# 绿盟远程安全评估系统

# 产品白皮书

**【绿盟科技】**

# 目录

# 插图索引

# 一. 攻防威胁的变化

利用安全漏洞进行网络攻击的互联网安全问题，好像阳光下的阴影，始终伴随着互联网行业的应用发展。近些年，网络安全威胁的形式也出现了不同的变化，攻击方式从单个兴趣爱好者随意下载的简单工具攻击，向有组织的专业技术人员专门编写的攻击程序转变，攻击目的从证明个人技术实力向商业或国家信息窃取转变。

新攻击方式的变化，仍然会利用各种漏洞，比如：Google 极光攻击事件中被利用的 IE 浏览器溢出漏洞，Shady RAT 攻击事件中被利用的 EXCEL 程序的 FEATHEADER 远程代码执行漏洞。其实攻击者攻击过程并非都会利用 0day 漏洞，比如 FEATHEADER 远程代码执行漏洞，实际上，大多数攻击都是利用的已知漏洞。对于攻击者来说，IT 系统的方方面面都存在脆弱性，这些方面包括常见的操作系统漏洞、应用系统漏洞、弱口令，也包括容易被忽略的错误安全配置问题，以及违反最小化原则开放的不必要的账号、服务、端口等。

在新攻击威胁已经转变的情况下，网络安全管理人员仍然在用传统的漏洞扫描工具，每季度或半年，仅仅进行网络系统漏洞检查，无法真正达到通过安全检查事先修补网络安全脆弱性的目的。网络安全管理人员需要对网络安全脆弱性进行全方位的检查，对存在的安全脆弱性问题一一修补，并保证修补的正确完成。这个过程的工作极为繁琐，传统的漏洞扫描产品从脆弱性检查覆盖程度，到分析报告对管理人员帮助的有效性方面，已经无法胜任。

# 二. 环境变化带来的问题

随着 IT 建设的发展，很多政府机构及大中型企业，都建立了跨地区的办公或业务网络，系统安全管理工作由不同地区的安全运维人员承担，总部集中监管。按照安全扫描原则，漏洞扫描产品一般被部署到离扫描目标最近的位置，这就形成了漏洞扫描产品分布式部署的要求。

对 IT 系统来说，网络中每个点的安全情况都会对整个 IT 系统造成威胁，运维人员不但要关注某个地区的安全情况，还需要关注整个 IT 系统的安全风险情况。这要求有相应的漏洞管理平台对整个网络中的漏洞扫描产品进行集中管理，收集信息，汇总分析，让运维人员掌握整体网络安全状况。

另外，虚拟化系统也已经在各个行业得到了广泛应用，IPv6 网络也将在今年实现商业化，新技术的应用带来了新的安全威胁，要求漏洞扫描产品能够适应新的的环境，实现完整的系统脆弱性扫描。

# 三. 新一代漏洞管理产品必备特性

攻防威胁的转变和系统环境的变化，要求漏洞扫描产品能够及时应对这些变化，为系统安全脆弱性评估提供有力手段，新一代的漏洞管理产品应该具备以下特性：

- 能够全面发现信息系统存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告
- 能够快速定位风险类型、区域、严重程度，直观展示安全风险
- 能够结合安全管理制度，支持安全风险预警、检查、分级管理、修复、审计流程，并监督流程的执行
- 能够提供多种灵活部署方式，适应复杂的网络环境下的部署，并尽量控制降低安全建设成本
- 能够在虚拟化环境、IPv6 环境中部署和检测其脆弱性

# 四. 绿盟远程安全评估系统

绿盟远程安全评估系统（NSFOCUS Remote Security Assessment 简称：NSFOCUS RSAS）是绿盟科技结合多年的漏洞挖掘和安全服务实践经验，自主研发的新一代漏洞管理产品，它高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面，是您身边专业的“漏洞管理专家”。

