绿盟安全配置核查系统

产品白皮书

目录

插图索引

前言

信息化建设中，信息安全风险检查与评估是信息安全保障工作的基础性工作和重要环节，贯穿于网络和信息系统建设、工程验收、运行维护等设备运行的全部生命周期。很多大型企业及政府机构都明确要求进行定期安全风险检查，并颁布了明确的信息系统安全风险检查指导性文件。

信息系统配置操作是否安全是安全风险的重要方面，安全配置错误一般是人员操作失误导致，而满足大量信息系统设备的安全配置要求，对人员业务水平、技术水平要求相对较高，所以一些行业和大型企业制定了针对自身业务系统特点的配置检查 Checklist 和操作指南，而国务院《中华人民共和国计算机信息系统安全保护条例》（147 号令）以及公安部颁布的一系列信息安全等级保护标准，也明确了信息系统安全等级保护测评的纲领性要求。

行业规范和等级保护纲领性规范要求让运维人员有了检查安全风险的标杆，但是面对网络中种类繁杂、数量众多的设备和软件，如何快速、有效的检查设备，又如何集中收集核查的结果，以及制作风险审核报告，并且最终识别那些与安全规范不符合的项目，以达到整改合规的要求，这些是网络运维人员面临的难题。

在此背景下，绿盟科技推出了专用检查工具——绿盟安全配置核查系统（NSFOCUS Benchmark Verification System， 简称：NSFOCUS BVS）系列产品。该产品基于绿盟科技多年安全服务和等级保护实施的经验积累，形成完善的安全配置知识库，该知识库涵盖了操作系统、网络设备、数据库、中间件等多类设备及系统的安全配置加固建议，通过该知识库可以全面的指导 IT 信息系统的安全配置及加固工作。特别是通过该产品能够采用机器语言，自动化的进行安全配置检查，从而节省传统的手动单点安全配置检查的时间，并避免传统人工检查方式所带来的失误风险，同时能够出具详细的检测报告。它可以大大提高您检查结果的准确性和合规性，节省您的时间成本，让检查工作变得简单。

一. 为什么要安全配置检查

在经济全球化和信息技术飞速发展的今天，支撑业务运行的信息系统已经变得越来越重要，甚至已经已广泛地融合于社会和国民经济的各个领域。如何保障业务的持续运行，与恶意访问者的持续攻防对抗，是信息安全运维人员需要面对的现实问题。据统计，每年因为信息安全及网络犯罪导致的直接经济损失要超过 2000 亿元人民币。因此，配合安全制度要求，

对信息系统进行定期安全漏洞修补以及人员配置操作进行安全检查，已经成为安全运维人员的日常性工作。

但是对网络中种类繁多的设备和软件，真正完成满足安全要求的系统配置检查和修复，需要安全运维人员熟悉业务系统并有较高的技术能力和经验。鉴于此，国内许多企业和行业制定了安全配置指导标准和规范。

依据企业和行业安全配置指导标准和规范进行安全配置检查，是对信息系统安全的最基本要求，通过采用统一的安全配置标准来规范技术人员在各类系统上的日常操作，让运维人员有了检查默认风险的标杆，但安全运维人员在实际工作中仍然会遇到

- 安全配置检查及问题修复都需人工进行，对检查人员的技能和经验要求较高；
- 做一次普及性的细致检查耗费时间较长，而如果改成抽查则检查的全面性就很差；
- 自查和检查都需要登录系统进行，对象越多工作越繁琐，工作效率也不高；
- 每项检查都要人工记录，稍有疏漏就需要重新补测。
- ……

对自查或检查人员来说，需要花费大量的时间和精力来检查设备、收集数据、制作和审核风险报告，以识别各项不符合安全规范要求的系统。如何快速有效的在新业务系统上实现上线安全检查、第三方入网安全检查、合规安全检查（上级检查）、日常安全检查等全方位设备检查，又如何集中收集核查的结果，以及制作风险审核报告，并且最终识别那些与安全规范不符合的项目，以达到整改合规的要求，这些是网络运维人员面临的新的难题。

