智维数据
Intelligent Analytics Platform

nCompass 防火墙策略可视化平台

产品白皮书

北京智维盈讯网络科技有限公司

第一章 运维现状

防火墙是企业网络安全的第一道防线，也是最重要、应用最广的安全产品。安全策略的配置是发挥防火墙防护作用的关键。一方面，互联网业务爆发增长伴随着安全威胁的剧增，精细化安全策略配置成为企业应对威胁的重要手段；另一方面，业务的增长的同时带来策略配置数量的指数级增长，而仅仅使用防火墙厂家自带的配置工具已经无法满足防火墙策略管理的运维需求。主要体现在以下方面：

1、防火墙策略越积越多

防火墙策略的堆积问题已经越来越多，成为了不少客户头疼的一个难点。举例来说，一个银行的内网单一个防火墙也有几千条策略，大的金融机构策略数量可达几十万条。策略梳理、策略收敛、策略回收等日常运维工作变得非常困难。

2、通过日志收敛宽泛策略变得不可行

由于历史原因，许多防火墙会存在不少过于宽泛的策略，这些策略可能是在很久以前配置的。例如，某条策略允许了很多 IP 地址，但实际仅有几个 IP 地址是有流量的，这其实就存在安全风险，也不符合等保 2.0 的要求。利用防火墙日志做策略收敛不仅会导致防火墙性能大幅下降，而且无法做到一次收敛多条策略。

3、策略回收无法实现

旧的业务已下线，但是该业务策略没有及时删除。这条策略就会像墙洞一样一直存在，有可能会出现两种情况：第一种，这条策略一直没有流量命中；第二种，可能有命中，但是没有业务流量。因此这条策略一直存在的话都会是一巨大

的安全隐患。这种问题无法用日志方式解决，必须有实际的会话流和策略的对应关系，还需要统计会话流是否有业务流量。

4、无法快速定位威胁入口

安全部门发现有 IP 存在攻击的行为，想知道该 IP 从哪个防火墙进来？哪条策略放行的？从而快速进行阻断。这时，网络流量和安全策略配置结合就变得必不可少。

【nCompass 防火墙策略可视化平台界面展示】

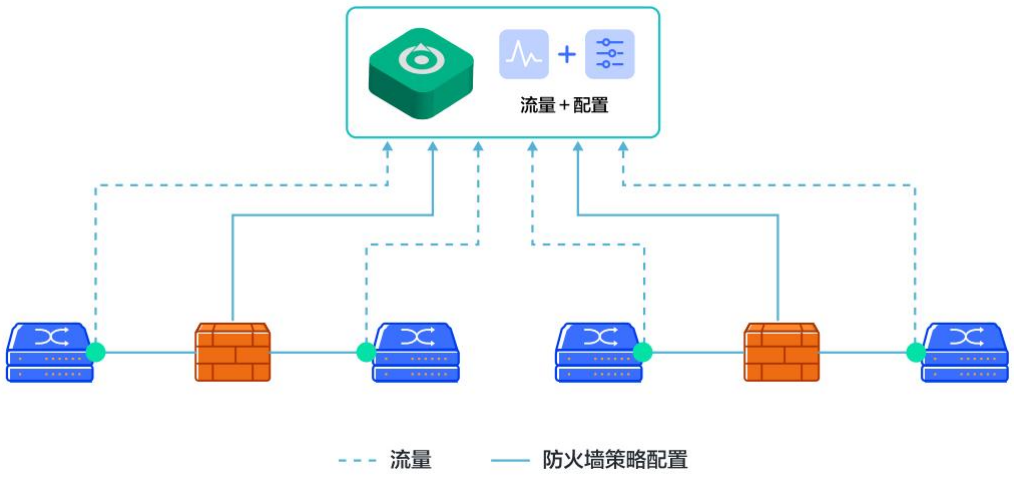
鉴于以上情况，北京智维盈讯网络科技有限公司的 nCompass 防火墙策略可视化平台从用户的实际情况出发，以流量和策略结合作为切入点进行防火墙策略可视化分析，可解决目前防火墙管理中面临的各种实际问题。达到企业提升业务连续性管理水平、运维管理水平，从而最终提升 IT 服务质量及用户满意度的目的。