- **全方位系统脆弱性发现**：全面发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告。

- **从海量数据中快速定位风险：**提供仪表盘报告和分析方式，在大规模安全检查后，快速定位风险类型、区域、严重程度，根据资产重要性进行排序，可以从仪表盘报告直接定位到具体主机具体漏洞。
- **融入并促进安全管理流程：**安全管理不只是技术，更重要的是通过流程制度对安全脆弱性风险进行控制，产品结合安全管理制度，支持安全风险预警、检查、分级管理、修复、审计流程，并监督流程的执行。
- **灵活的部署方案：**支持单机单网络、单机多网络、分布式部署、扫描代理等多种接入方式，灵活适应各种网络拓扑环境，降低成本，便于扩展。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。

## 4.1 产品体系结构

NSFOCUS RSAS V6.0 采用模块化设计，内部分为基础平台层、系统服务层、系统核心层、系统接入层，每层内部划分不同的功能模块，整体工作架构如图 4.1 所示。

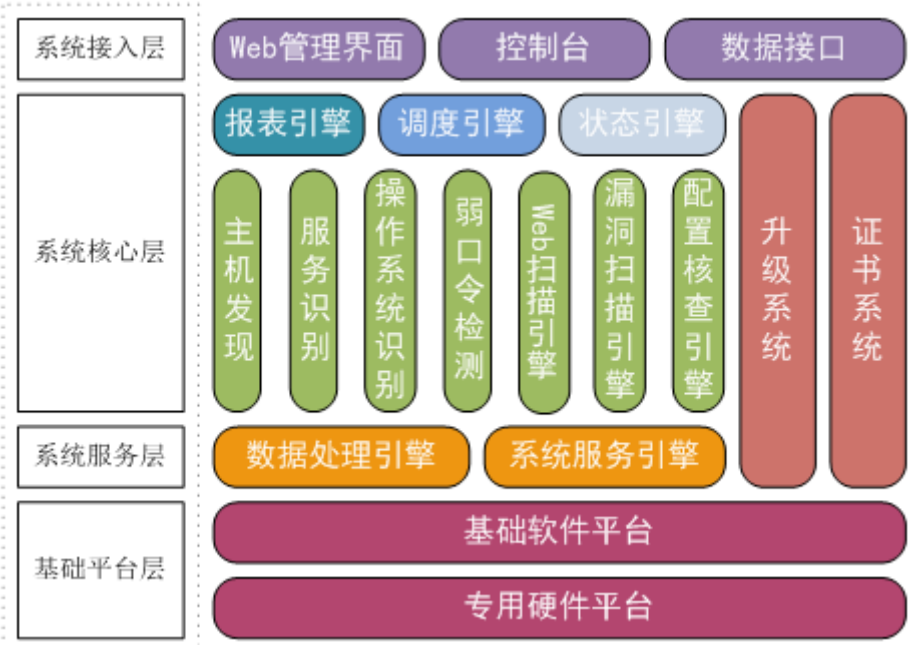



图 4.1　NSFOCUS RSAS 整体架构图

### 4.1.1 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。

专用硬件平台包含五款绿盟科技基础硬件平台，分别对应便携型号 RSAS NX3-P 与 RSAS NX3-A，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。

### 4.1.2 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。

### 4.1.3 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，包含主机发现、操作系统识别、服务识别、弱口令检测、漏洞扫描、配置核查、漏洞验证等，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、XML 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，进行漏洞扫描或者配置检查、口令猜测。