二. 遵循等级保护进行配置检查的实践

等级保护是我国促进信息安全发展的一项基本制度，国家围绕等级保护制度制定了一系列的管理规范和技术标准，这些规范和标准明确了信息系统分等级开展实施、监督、管理工作的基本要求。

等级保护规划和技术标准要求是原则性的指导要求，在实际工作中，如何参考等级保护要求，对每一个业务系统的每一种设备类型进行安全配置检查并没有明确的技术指引，这需要安全运维人员以及安全厂商在实践中不断摸索。

绿盟科技服务团队作为专业的安全专家，参与了大量业务系统的等级保护实施和维护工作，在实际工作中根据等级保护定级，对信息系统所属资产进行全面安全检查，并给出了安全改进意见。经过多年的经验和技术积累，并结合经过市场验证的绿盟安全配置核查系统，推出了新版的绿盟安全配置核查系统－等级保护专版，能够根据等级保护资产定级，维护业

务系统资产信息，并提供符合不同等级保护级别的安全配置检查模板近 50 种，能对大多数常见操作系统、网络设备、数据库、中间件进行检查，并出具等级保护符合性报告。

三. 绿盟安全配置核查系统

基于多年安全服务的执着实践，绿盟科技形成了国内最完善的专业安全服务体系和专业安全服务方法论，根据经验总结了完善的安全配置检查体系，同时结合用户对自动化安全评估产品的实际应用需求，自主研发了绿盟安全配置核查系统（NSFOCUS Benchmark Verification System， 简称：NSFOCUS BVS）。

NSFOCUS BVS 具备符合多个行业安全配置要求的安全配置知识库，以及绿盟科技专家推荐的安全配置知识库，全面的指导 IT 信息系统的安全配置及加固工作，保障安全运维并满足行业规划要求。同时也根据等级保护定级、系统建设、等级测评、监督检查各个环节要求，完善了产品操作功能，保障等级保护工作高效准确执行。

NSFOCUS BVS 通过自动化的进行安全配置检查，从而节省传统的手动单点安全配置检查的时间，并避免传统人工检查方式所带来的失误风险，同时能够出具详细的检测报告。它可以大大提高您检查结果的准确性和合规性，节省您的时间成本，让检查工作变得简单，是您身边专业的“安全配置专家”。

- 丰富、权威的安全配置检查知识库，经过 NSFOCUS 安全团队实践考验，为业务系统安全配置检查及加固提供专业指导。
- 结合等级保护进行安全配置检查，围绕等保定级开展业务系统资产管理、安全配置检查、安全配置报告和建议，保障等级保护工作准确高效执行。
- 结合授权认证系统自动化安全配置检查，减少人员维护业务系统账号的工作量，减少失误带来的账号信息泄露风险，提供安全配置检查工作效率。
- 多种部署和管理方式，简单的嵌入到安全管理体系中，并为集中安全管理系统提供基础数据，为安全管理提供全面准确的安全配置风险依据。

3.1 产品体系结构

NSFOCUS BVS 是基于 WEB 的管理方式，用户使用浏览器通过 SSL 加密通道和系统 WEB 界面模块进行交互，方便用户管理。NSFOCUS BVS 采用模块化设计，从底层到上层分为基础平台层、系统服务层、系统核心层、系统接入层,内部整体工作架构如下图所示。