第二章 产品介绍

2.1 防火墙策略可视化平台介绍

防火墙策略可视化平台，通过网络旁路部署的方式，在对现有的网络、应用不产生任何影响的前提下，7x24 小时采集防火墙前后交换机的流量和防火墙策略配置。图表化界面将提高对防火墙策略的可视性。帮助管理员消除防火墙存在的问题策略，了解当前防火墙策略的使用状况，更好的去优化防火墙策略，让防火墙策略管理变得简单。

2.2 方案部署



防火墙策略可视化平台以软硬一体化设备的方式部署，在对现有网络、应用不产生任何影响的前提下，通过旁路部署的方式 7x24 小时采集防火墙前后交换机的流量和防火墙策略配置，对防火墙性能零影响。

2.3 产品型号

型号	设备类型	处理能力	采集口	储存
NFM400	1U机架式服务器	4Gbps	2*万兆或4*千兆	8TB
NFM1000	2U机架式服务器	10Gbps	2*万兆	16TB
NFM2000	2U机架式服务器	20Gbps	4*万兆	24TB
NFM4000	2U机架式服务器	40Gbps	4*万兆或2*40G	48TB
NFM8000	2U机架式服务器	80Gbps	4*40G	96TB

2.4 功能概述

nCompass 防火墙策略可视化平台主要包括以下 6 个重点功能：

2.4.1 策略优化

防火墙由于日积月累，策略越积越多，通常会存在宽泛策略等原因形成的无效策略，这些无效策略会增加防火墙管理的难度，导致防火墙性能随之降低。另外，由于策略数量巨大，如果采用人工方式逐条筛查，会消耗大量的人力和时间。而不同设备的厂商策略的格式和表达方式也都各不相同且操作流程不规范，需要反复进行策略分析优化。nCompass 防火墙策略可视化平台可通过获取防火墙的配置信息，对防火墙策略进行逐条筛查，自动分析相互之间的重复、包含与被包含的关系，发现宽泛策略、无业务策略、长期未命中策略和可合并策略等问题

策略，并且提供防火墙策略优化方案，将分析的结果作为运维人员策略优化的依据。从而大大减少防火墙策略的数量，优化防火墙性能，提升其工作效率。

2.4.2 实时监控

可视化能力是运维的核心能力，只有看得到才能谈管理。如何消除防火墙策略可视化盲区，是众多用户的需求所在。nCompass 防火墙策略可视化平台提供了实时监控功能，具备同时分析防火墙流量和策略配置的能力，以柱状图的方式呈现出最近 1 小时的防火墙无关、未命中与命中的流量，并且呈现出命中策略、未命中策略与非防火墙的数据流以及每一条策略数据流的状态信息。

2.4.3 策略查询

在安全演练阶段，当安全部门发现有 IP 存在攻击行为，需要快速定位该威胁入口时；当业务部门新上业务，访问不了，需要了解防火墙策略的开通情况时；如果有一个功能可以准确地排查到问题策略,那么业务部门就可以自行去确认防火墙策略的开通情况。在过去出现以上情况通常只能让运维人员人工去逐条排查问题策略,会消耗运维团队大量的时间和人力,而且对问题策略无法保证准确性,对一些风险、不规范策略有时甚至无法检出。nCompass 防火墙策略可视化平台同时具备实时流量和策略配置结合分析能力，以及策略查询自服务功能，能让防火墙策略管理工作效率得到极大提升。

2.4.4 合规检测

数据中心内部业务区之间的互访往往有防火墙隔离，如果存在被这些防火墙阻断的数据流，那么这些数据流很可能是非法的尝试。合规检测可以专门分析这种异常跨区访问被防火墙 Deny 的策略，还能够对异常跨区访问做统计分析，并提供所有异常的数据流。

2.4.5 变更验证

更换数据中心防火墙时，运维人员通常需要将流经旧设备的流量镜像到新的设备，并将原有设备的配置预先做一个备份，然后将被替换设备的配置完整迁移到替换的设备上面，配置迁移完成之后，则需要按照业务需求进行测试。但是运维人员对替换后的效果常常会心存疑虑，因为会存在许多无法预测的问题。

