安全基线核查方案研究

Research on Security Baseline Verification Scheme

刘　安，徐　雷，郭新海，蓝鑫冲（中国联通研究院，北京 100048）
Liu An，Xu Lei，Guo Xinhai，Lan Xinchong（China Unicom Research Institute，Beijing 100048，China）

摘　要：
安全基线核查是系统及设备对自身需求、部署环境和特定时期内应满足的基本安全要求，也是网络防护的第一道防线。分析了安全基线核查的痛点，探讨了通过堡垒机连接设备自动化进行基线核查的方案，提高自动化水平，降低设备账号、密码等敏感信息泄漏的风险。方案能够针对设备不合规检查项自动生成修复脚本，对设备进行整改，并从不同维度统计展示核查结果，方便从整体把握设备安全状态，从而使安全基线核查过程达到自动化、标准化、持续化、可视化，进一步提升网络的安全合规化水平。

关键词：
安全基线核查；修复脚本；自动化
doi：10.12045/j.issn.1007-3043.2023.04.005
文章编号：1007-3043（2023）04-0020-04
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Security baseline verification is the basic security requirements that the system and equipment should meet for their own needs，deployment environment and specific period，and it is also the first line of defense for network protection. It analyzes the pain points of security baseline verification，and discusses the scheme that realizes security baseline verification by connecting equipment automatically through fortress machine，which improves the automation level and reduces the risk of leakage of sensitive information such as equipment account number and password. The scheme can automatically generate repair scripts for equipment non-compliance inspection items to rectify the equipment. Moreover，the verification results are statistically displayed from different dimensions，which is convenient to grasp the safety status of the equipment as a whole. Thus，the safety baseline verification process can be automated，standardized，sustained and visualized，and the safety compliance level of the network can be further improved.

Keywords：
Security baseline verification；Remediation scripts；Automation

引用格式：刘安，徐雷，郭新海，等. 安全基线核查方案研究[J]. 邮电设计技术，2023(4)：20-23.

1 背景

随着云网融合以及互联网技术的高速发展，人们的衣食住行处处离不开网络。近年来，网络规模快速扩展，并与业务深度融合，配置参数和策略日益复杂，尤其是云原生技术的发展，业务上云、容器化部署等技术的广泛应用，使得基线核查不仅面对海量的传统网络设备，云原生中的配置风险也逐渐凸显。配置或策略的不当操作，会造成设备带病入网运营，一个不恰当的配置可能造成木桶效应，造成网络入侵、信息泄露等威胁，给整个网络的设备带来安全风险。

安全基线是设备运行的最小安全保障，是设备得到统一的、最低要求的安全设置，是系统及设备对应自身需求、部署环境和特定时期内满足的基本安全要求合集，是网络安全防护的第一道防线。所以对设备或系统进行安全基线核查是必要且常态化的工作。目前的网络结构复杂、设备数目庞大，网络设备和配置也在不断更新，网络之间的隔离等给统一进行基线核查带来不小的挑战，常态化的安全基线核查成为一种周期长而复杂的工作。为提高基线核查效率，对设备进行全面自动化的核查，需要利用现有的工具进行联动，进一步提高核查工作的自动化水平。

收稿日期：2023-02-16

2 安全基线核查面临的痛点

安全基线核查对于整个网络的重要性不言而喻，每年的安全基线核查工作都花费了大量的人力物力，基线核查工作中面临的痛点主要有以下几点。

a）在核查系统上管理设备的敏感信息，易造成信息泄露。目前市面上的核查系统在完成在线设备的核查任务时，需要输入设备的账号、密码等敏感信息。如果核查设备自身安全防护不足，系统一旦被攻击，容易造成大量核心设备敏感信息泄露，给核查设备带来新的安全风险。

b）设备功能不断更新，检查项滞后。随着网络设备和业务的深度融合，设备的版本也在不断迭代更新，新的业务逻辑和配置也在随之变化，如果没有新的检查项适配检测设备的风险点，就会造成检查项的更新滞后，造成设备带病入网运行。

c）安全基线核查自动化程度不高，投入较大。目前的安全基线核查系统需要手动输入设备信息，包括登录账号密码等信息，对于网络隔离等情况，则需要借助离线手段进行核查。靠人工录入设备的方式会导致核查覆盖范围不全面，容易遗漏某些设备，而且设备数目庞大，过多的人工操作导致一个核查周期需要消耗大量人力物力，常态化的安全基线扫描工作难以推进。

d）不合规检查项加固困难。在不合规检查项整改加固期间，由于运维人员能力不一，很难做到对不合规检查项的正确加固。并且许多系统都是在网运行的业务系统，一条不正确的命令可能造成整个业务的瘫痪，产生不必要的损失。