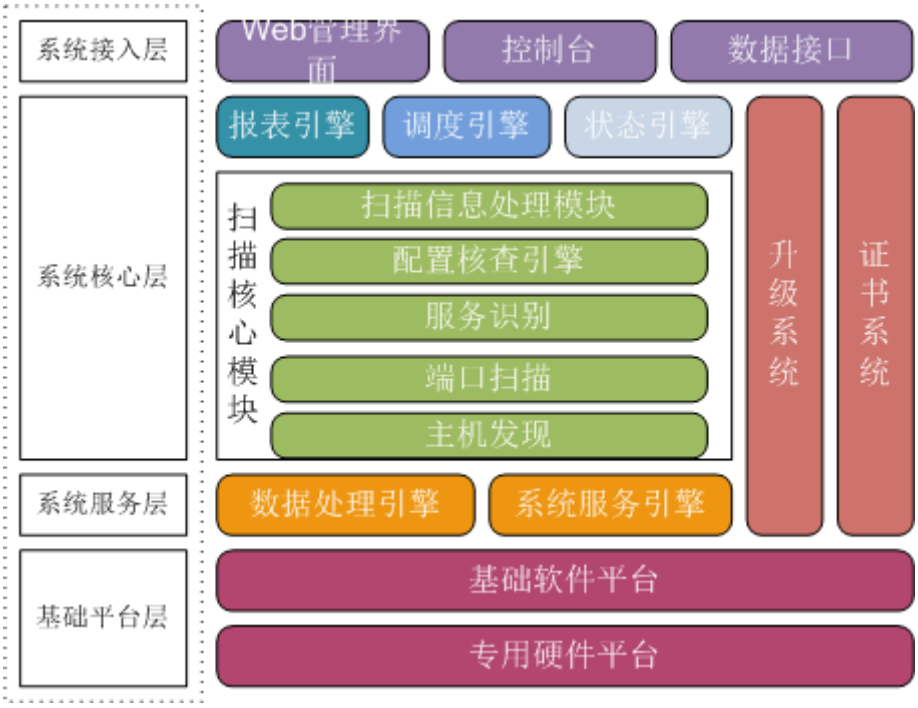

图 3.1　NSFOCUS BVS 整体模块图

3.1.1 基础平台层功能

基础平台包含专用硬件平台和基础软件平台。

专用硬件平台包含四款绿盟科技基础硬件平台，分别对应便携型号 RSAS NX3-P，精简型号 RSAS NX3-X，标准型号 RSAS NX3-S，企业版型号 RSAS NX3-E。

基础软件平台包含了绿盟科技定制操作系统、文件系统、硬盘加密解密、应用程序加密解密、输入输出加密解密、IPv4/IPv6 网络服务、内置数据库、Web 服务、程序运行环境等功能。

3.1.2 系统服务层功能

系统服务层包含数据处理引擎和系统服务引擎。

数据处理引擎是系统内部的数据接口，提供了数据库访问、数据缓存、数据同步等功能。数据处理引擎屏蔽了数据库系统操作的细节，减少数据库的连接，优化数据库的访问，缓存常用和计算复杂的数据，集中处理数据的逻辑，降低了其他功能模块的维护工作量。

系统服务引擎是系统内部的功能接口，提供了系统还原点备份与恢复、任务数据导入导出等功能。系统服务引擎解耦了前台操作和后台操作，后台功能以特定的权限运行，增加了系统的安全性。

3.1.3 系统核心层功能

系统核心层是产品的核心，提供最具竞争力的功能，包含配置核查，强大的模板等，有较多可扩展的模块和插件。

报表引擎是报表展示的核心处理模块，能够提供 HTML、WORD、EXCEL、PDF 等多种报表格式。

调度引擎是扫描工作的协调中心，根据用户操作的不同可能有立即执行的任务、定时执行的任务、周期执行的任务等，检测出任务的类型和优先级，进行者配置检查。

状态引擎是系统状态的协调中心，主要包含系统资源状态信息、系统的授权证书信息、BDB 配置项、任务执行进度信息、升级进度信息等。

证书系统提供了产品可授权使用的信息，包含购买用户、设备 HASH 值、授权 IP 数、授权使用模块、授权起止信息等。

升级系统提供了产品更新的能力，为扫描插件更新、产品功能更新、产品反馈修改等提供了可能。

3.1.4 系统接入层功能

系统接入层包含了用户通过浏览器访问 Web 页面、通过串口访问控制台、通过数据接口进行数据交互等方式，其中数据接口包含进行二次开发的数据接口、A 接口、SNMP Trap 等。

3.2 产品特色

3.2.1 丰富、权威的 Checklist 知识库

绿盟科技拥有一支业内领先的安全服务团队，拥有多位 PMP、CISA、BS7799 LA、ISO 27001 LA、CISSP、CISP、CCIE、CIW、COBIT、ITIL 等国际/国内认证专家，经过 7 年专业安全服务的执着实践，形成了国内最完善的专业安全服务体系和专业安全服务方法论，制定了完善详细的安全配置检查点。

