全域划分合规核查内容:通过安全域访问规则与互联关系白名单对比,分析互联关系白名单是否符合安全域管理要求。
- 边界访问控制策略核查内容:策略冲突、策略交叉

冲突、策略重复、策略交叉重复、目的地 IP 地址范围过大、目的地端口范围过大、超范围目的端口(包含管理端口)。

3.4 安全域合规问题整改闭环处理设计

对于安全域合规检查中发现的各类问题,采取闭环管理的流程和自动化跟踪的方式,确保每个安全问题得到及时和妥善处理。

为实现安全域合规问题的强制性处理,通过流程平台将问题处理流程化,到达限定时间后系统自动进行复查。对复查不达标的问题按照既定的重复次数自动重发工单;对于整改达标的情况,自动出具历史对比报告。

4 安全域合规自动核查系统应用效果

安全域合规自动核查系统在省内完成两大高风险系统的安全域拓扑结构还原、展现和核查。安全域管理的实际应用效果见表1。

通过系统的持续应用,实现了精准、实时、全面的安全域管理,有效降低了安全域划分和访问控制方面的风险:

- 自动及时地发现违反安全域规定私自部署或者调整设备等行为;
- 自动分析呈现真实的安全域拓扑结构;
- 能够基于真实网络拓扑结构进行安全域划分审计;
- 能够准确掌握安全域出口设置情况;

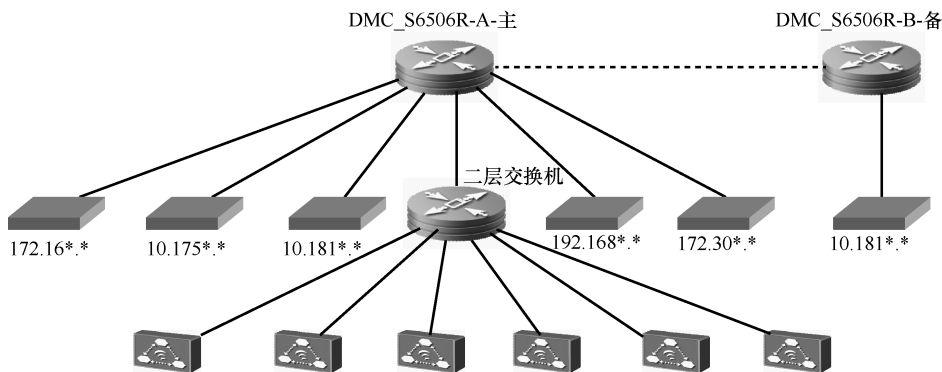


图4 安全域拓扑还原效果

表 1 安全域合规自动核查应用测试情况

核查项	业务系统	
	业务系统 1	业务系统 2
在网设备发现	实际在网设备 49 台,实际发现 49 台,设备发现率 100%	实际在网设备 172 台,实际发现 172 台,设备发现率 100%
安全域拓扑还原	准确还原业务系统安全域拓扑	准确还原业务系统安全域拓扑
设备互联关系变更核查	可自动分析出两次核查间的资产互联关系变更情况、VLAN 所拥有端口和 IP 地址变更情况、端口(接口)IP 地址变更情况	可自动分析出两次核查间的资产互联关系变更情况、VLAN 所拥有端口和 IP 地址变更情况、端口(接口)IP 地址变更情况
业务系统 VLAN 核查	如实核查出系统划分了 2 个 VLAN,无违规情况	如实核查出系统划分了 4 个 VLAN,其中一个 VLAN 与其他业务系统共用,存在违规情况
安全域边界出口变动核查	如实分析出有边界出口 2 个;如实核查出两次核查间的边界出口数量和边界出口 IP 地址没有发生变化	如实分析出有边界出口 3 个;如实分析出两次核查间的边界出口增加了 1 个,原有边界中有 1 个出口 IP 地址发生变化
安全域划分合规核查	如实核查出有 2 条设备互联白名单违反安全域划分规定	如实核查出有 17 条设备互联白名单违反安全域划分规定
边界访问控制策略核查	可自动分析出其出口防火墙设备存在端口开放范围过大的问题	可自动分析出其出口防火墙设备的 IP 地址和端口开放范围过大的问题
核查效率	手工核查耗时 2 天 系统自动核查耗时 17 min	手工核查耗时 5 天 系统自动核查耗时 21 min

- 自动准确分析边界访问控制策略是否实现了对应合理互联需求的最小化;
 - 有效限制安全域随意调整的情况,确保网络实际情况长期符合安全域划分标准要求。
- 通过安全域合规核查自动化的实现,大大提升了核查效率,并为安全域合规核查的常态化和持续合规化提供了技术支撑手段。

5 结束语

分析了现有网络安全域管理的现状和风险,并结合通信运营商的业务特点,设计了安全域合规自动核查模型和系统。实现了在网设备准确发现、真实的安全域拓扑展现与合规审计、子域之间和安全域之间边界访问控制策略审计等,提供了一体化自动核查的支撑能力。为安全管理员和网络系统管理员提供了有效的技术支撑手段,为管理员打造火眼金睛,有效保障安全域管理的持久健康和合规。

参考文献

1 邱岚,谭彬. 安全域划分研究与应用.计算机安全, 2012(6)
Qiu L, Tan B. Research and application of security domain. Computer Security, 2012(6)

2 中国移动通信集团公司. 中国移动支撑系统安全域划分与边界整合技术要求, 2008
China Mobile Communications Corporation. Technical Specification

of Secure Domain and Boundary Convergence for Supporting Systems, 2008

3 GB/T 25058-2010. 信息安全技术 信息系统安全等级保护实施指南, 2010
GB/T 25058-2010. Information Security Technology-Implementation Guide for Classified Protection of Information System, 2010

4 李萍,于慧龙.大型信息系统安全域划分和等级保护.计算机安全,2006(7)
Li P, Yu H L. Large-scale information systems security domain partitioning and graded protection. Computer Security, 2006(7)

[作者简介]



刘晓峰,男,中国移动通信集团广西有限公司高级工程师,主要研究方向为移动通信网络信息安全、不良信息治理。

谭彬,男,中国移动通信集团广西有限公司高级工程师,主要研究方向为移动通信网络信息安全、不良信息治理。

邱岚,女,中国移动通信集团广西有限公司高级工程师,主要研究方向为移动通信网络信息安全管理、信息安全体系。

王焕如,男,中国移动通信集团广西有限公司工程师,主要研究方向为移动通信网络信息安全、不良信息治理。