现在这个问题找到了更好的解决方案，通过 nCompass 防火墙策略可视化平台采集新、旧防火墙的策略配置，并一一比对新、旧防火墙的策略，在防火墙更换时为运维人员提供有效的数据支撑，在防火墙变更之后，还可以对比实际流量是否一致，大幅减轻变更后的业务访问验证等工作量，提高运维效率。

2.4.6 统计报告

nCompass 防火墙策略可视化平台的统计报告功能，内置常用的报表系统，可以按照不同的使用场景、不同部门生成所需的报表，如导出防火墙问题策略、导出被防火墙 Deny 的通讯对等。

第三章 用户使用场景

3.1 满足等保 2.0 的要求

随着《网络安全法》出台，网络安全等级保护制度被提升到了法律层面，国家网络安全等级保护工作进入了 2.0 时代，各行各业的网络运营者对等级保护标准进行重新学习、认识，并基于相关标准建设网络安全防护措施。nCompass 防火墙策略可视化平台重点关注到对防火墙策略访问控制的要求，综合起来主要有三个方面：宽泛策略必须收敛、无效策略必须删除和策略数量最小化。如此多新增的安全策略控制要求，对运维人员而言确实是一个不小的挑战。nCompass 防火墙策略可视化平台针对上述要求均给出了优化方案。

等保 2.0 要求（节选）

访问控制要求包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许 / 拒绝数据包进出；

d) 应能根据会话状态信息为进出数据流提供明确的允许 / 拒绝访问的能力；

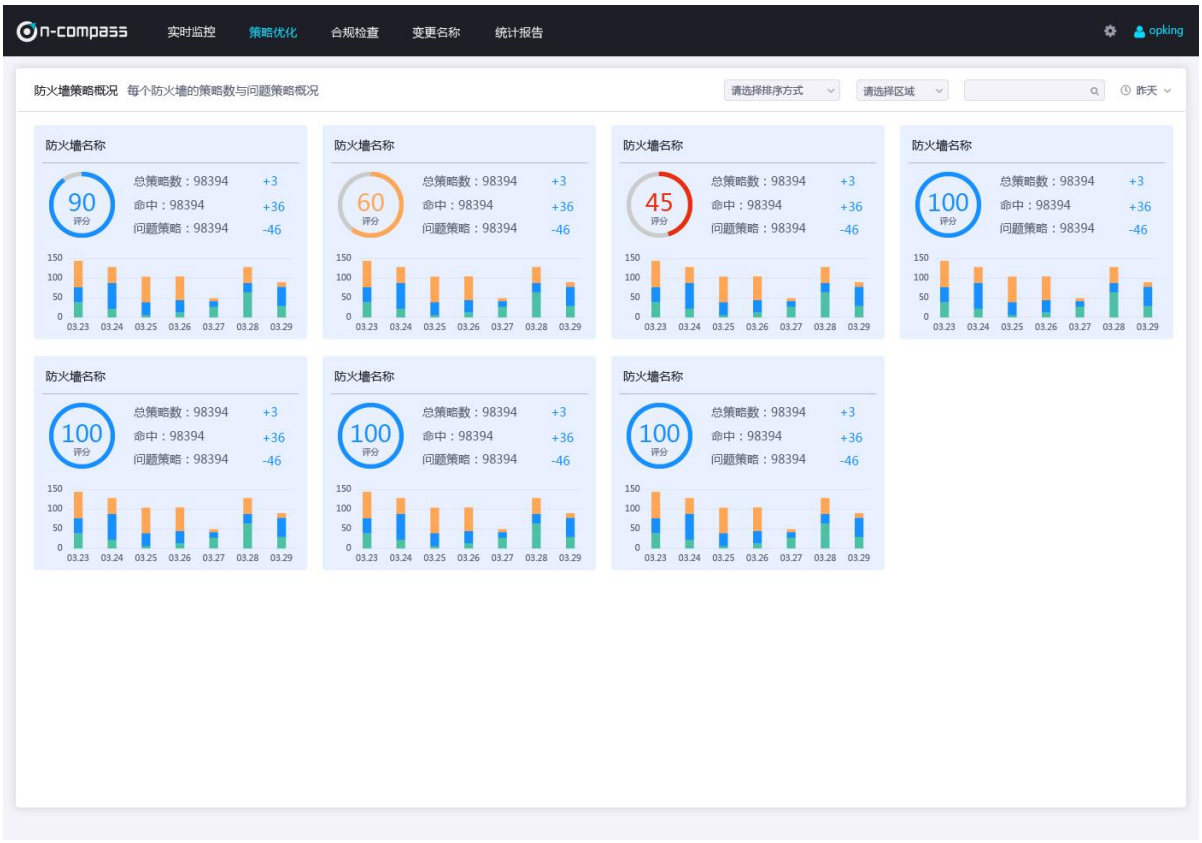
e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