经过专业团队不断在安全服务实践中进行 Checklist 知识库的完善，NSFOCUS BVS 产品已经支持近 30 种网络系统类型配置检查能力，覆盖操作系统、数据库、网络设备、中间件等常见网络设备。另外，产品还支持符合移动、电信等多个行业性质规范的配置检查模板，以及满足等级保护要求的配置检查模板，形成了经过专家在实践中验证的权威、完备的 Checklist 知识库。

3.2.2 结合等级保护的安全配置检查

在等级保护检查、测评、整改工作过程中，对定级业务系统进行对应级别的安全风险检查是技术方面的必要工作。NSFOCUS BVS 产品根据绿盟科技安全服务团队的经验积累，对国家等级保护规范进行了细化整理，把技术要求落实到每一种网络设备的配置检查工作上

NSFOCUS BVS 能够结合等级保护工作过程，对业务系统资产进行等保定级跟踪，根据资产定级自动进行对应级别的安全配置检查，对合规情况进行等保符合性报告，保证系统建设符合等保要求、促使等保监督检查工作高效执行。

3.2.3 结合授权认证系统简化配置检查操作

安全配置检查工作需要具备被检查目标的账号、密码等授权信息，登录到被检查目标设备中，执行配置查看命令列举配置信息，然后与规范要求进行对比，得到合规及不合规的配置项，自动化的配置检查过程也类似，需要目标系统的账号、密码等授权信息，对数量众多的网络设备的安全配置检查，每一组目标系统的账号、密码由管理员维护和录入，工作量巨大，也容易出错。

一些企业部门已经部署了 4A 认证授权系统或者堡垒机运维审计系统，能够很好的维护业务系统中各主机、设备的登录授权信息，NSFOCUS BVS 充分考虑配置检查工作的方便性，能够和 4A 系统或者堡垒机系统对接，自动化获取被检查目标系统的登录授权信息，批量检查业务系统安全配置，使配置检查操作简单易用。

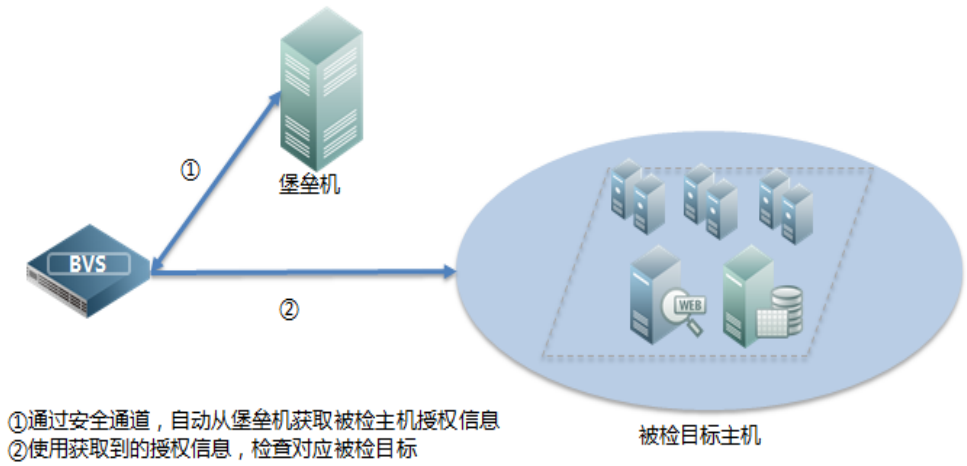

图 3.2 NSFOCUS BVS 通过堡垒机获取授权信息

3.2.4 自定义安全配置检查项目

通常网络环境的情况是，设备类型逐渐增多，各种服务平台被应用，应用软件不断更新升级，这些变化给安全配置检查带来一定的困难。

作为 Checklist 知识库的补充，NSFOCUS BVS 提供自定义安全配置检查功能，可以由用户根据需要或者行业标准，自行制定对目标系统执行的各种安全配置检查操作，可以形成针对自身企业或行业的自定义安全配置检查模板。