3 安全基线核查整体架构

安全基线核查平台采用分布式架构，分为平台和检测节点2个部分。如图1所示，平台将核查脚本下发至各检测节点的管理平台，在管理平台上选择要核查的设备，通过堡垒机自动连接设备执行核查脚本。核查脚本执行后生成执行结果文件，通过管理平台将结果文件上传至安全基线核查平台进行解析。平台将解析后的结果进行统计分析并从不同维度展示核查结果，能够更好凸显核查设备的薄弱点。同时，针对不合规的检测项，自动生成加固命令下发至检测节点进行加固。

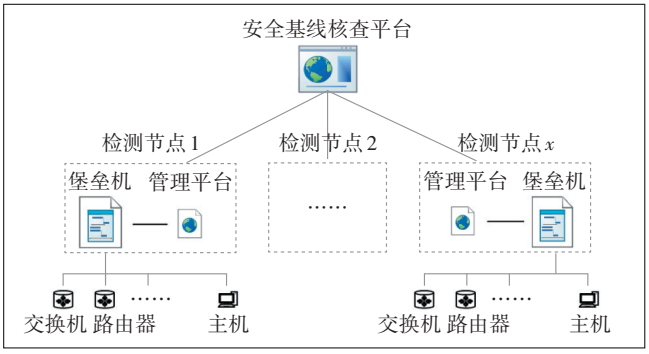

图1　安全基线核查平台整体架构

3.1 安全基线核查平台

安全基线核查平台主要功能是将核查脚本下发至各个检测节点，并对每个检测节点上报的脚本执行结果进行解析，归类呈现总体核查结果。整个系统包括UI展示层、业务逻辑层和数据层，如图2所示。

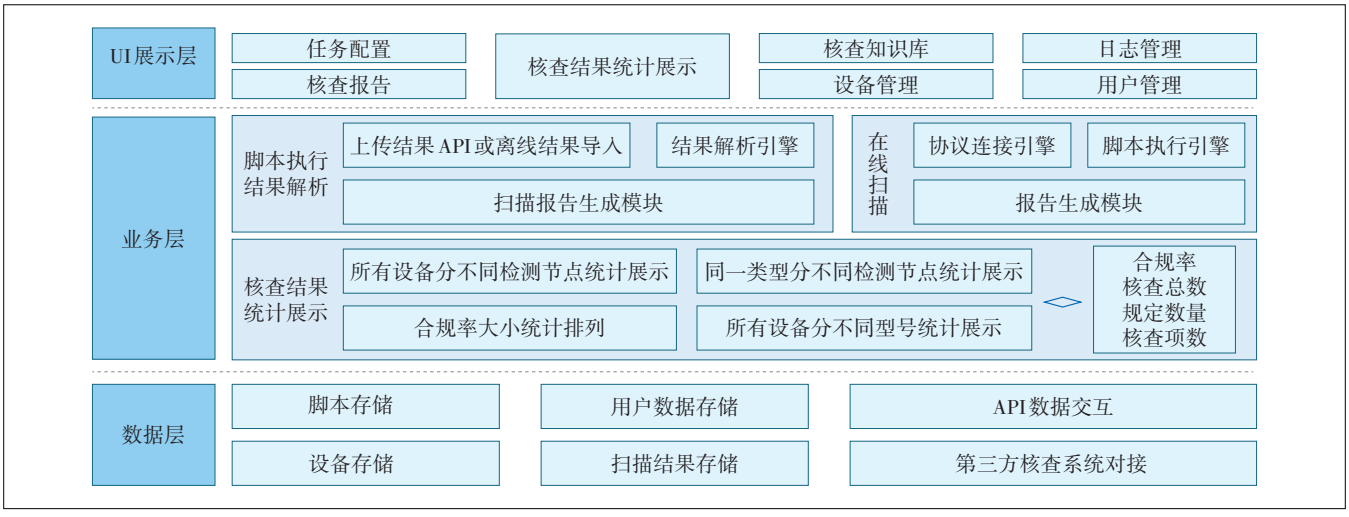

图2　安全基线核查平台层级

UI展示层通过Web界面的形式，完成系统数据的可视化呈现以及人机交互功能。通过页面配置扫描任务，包括在线扫描和离线扫描2种形式；通过页面查看核查知识库，包括扫描设备类型、检查项、检查内容、检查方法和加固建议等信息，也可以添加和修改检查项，保证检查项不断更新适用，同时也能够动态新增脚本和检查规则，保证对新增设备类型的核查；通过页面查看设备管理，查询扫描过的设备以及设备的扫描报告；通过页面查看核查结果的统计展示，从不同维度统计核查结果，从全局掌握网络设备的整体情况以及薄弱点；通过用户管理页面，配置平台和检测节点账号，对设备进行分权查看；日志管理功能可以查看用户的操作日志，用来做后期审计。