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。

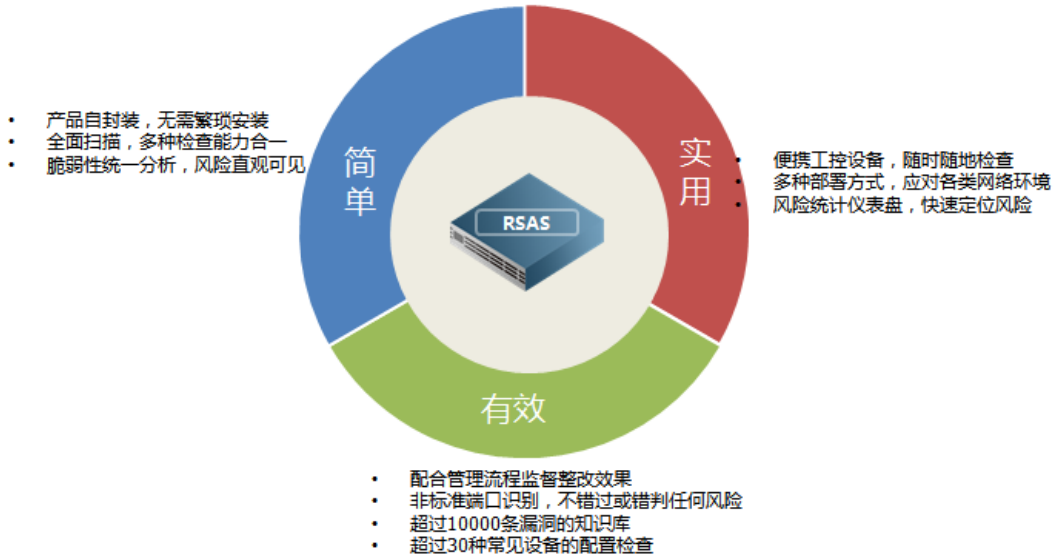
证书系统提供了产品可授权使用的信息，包含购买用户、设备 HASH 值、授权 IP 数、授权使用模块、授权起止信息等。

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。

### 4.1.4 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，其中数据接口包含第三方平台管理数据接口、SNMP Trap。

## 4.2 产品特色




### 4.2.1 多种检查能力合一，全面系统脆弱性发现

对于攻击者来说，IT 系统的方方面面都存在脆弱性，这些方面包括常见的操作系统漏洞、应用系统漏洞、弱口令，也包括容易被忽略的错误安全配置问题，以及违反最小化原则开放的不必要的账号、服务、端口等。


绿盟远程安全评估系统能够全方位检测 IT 系统存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

### 4.2.2 风险统一分析

目前市场上有很多独立的漏洞扫描、配置检查、Web 应用扫描产品，对信息系统进行安全检查后，分别得到不同的检查报告，互相之间没有联系，实际上不同脆弱性的扫描结果都从不同方面反映网络系统的安全风险状态，要了解信息系统总体安全风险状况，需要对脆弱性的所有方面统一进行分析和评估。

绿盟远程安全评估系统支持全方位的安全漏洞、安全配置、应用系统安全漏洞扫描，通过绿盟科技专利安全风险计算方法，对网络系统中多个方面的安全脆弱性统一进行分析和风险评估，给出总体安全状态评价，全面掌握信息系统安全风险。

### 4.2.3 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。

绿盟远程安全评估系统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。绿盟远程安全评估系统支持单机单网络、单机多网络、分布式部署、扫描代理等多种接入方式，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，绿盟远程安全评估系统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。

### 4.2.4 独创便携工控设备，随时监督检查

安全管理体系中，定期或不定期的现场安全监督检查是必不可少的重要环节，安全检查工具是否便携，成为监督检查人员除了性能之外的重要考虑因素。

绿盟远程安全评估系统独创便携式工控设备，小巧轻便，普通笔记本包即可携带，在保证快速安全脆弱性扫描的基础上，方便携带进行现场监督检查，实现了性能和便携要求的和谐统一。

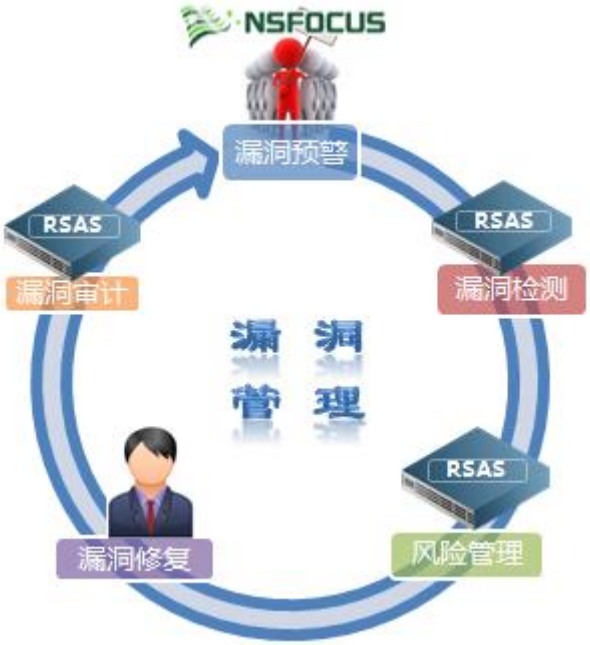
### 4.2.5 结合资产从海量数据快速定位风险

IT 系统规模越来越大，资产数量、漏洞数量、更多的脆弱性问题越来越多，汇总成大量的风险数据，传统的关注扫描漏洞、补丁修补的安全管理工作方式会使安全管理人员疲于应付，又不能保证对重要资产的及时修补。