自定义安全配置检查的功能让安全管理员能够很好的适应网络情况的变化，对产品暂不支持的安全规范或配置检查点，都可以通过自定义安全配置检查功能轻松实现。

3.2.5 基于业务系统的资产管理

安全配置检查系统上线之前，要对业务系统资产进行梳理，收集资产系统类型、授权认证、访问跳转等信息，对资产按照业务系统进行组织录入到安全配置检查工具中，尤其是经过等级保护定级的业务系统，资产信息要记录等级保护定级信息。

NSFOCUS BVS 能够灵活的根据业务系统 IP 地址群组组织资产信息，梳理后的资产信息形成直观的资产树状结构视图展示，并存储资产系统类型、权重、等保定级等信息。围绕业务系统资产信息，可以方便进行下一步的安全配置检查、合规性报告、整改审计等各项工作。

3.2.6 灵活的部署方案

业务系统的多样性，决定了 IT 网络建设环境不尽相同，对于脆弱性管理产品来讲，没有灵活的部署方案适应多种网络环境，就意味着有些网络无法接入或者建设成本极大增加。

NSFOCUS BVS 提供了多种灵活的部署方式，能够满足复杂的网络环境下的部署，并且优先应用轻量级部署方案，最大程度降低安全建设成本。NSFOCUS BVS 支持单机单网络、单机多网络、安全平台分布式管理、跳板机跳转等多种部署方式，灵活适应各种网络拓扑环境，便于扩展。

另外，考虑到虚拟化和 IPv6 网络的逐步应用，NSFOCUS BVS 也支持通过虚拟化镜像方式在虚拟化环境下直接部署，支持 IPv6 网络环境下的部署和漏洞扫描。

3.3 实施过程

NSFOCUS BVS 上线到能够开始投入日常运维，需要经过 3 个步骤的准备：系统部署上线、业务系统资产梳理、业务系统安全配置基线调整和确定。NSFCOCUS BVS 能支持多种网络环境，部署简单，下面主要介绍一下业务系统资产梳理、安全基线调整和确定过程。

3.3.1 业务系统资产梳理

业务系统中每一个网络设备都是整个系统安全风险的脆弱性环节，对每一个业务系统资产进行梳理，了解资产的网络拓扑划分，有哪些业务支持系统类型，以及网络边界，所有这些工作是进行系统安全配置检查的预备性基础工作。

对业务系统资产的梳理需要关注低层支撑系统，如操作系统，和支撑的数据库、网络中间件，以及网络边界的路由器、交换机、防火墙等设备，收集所有这些系统的厂商、型号、版本等信息、并整理这些系统具备管理员权限的账号授权信息，是否需要经过跳板机跳转才能访问。对于系统账号信息建议收集整理后单独保存，保障信息的安全性。