3.2 防火墙策略优化

防火墙是通过安全策略来进行安全防护的，所以防火墙的安全策略配置和管理是企业信息安全工作的主要组成部分。目前大多数企业的防火墙策略已经实现安全策略申请→审批→配置下发→策略验证的自动化配置流程。但基本上都缺乏

安全策略的退出机制，比如定期的策略风险核查、策略生命周期管理、持续的策略收敛优化等。

由于系统管理人员变更、新增策略记录不完整、防火墙新旧更替等原因，许多防火墙策略建立的原因、用途变得不可追溯。nCompass 防火墙策略可视化平台对防火墙策略逐条数据流进行统计分析，可自动分析出存在安全风险的问题策略。用户通过报告能及时发现哪些是有问题的策略，从而对策略进行优化。



【防火墙策略可视化平台优化详情界面】

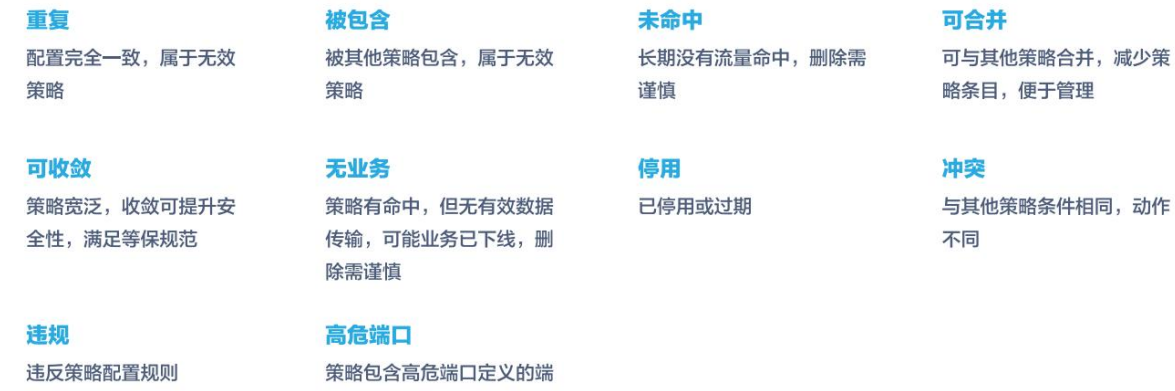
nCompass 防火墙策略可视化平台提供一个全局视图功能叫“防火墙概况”，用户可以快速了解每一个防火墙的策略与问题策略的概况。该界面会对每一个防火墙进行评分，评分的机制来源于问题策略的占比。概况用文本与柱状图的形式

显示历史新增的问题策略，将分别展示有问题的策略、命中的策略以及策略的总数量。

【防火墙策略可视化平台优化详情界面】

在“防火墙概况”，用户可以点击进入存在问题策略的防火墙，在优化详情界面，将对防火墙的问题策略自动分析后进行归类，在不同的优化方向，有多少条目可优化变得一目了然。不同的用户，优化方向的优先级不同。在该界面下方，将显示问题与建议，告诉用户这条策略相互的重复关系。左边是问题策略；右边是相关策略；最右边是优化建议，提供操作建议与操作风险提示，可作为用户对该策略优化的依据。点击策略详情可以看到这条策略相关的更多信息。

nCompass 防火墙策略可视化平台支持发现以下类型的问题策略:



3.3 定位威胁入口

再高级的攻击，都会留下痕迹，因为所有的访问都会经过防火墙。那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。比如安全部门在安全演练项目中，当发现网络可疑的操作，或者发现存在攻击行为的 IP 时，安全人员希望能准确定位到与攻击路径相关的防火墙。

nCompass 防火墙策略可视化平台可基于实时采集的防火墙流量和策略配置，提供安全人员“IP 查策略”这个功能，协助安全部门及时通过灵活的检索规则，对存在攻击行为的 IP 作出相应的安全处理动作。

【防火墙策略可视化平台根据 IP 查询策略界面】

在使用“IP 查策略”的这个功能界面里，只需要在右上角输入源 IP 地址、目的 IP 地址、以及端口与协议，就可以快速的自动分析出该 IP 或会话由哪个防火墙进来，是哪条策略放行的。如果此时左侧显示这个 IP 或通讯对的防火墙、流量为零，说明这条流没有经过防火墙。此时需要查看相关策略，点一下左边的防火墙，右侧表格会显示哪条与该 IP 相关策略放行了这个 IP 或通讯对，也会显示这条数据流的实际流量有多少。在界面下方，提供了相关策略的原文本与格式化的详细信息。基本上，用户输入一个查询条件，就可以看到他所需要的所有信息了，简单快捷。

3.4 策略查询自服务

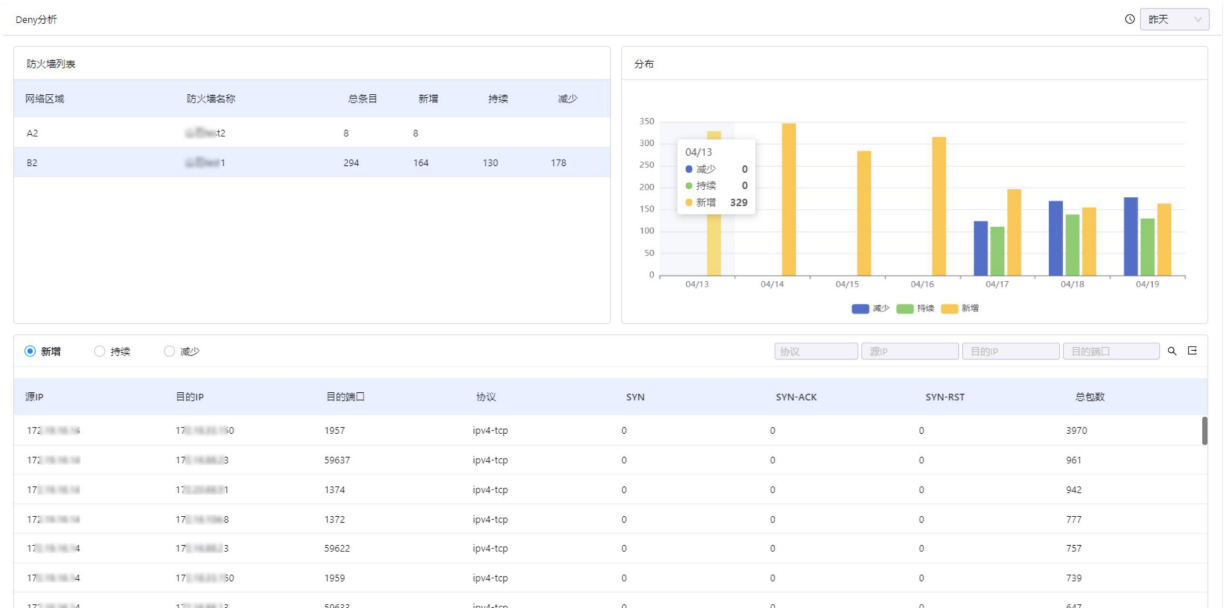
很多时候业务部门新上的业务访问不了，需要运维人员去确认防火墙策略是否开通，这些工作会消耗运维人员大量时间。nCompass 防火墙策略可视化平台提供了策略查询自服务功能，业务部门可以自行确认防火墙策略开通的情况；还有一种需要自服务的场景是：业务部门计划将一组服务器从一个数据中心迁移到另外一个数据中心，此时防火墙策略也要相应迁移，必须获取与该业务相关的所有策略，以便业务快速上线。而相关人员往往很难将需要开通什么端口记得清楚。