绿盟远程安全评估系统在上线后，首先尽量收集 IT 系统环境信息，建立起 IT 资产关系列表。准备工作完成后，系统基于资产信息进行脆弱性扫描和分析报告。绿盟远程安全评估系统脆弱性扫描分析结果以仪表盘方式展示，从风险发生区域、类型、严重程度进行不同维度的分类分析报告，用户可以全局掌握安全风险，关注重点区域、重点资产，对严重问题优先修补。对于需要定位主机安全脆弱性的安全维护人员，通过直接点击仪表盘风险数据，可以逐级定位风险，直至定位到具体主机具体漏洞。绿盟远程安全评估系统也提供了强大的搜索功能，可以根据资产范围、风险程度等条件搜索定位风险。

### 4.2.6 融入并促进安全管理流程

安全管理不只是技术，更重要的是通过流程制度对安全脆弱性风险进行控制，很多公司制定了安全流程制度，但仍然有安全事故发生，人员对流程制度的执行起到关键作用，如何融入管理流程，并促进流程的执行是安全脆弱性管理产品需要解决的问题。




安全管理流程制度一般包括预警、检测、分析管理、修补、审计等几个环节，结合绿盟科技 NSFOCUS 安全研究团队的工作，绿盟远程安全评估系统能够参与安全流程中的预警、检测、分析管理、审计环节，并通过事件告警督促安全管理人员进行风险修补。

### 4.2.7 识别非标准端口，准确扫描服务漏洞

在 IT 系统安全管理中，经常会遇到由于业务需要而改变默认应用服务端口的情况，改变协议默认端口能够规避业务冲突、减少设备投入、充分利用资源，但某种协议在非标准端口上如何识别和扫描也成为安全管理产品需要解决的问题。

绿盟远程安全评估系统应用先进的非标准端口识别技术、以及丰富的协议指纹库，能够快速准确的识别非标准端口上的应用服务类型，并进一步进行漏洞检测，极大的避免了扫描过程 中的漏报和误报。

### 4.2.8 丰富的漏洞、配置知识库

绿盟科技 NSFOCUS 安全小组，有多位专职的研究员进行漏洞跟踪和漏洞前瞻性研究，并且为国际上的知名网络安全厂商提供相关漏洞的规则支持。NSFOCUS 安全小组负责 NSFOCUS RSAS 的漏洞知识库和检测规则的维护，除定期的每两周的升级外，重大漏洞的升级在全球首次发现后两天内完成。

依靠专业的 NSFOCUS 安全小组的研究积累，NSFOCUS RSAS 产品知识库已经有超过 10000 条系统漏洞信息，涵盖所有主流基础系统、应用系统、网络设备等网元对象；知识库中还提供 8 大类上百个版本的系统的配置检查库，提供绿盟科技作为专业安全厂商的加固修补建议，以及多个行业的安全配置检查标准。

## 4.3 典型应用方式

### 4.3.1 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。绿盟远程安全评估系统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 RSAS NX3-P 型号以及 RSAS NX3-A 型号。使用一套绿盟远程安全评估系统，通过简单部署即可全面检查业务系统的各种安全脆弱性问题。