业务层完成系统功能的业务逻辑，主要包含脚本执行结果解析、在线扫描以及核查结果的统计展示。脚本执行结果解析主要是对离线导入的、检测节点上报的或者在线执行的结果进行解析，通过结果分析引擎将执行后的结果进行解析，然后和内部的规则进行匹配，生成扫描报告。在线扫描能够通过协议连接引擎远程连接现网的设备，包括Telnet、SSH等常见协议，通过在线方式执行脚本，生成扫描结果。核查结果统计展示能够从不同的维度进行扫描结果筛查，从不同角度分析把握扫描结果，从全局掌握重点薄弱点并进行整改，扫描统计结果中至少包括合规率、核查总数、规定核查数量以及核查项数等信息。

数据层主要完成数据的交互和存储。存储功能主要完成脚本、设备、用户以及扫描结果的存储。API数据交互完成脚本下发、检测节点脚本执行结果的上报以及不合规项信息的下发。系统对接主要完成对不同厂家设备第三方系统接口的对接，用来更新扫描脚本。

3.2 检测节点

检测节点包含管理平台和堡垒机2个部分。管理平台能够创建基线核查任务，选择待核查的设备，通过堡垒机自动化连接设备进行基线核查，并将核查脚本执行后的结果一键上传至基线核查平台。同时接收从平台侧下发的不合规项的信息，不合规项的整改命令由系统管理员确认后生成修复脚本，下发至扫描设备并执行修复命令。

4 安全基线核查主要功能设计

安全基线核查平台能够通过检测节点中的堡垒机连接设备，进行自动化基线核查，使安全基线核查过程达到自动化、标准化、持续化、可视化，有利于提高检查结果的准确性和合规性，进一步提升网络的安全合规化水平。平台的主要功能包括自动化基线核查功能、在线和离线核查功能、自动化修复功能以及基线核查脚本。

4.1 自动化基线核查功能

自动化基线核查功能如图3所示，由系统管理员登录设备管理系统，新建核查任务，选择要核查的设备。通过堡垒机登录到设备，执行由平台下发的基线脚本，生成执行结果。结果文件由设备管理系统上传至基线核查平台进行解析。该功能保证了设备账号、密码等信息的安全性，提高自动化水平。

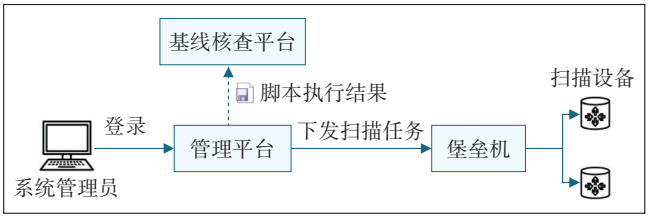

图3　自动化基线核查功能

4.2 在线、离线核查功能

基线核查平台可以通过Telnet、SSH、WinRM等协议，远程连接设备执行脚本，生成结果文件进行解析，适用于不会泄露设备敏感信息的环境。平台也可以将导出的离线脚本在待核查设备上执行后，把离线结果文件直接导入平台进行解析。

4.3 自动化修复功能

如图4所示，当设备有不通过的检查项时，基线核查平台根据加固建议，针对每一条不通过的检查项生成加固命令，连同检查项的其他信息一同下发至设备管理平台。系统管理员逐个对检查项加固命令进行

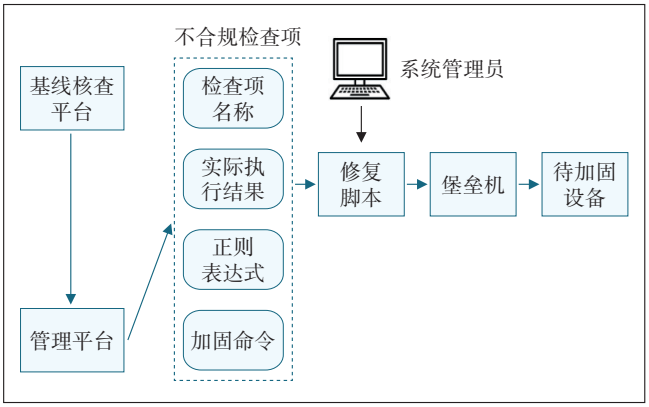

图4　自动化修复功能

确认或者修改，生成修复脚本后远程连接到设备进行一键加固。该功能解决了不合规检查项加固困难的问题，能够及时消除安全风险。

4.4 扫描结果统计展示功能

如图5所示，平台通过在线、离线或者检测节点上报的形式获取脚本执行结果，解析引擎生成的扫描报告，扫描报告包括设备信息以及检查结果。检查结果应包括检查项ID、检查项名称、检查方式、实际值、预期值、加固建议等信息。根据设备的扫描结果，生成统计报表，可根据关键字段筛选出要统计的设备，并可以从IP、设备型号以及设备类型的维度生成报表。根据设备的扫描结果生成综合展示模块，从3个维度不同的数据表展示所有设备的核查情况。