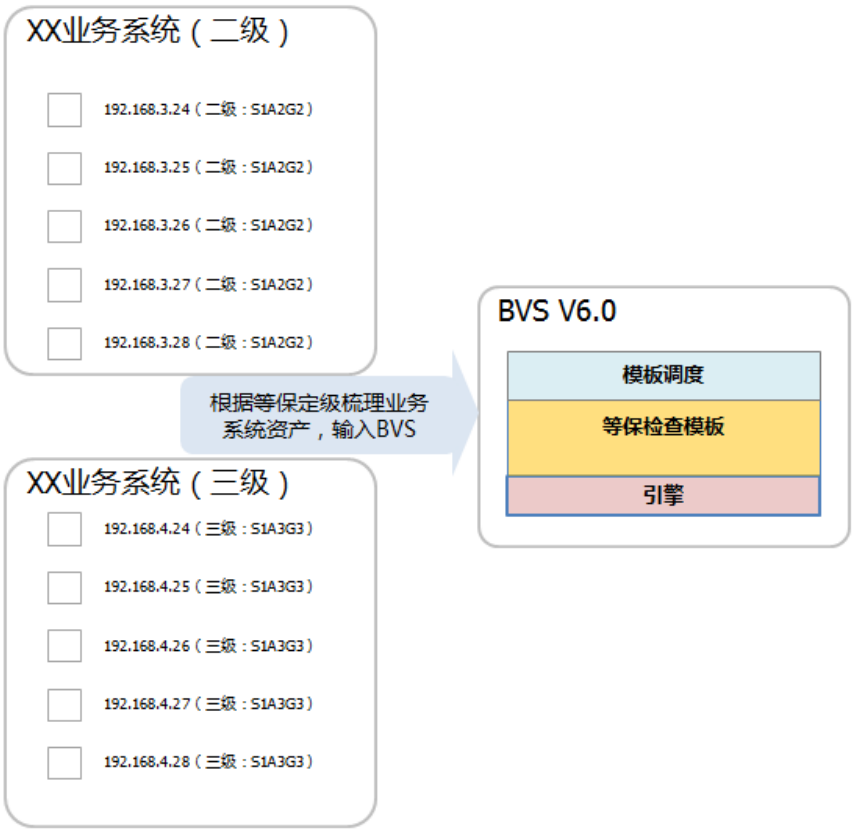

图 3.3 NSFOCUS BVS 业务系统资产定级信息梳理示意

资产信息录入整理后，即可录入到 NSFOCUS BVS 产品中，NSFOCUS BVS 提供通过离线文件便捷的导入到产品中的功能。另外，对于需要满足等级保护要求的系统，还需要录入资产的等级保护定级信息。

图 3.4　NSFOCUS BVS 业务系统资产定级信息管理

3.3.2 业务系统安全配置基线确定

安全配置规范中的要求，对不同的业务系统不应该是一成不变的，如何即满足业务系统的可用性和有满足业务系统的安全性是一个综合考虑的过程，每一类业务系统的业务要求不同，可能需要安全配置的要求也进行对应的调整，对业务系统运行有影响的安全配置需要慎重采用。所以在安全配置核查系统上线前，安全配置规范需要根据不同业务系统的特性进行调整，形成针对每一类业务系统的安全配置基线，是保障业务可用和系统安全的重要过程。

NSFOCUS BVS 支持安全配置检查模板的微调修改和全新安全配置检查模板的自定义，通过这个这两种功能，很好的支持了上线前业务系统安全配置基线确定工作的要求。

图 3.5　NSFOCUS BVS 配置检查模板修改

3.4 典型应用

NSFOCUS BVS 贴合安全管理流程，能够支持业务系统资产管理、安全配置检查、安全风险报警、安全风险审计等各个安全配置检查环境的使用，并能够适应多种网络环境，灵活的部署在用户网络中进行检查。NSFOCUS BVS 常被应用于监管机构安全检查、安全运维工作的定期安全风险检查、以及为第三方安全管理平台提供安全风险数据。

3.4.1 监督、检查或小规模网络安全运维

小规模网络下单独部署漏洞扫描产品，完成全部网络的安全检查，是传统使用方法。NSFOCUS BVS 可以部署应用在小规模网络安全运维环境中，另外，针对需要携带设备到现场的监督检查使用要求，提供了便携式工业硬件的 BVS NX3-P 型号。使用 NSFOCUS BVS，通过简单部署即可完成业务系统安全配置检查工作