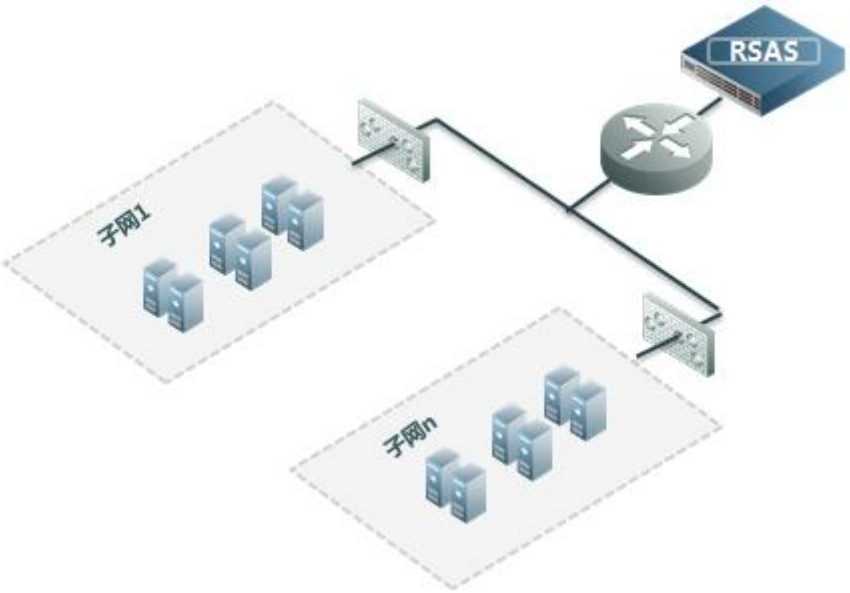



图 4.2　NSFOCUS RSAS 单机部署

### 4.3.2 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漏洞管理系统成本过高，而要求子网防火墙开放漏洞管理设备的访问权限，又带来安全风险。绿盟远程安全评估系统提供多条链路扫描方式，系统提供多个扫描口，每个扫描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。

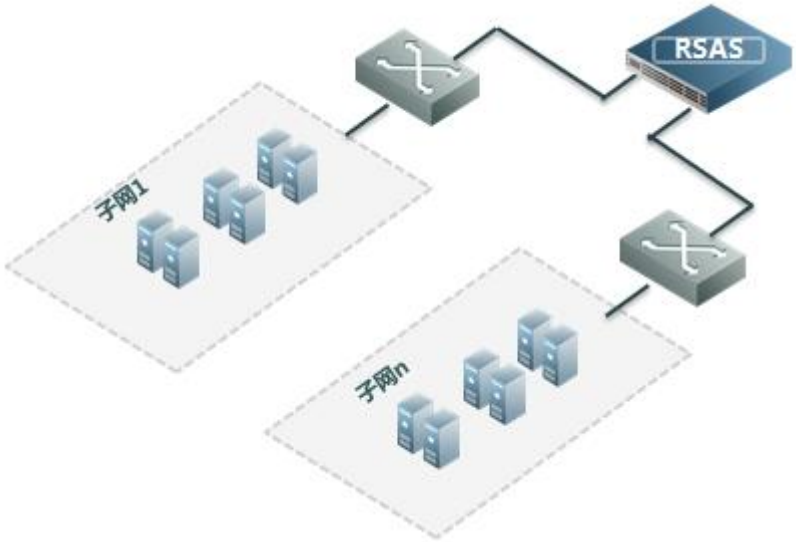



图 4.3 NSFOCUS RSAS 单机多网口多子网接入

### 4.3.3 大规模跨地区网络安全运维

在大中型企业中，通常是大规模跨地区的网络，漏洞管理产品分布式部署在各地区，在总部进行集中管理，绿盟远程安全评估系统提供集中管理软件（ESPC），实现系统的分布式部署能力。大型企业中通常网络环境复杂，上述绿盟远程安全评估系统多链路扫描、代理扫描方案也可能会混合应用在大规模部署环境中。