【防火墙策略可视化平台根据 IP 查询策略界面】

上述两种情况，业务部门如果需要解决的话，同样可以通过 IP 查策略功能。输入源 IP 地址网段和目的 IP 地址，便能自动分析出该业务 IP 处在哪一个防火墙，是否有开通。选中分析出的相关策略，就能查看该策略原文本与格式的信息。

3.5 异常跨区访问

在数据中心内部业务区之间的互访有防火墙隔离，如果存在被这些防火墙阻断的数据流，这些数据流很可能是非法的尝试。需要一些技术方式找出这种异常的跨区访问，对异常跨区访问做统计分析，并提供所有异常的数据流。



【防火墙策略可视化平台 Deny 分析界面】

针对该问题，用户可以通过 nCompass 防火墙策略可视化平台提供的 Deny 分析界面查看。页面特有的统计分析功能将展示出流量到达防火墙，但是被防火墙 Deny 的流量。统计维度是源 IP、目的 IP、目的端口。上图可以看到 Deny 分析功能界面，左边可以显示防火墙存在被 Deny 的流量，包括总数、新增减少、持续：

总数	新增	减少	持续
这段时间被 deny 的总通讯对数量	代表上周没有，这周新出现的，或者前天没有，昨天新出现的；	代表上周有，但这周没有，这种有可能是已经找到问题流量，并解决了；	代表一直存在的，没有解决。

右边的柱状图提升了防火墙策略管理的可视性，可以显示这一周以来每天的情况，可以看到我们设定最新的时间为昨天，这是为了全量对比，确保数据的准确性。

界面下方我们通过表格的方式可以显示新增、持续、减少的通讯对列表，也可以将表格数据导出给相关部门处理。帮助用户进行快速梳理，对异常跨区访问做统计分析。

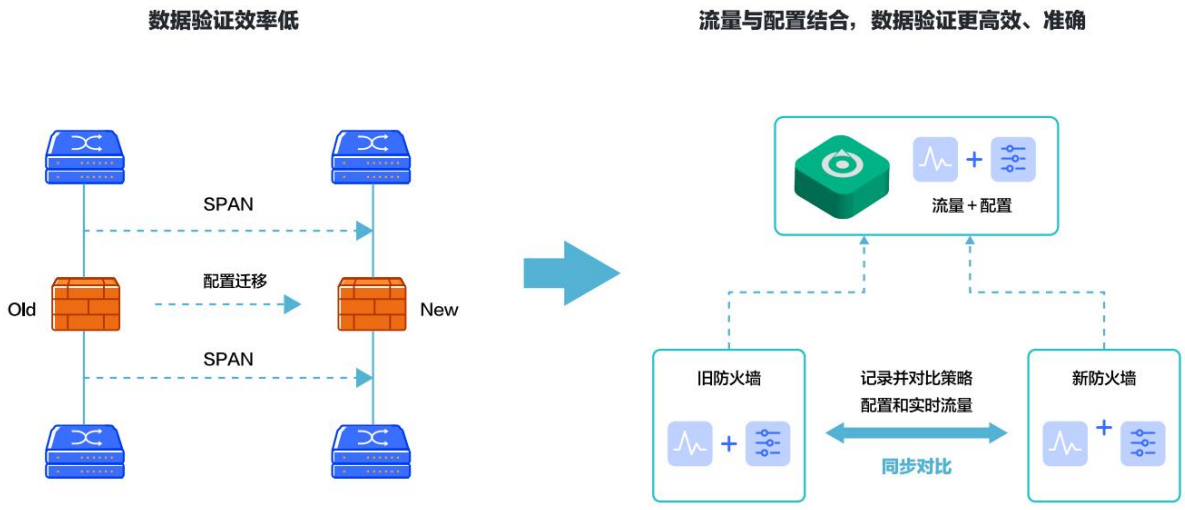
3.6 防火墙变更，为更换后验证提供数据支持

在运维人员对数据中心的防火墙进行更换时，通常需要将流经旧设备的流量镜像到新的设备，并将原有设备的配置预先做一个备份，然后将被替换设备的配置完整迁移到替换的设备上面。配置迁移完成之后，则需要按照业务需求进行测试。