4.5 基线核查脚本

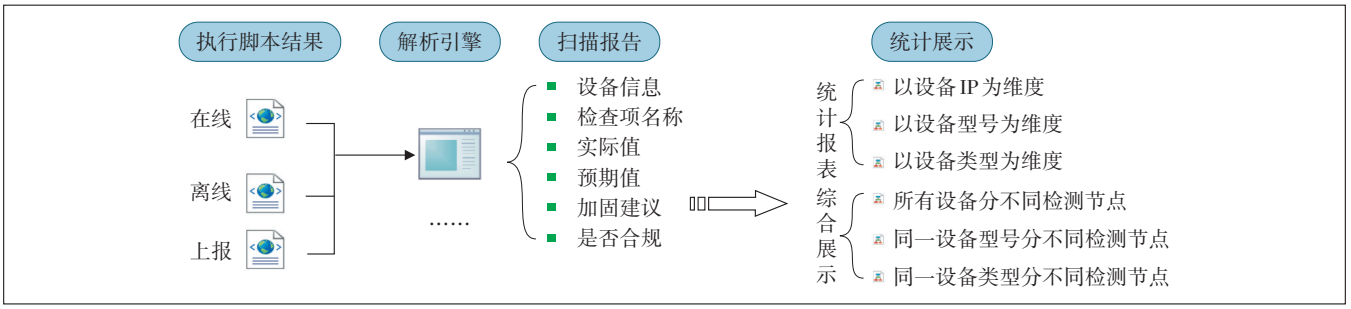

图5　扫描结果统计展示功能

核查脚本是整个基线核查工作的核心，核查脚本应覆盖全面，对现网中的核心设备都有覆盖，表1中列出了常见的设备类型。平台设计中也增加了第三方安全厂家的对接接口，可以动态拉取核查脚本，同时也可以自定义脚本以及核查规则，保证覆盖核心的设备类型。

表1　设备列表

序号	类型	型号	序号	类型	型号
1	中间件	WebLogic	21	路由器	Juniper
2		Tomcat	22		Cisco
3		Apache	23		Huawei
4		WebSphere	24		ZTE
5		Jboss	25		H3C
6		IIS	26	交换机	Cisco
7		Nginx	27		Huawei
8		BIND	28		ZTE
9	操作系统	Windows	29		H3C
10		Solaris	30		Maipu
11		Debian	31	防火墙	Cisco
12		HP-UX	32		Huawei
13		AIX	33		Juniper
14		Suse	34		H3C
15		Linux	35	云原生基础设施	Docker
16	数据库	Oracle	36		Kubernetes
17		Sybase	37		OpenShift
18		DB2	38		OpenStack
19		SQL Server	39		Yaml文件
20		MySQL	40		Dockerfile

5 结束语

本方案从现有基线核查工作的痛点出发，复用现有的安全机制，通过管理平台连接堡垒机自动化扫描设备，不仅提高自动化核查水平，而且能够减少账号、密码泄露带来的安全风险。在平台知识库中可以对检查项进行编辑和新增，保证了检查项的更新，避免因检查项滞后遗漏设备的风险。同时能够对接安全厂商的核查系统拉取核查脚本，自定义增加脚本和检测规则，保证核查脚本型号覆盖核心设备。平台能够自动生成修复脚本，一键式修复不合规的检查项，保证设备安全运行。界面中提供了丰富的结果统计展示信息，方便管理者从整体把握设备安全风险，从设备管理、设备核查到设备加固、结果展示等方面进一步提高基线核查工作的自动化水平，减轻安全人员的负担，使常态化的安全基线核查工作变得更加方便。

参考文献：

[1] 纪炜灿. Windows终端安全基线检查及补丁修复工具[J]. 互联网周刊，2021(22)：68-69.

[2] 陆庭辉，郭凤婵，刘翠媚，等. 一种计算机终端安全基线核查方法：CN202011288142.4[P]. 2021-02-19.

作者简介：

刘安，工程师，硕士，主要从事网络与信息安全研究工作；徐雷，教授级高级工程师，博士，主要从事网络与信息安全研究工作；郭新海，工程师，硕士，主要从事网络与信息安全研究工作；蓝鑫冲，工程师，硕士，主要从事网络与信息安全研究工作。