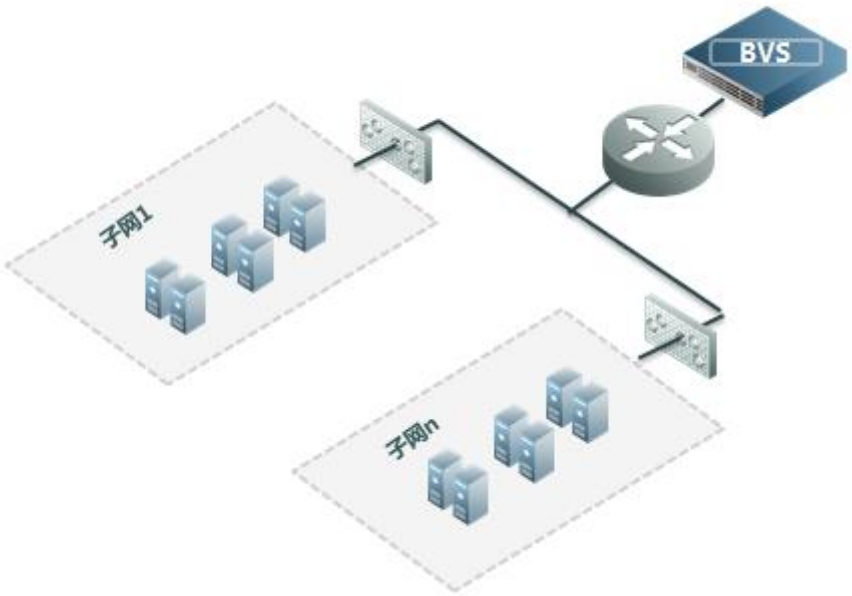

图 3.6　NSFOCUS BVS 单机部署

3.4.2 中小规模多子网安全运维

对于中小企业，网络规模不大，但一般会划分为多个业务子网，每个子网都分别部署安全配置核查系统成本过高，而要求子网防火墙开放安全配置核查设备的访问权限，又带来安全风险。NSFOCUS BVS 提供多条链路检查方式，系统提供多个检查网口，每个网口可以通过配置接入不同子网，无需防火墙单独开放规则，节约成本的同时也避免了风险。

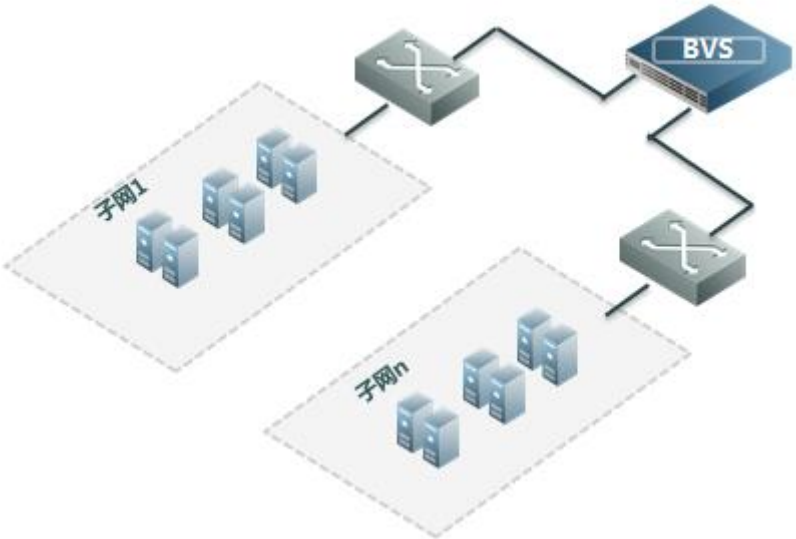

图 3.7　NSFOCUS BVS 单机多网口多子网接入

3.4.3 第三方系统集成

安全运维各项工作不应该是孤立的，经常需要把各种安全设备的数据收集后集中分析，概括性的了解系统中安全风险情况，企事业单位一般会上线安全管理中心来完成安全数据集中分析的工作。

NSFOCUS BVS 支持开放式的管理接口，通过接口可以实现安全管理中心对配置检查任务、检查结果分析的操作接管，NSFOCUS BVS 作为执行引擎为安全管理中心提供安全配置检查结果数据。

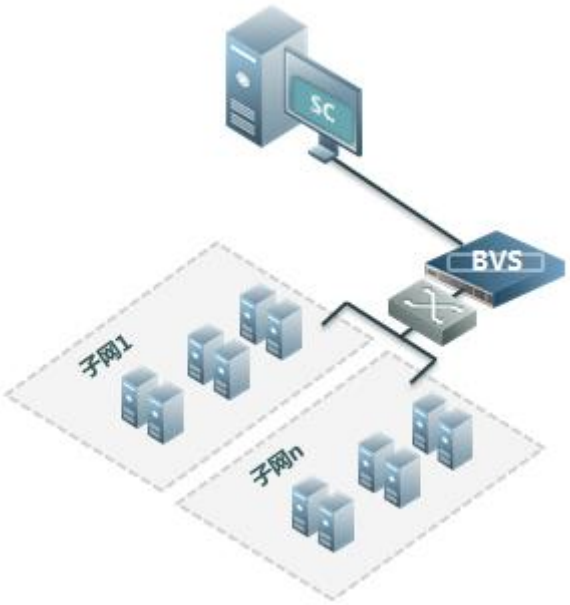

图 3.8 NSFOCUS BVS 接入第三方安全中心

3.4.4 大规模网络安全运维

在大中型企业中，通常是大规模跨地区的网络，NSFOCUS BVS 被分布式部署在各地区，在总部进行集中管理，NSFOCUS BVS 提供集中管理软件，实现系统的分布式部署能力。