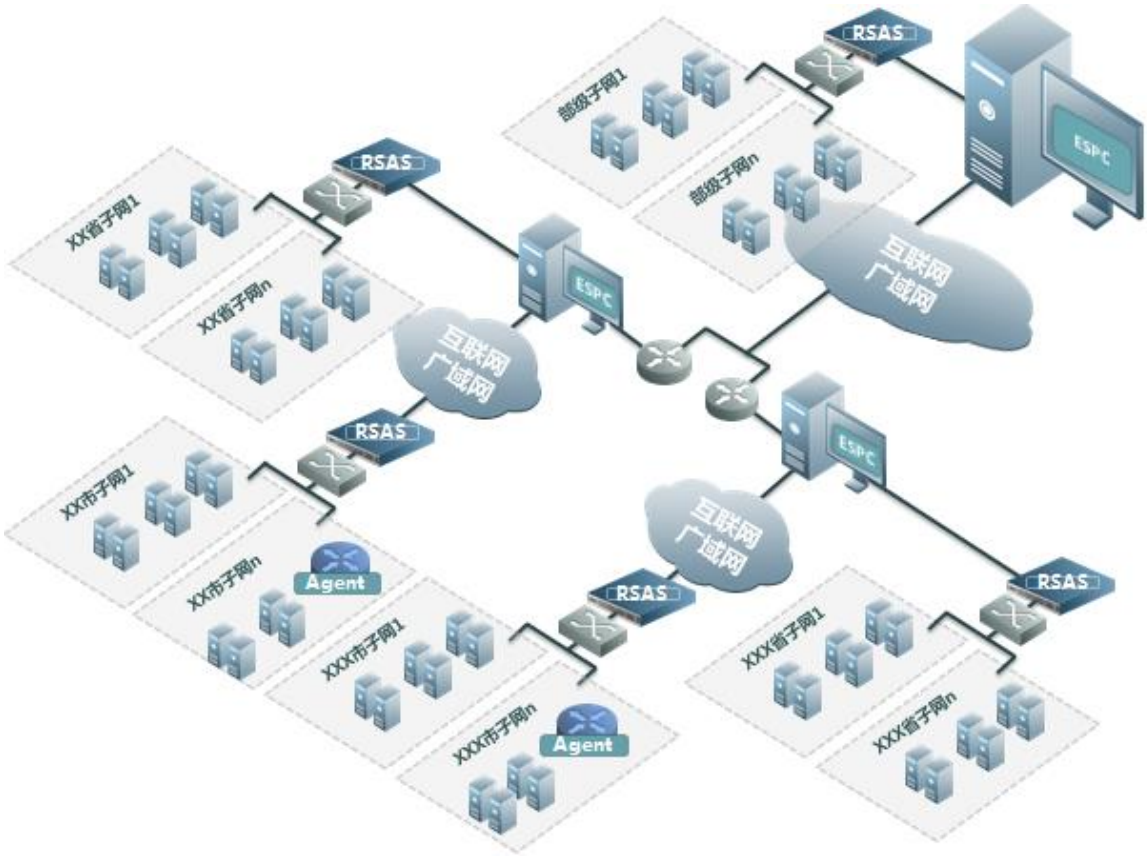



图 4.4 NSFOCUS RSAS 大规模部署

# 五. 结论

每年都有数以千计的网络安全漏洞被发现和公布，再加上攻击者手段的不断变化，用户的网络安全状况也随着被公布安全漏洞的增加而日益严峻。因此，安全评估对于绝大多数用户都是不容忽视的，用户必须比攻击者更早掌握自己网络安全漏洞并且做好适当的修补，才能够有效地预防入侵事件的发生。

事实证明，99%的攻击事件都是利用未修补的漏洞。许多已经部署防火墙、入侵检测系统和防病毒软件的企业仍然饱受漏洞入侵之苦，其中有更多受到蠕虫及其变种的破坏，造成巨大的经济损失。归根结底，其原因是用户缺乏一套完整的漏洞管理体系，未能落实定期评估与漏洞修补工作，忽视了漏洞的管理，最终漏洞成为攻击者实施攻击的有效途径，甚至成为蠕虫攻击的目标。

依托国内权威中文漏洞知识库和已在国际上享有盛名的 NSFOCUS 安全小组，绿盟远程安全评估系统已经是国际领先的漏洞管理产品之一，配合专业的 Web 扫描模块，它能够定期和持续地给用户提供全面可靠的安全评估服务，满足多种应用需求，并且提供完整的漏洞管理机制，有效降低用户网络和主机风险，更大限度地保证用户网络和系统的安全性和稳定性。