这种迁移流程通常会存在以下问题：

配置迁移问题：在配置导入进新的设备后，这些配置有没有不兼容，有没有缺失以及有没有错误都无从知晓。

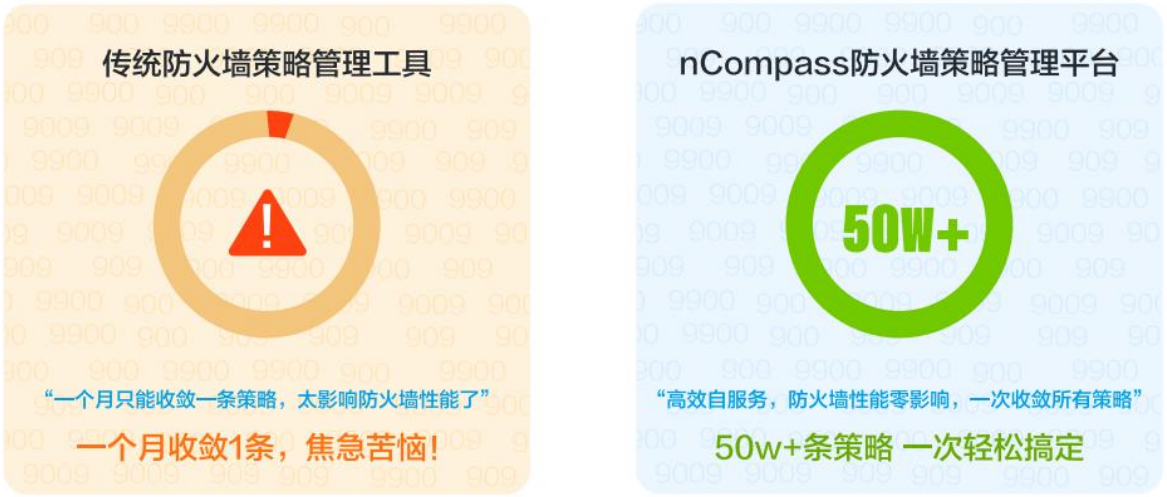
数据验证问题：在替换完成之后需要按照业务需求进行逐条测试，费时费力。



之前的方案导致数据验证效率降低，而 nCompass 防火墙策略可视化平台通过采集新、旧防火墙的实时流量和策略配置，同步比对新、旧防火墙的策略配置和流量数据，使流量与配置结合，数据验证更加高效和准确。为运维人员在防火墙更换时提供有效的数据支撑，减轻变更后验证等工作量，提高运维效率。

第四章 产品价值

nCompass 防火墙策略可视化平台的问世，让防火墙配置和策略管理有了新的技术手段,帮助用户主动识别防火墙配置缺陷和漏洞,大幅提升了策略查询、合规检测、策略优化等常规工作的运营效率。



【与传统产品对比，nCompass 防火墙策略可视化平台让工作效率大幅提升】

nCompass 防火墙策略可视化平台上手简单，能大幅提升工作效率，具备极好的兼容性，与大多数防火墙轻松适配。

nCompass 的愿景，是希望能通过多源数据的采集、对接，实现运维管理数据的整合。依托于内置的智能算法、专家知识库以及多平台联动能力，成为用户的业务保障指挥平台，帮助用户实现从设备级运维到基于用户体验、基于业务交易的场景化运维。

nCompass 系列产品可以在整个运维体系中，无论是在网络运维、安全运维、应用运维还是业务运维部门中，发挥其数据整合能力、智能分析的能力，为各个部门的运营工作，提供数据支撑，提升数字化转型的能力。

第五章 公司介绍

智维数据，全称是北京智维盈讯网络科技有限公司，成立于 2015 年，智维数据是一家使用全新智能分析软件技术，改变企业对网络流量数据的消费场景，提升用户在 IT 网络运维及安全上的响应能力的企业服务公司，致力于打造技术领先的智能流量数据分析平台。