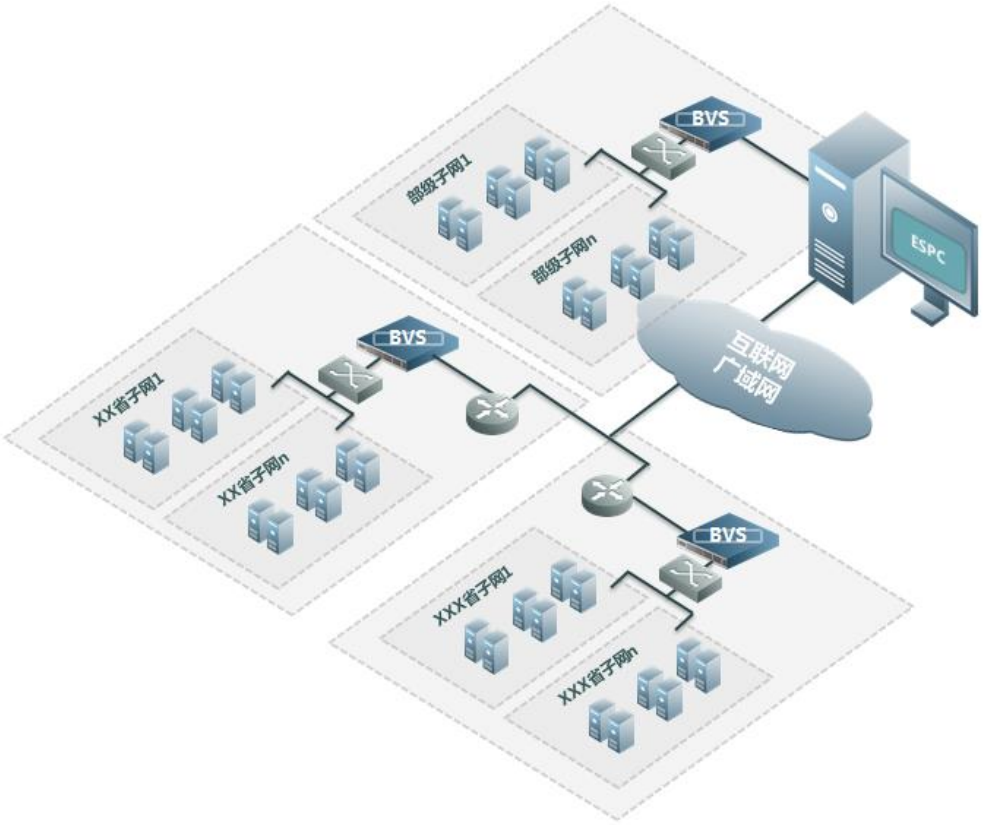

图 3.9 NSFOCUS BVS 分布式部署结构图

四. 结论

安全配置合规性要求，是 IT 业务系统安全性的基本安全要求，对各行各业安全规范要求的落地、对等级保护要求的具体化，建立和行之有效的检测手段是安全管理人员面临的最为重要和迫切的问题，也需要安全厂商要积极提供自动化的解决方案，帮助运维人员面对网络中种类繁杂、数量众多的设备和软件环境，快速、有效的检查设备，进行自动化的安全检查，以及制作风险审核报告，并且最终识别那些与安全规范不符合的项目，以达到整改合规的要求。

基于多年安全服务的执着实践，同时结合用户对安全评估产品的实际应用需求，绿盟科技推出了专用检查工具——绿盟安全配置核查系统（NSFOCUS BVS）系列产品，它具备符合多个行业安全配置要求的安全配置知识库，以及绿盟科技专家推荐的安全配置知识库，全面的指导 IT 信息系统的安全配置及加固工作，保障安全运维并满足行业规划要求。同时也根据等级保护定级、系统建设、等级测评、监督检查各个环节要求，完善了产品操作功能，保障等级保护工作高效准确执行。