核心产品 **nCompass 网络流量分析平台**可以接纳流量，Trafficlog 等各种数据源，通过规则引擎进行动态数据分析与展现，通过流数据采集，策略检索，AI 智能算法，知识图谱，可视化一体化平台，帮助用户清晰了解流量中应用及业务流的不同维度的状态，将故障与隐患在从事后排障提升到了事中预警，为用户实现机器的问题机器处理，帮助用户快速提升智能运维、安全、业务数据分析的能力、效率和准确性。

该能力已经被全球领导厂商和各行业头部企业认可并完成数据对接与合作。公司从 15 年成立至今，服务于金融、电力、医疗、政企、互联网等多行业，服务客户包含中国银行、民生银行、浦发银行、华夏银行、中信证券、中国人寿、银联商务、中金集团、中石油、中石化、国家电网、中国联通、中山医院、海尔集团、上海韵达等，累计合作头部客户超过百余家，得到客户的一致认可。


中国银行 BANK OF CHINA
招商银行 CHINA MERCHANTS BANK
中国民生银行 CHINA MINSHENG BANK
华夏银行 HUAXIA BANK
中信银行 CHINA CITIC BANK
浦发银行 SPD BANK
国家开发银行 CHINA DEVELOPMENT BANK
中原银行 ZHONGYUAN BANK
江苏银行 BANK OF JIANGSU
郑州银行 BANK OF ZHENGZHOU
大连银行 BANK OF DALIAN
厦门银行 Xiamen Bank
宁夏银行 BANK OF NINGXIA
山东城商行合作联盟 Shandong City Commercial Banks Alliance
BEA東亞銀行
银联商务 ChinaUMS
CICC 中金公司
中信证券 CITIC SECURITIES
平安证券
宏信证券 HONGXIN SECURITIES
新时代证券 New Times Securities
中国人寿财产保险股份有限公司 China Life Property & Casualty Insurance Company Limited
中国太平 CHINA TAIPING
嘉实基金 Harvest Fund
易方达
国家信息中心 国家电子政务外网管理中心
新华社 XINHUA NEWS AGENCY
人民网 people.cn
国家税务总局 State Taxation Administration
教育部考试中心 National Education Examinations Authority
中国石油
SINOPEC
国家电网 STATE GRID
中国南方电网 CHINA SOUTHERN POWER GRID
ENN 新奥
中国铁路总公司 CHINA RAILWAY
北京中科院软件中心有限公司 Software Engineering Center Chinese Academy of Sciences
郑州地铁 ZHENGZHOU METRO
市政交通一卡通
中华人民共和国福州海关 FUZHOU CUSTOMS DISTRICT P.R.CHINA
China unicom 中国联通
国美云服 gyun.com
Haier 海尔
韵达 EXPRESS
oppo
上海大众动力总成有限公司
sina 新浪
HITACHI 日立 Inspire the Next
TOYOTA

第六章 nCompass 产品系列

作为国内**率先实现全流量数据源智能分析的大数据公司，智维数据以流量数据作为切入点，结合日志、配置、CMDB、拨测、Netflow、Telemetry 等多种数据源，通过系统内置的 AI 算法库，分析海量运维数据，准确发现问题，进而从决策层面进一步提高运维效率。**从根本上改变了传统 IT 运维管理依靠工具+人工经验的模式，为服务企业提升数据挖掘及应用创新能力。

智维数据的产品系列可服务网络、安全、应用、业务等多类别场景。

nCompass 产品系列

第七章 联系我们

北京总部：

地址：北京市朝阳区八里庄西里 99 号住邦 2000 二号楼 807

电话：400-666-8216

上海办事处：

地址：上海市静安区大宁中心广场三期灵石路 718 号 A7202

电话：400-666-8216

广州办事处：

地址：广州市天河区天河北 906 号高科大厦 A 座 1906

电话：400-666-8216

深圳办事处：

地址：深圳市南山区高新科技园南十二路九洲电器大厦 B 座 3 层 F 室

电话：400-666-8216

公司网址：

www.ncmps.com

邮箱：

技术支持：support@ncmps.com

市场或合作渠道：marketing@ncmps.com