网站监控告警 服务白皮书V1.0

网世界 心归宿

网宿科技 全球领先的互联网基础设施平台

关注公众号，及时了解网宿产品与服务动态

400-010-0617 | www.wangsu.com

Content 目录

网宿监控告警服务隶属“网宿网盾”安全品牌旗下，能够帮助运维人员及时有效地了解到网站是否存在安全隐患、是否在遭受攻击、网络可用性等情况，支持多种告警方式，协助运维人员快速发现问题、定位问题、解决问题，为网站提供全方位的监控告警服务。

“网宿网盾”是网宿科技发布的云安全全新品牌，其业务全景主要覆盖网络安全、业务安全、内容安全、DNS 安全、源站可用性、传输安全、安全管理和安全评估等八大领域，“网宿网盾”依托高容量节点和自主研发的安全技术，构建出一套云端智能安全体系。

1.行业现状和挑战

随着互联网行业进入高度竞争状态，网站运维人员不但需要应对用户访问量增长所带来的访问压力，也需要时刻关注用户体验，保障服务质量。用户对安全性、访问速度有着越来越高的要求，网站可否访问、访问速度大大影响着用户的留存率。同时，随着攻击频发，网站的安全性也影响着用户对网站的信任。

- **IT 基础架构日益复杂，“响应式运维”已无法满足实际要求**

目前大部分 IT 运维工作主要通过“响应式”来保障系统及数据中心正常运营，在该模式下，运维人员处于被动状态，在问题出现后才疲于处理各种问题，耗费大量精力，且运维效率不理想。

- **漏洞频发，站点存在安全隐患**

随着漏洞挖掘技术的不断发展，攻击工具日益专业化、易用化，一些被广泛使用的基础组件的漏洞爆发频率越来越高，如：Bash 的 ShellShock 漏洞、OpenSSL 的 HeartBleed 漏洞、Struts2 的远程

任意代码执行漏洞等。而系统管理和运维人员对于不可预知的应用组件和依赖的安全漏洞无法及时发现和修补，进而可能导致漏洞被黑客利用进行窃取数据等，进而影响企业正常运作。

- **网络安全法，要求漏洞检查**

《网络安全法》于 2017 年 6 月 1 日起施行。其中规定网络运营者需履行“采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施”、“制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险”等安全义务。

2.服务介绍

2.1. 服务简介

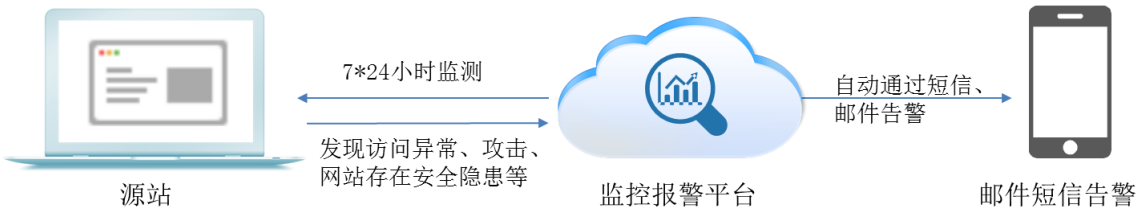
网宿“监控告警服务”能够帮助运维人员更加及时有效地了解站点是否存在安全隐患、是否在遭受攻击、可用性情况等，同时采用多种告警通知方式，协助运维人员快速发现问题、定位问题、解决问题。

2.2. 服务适用行业与场景

网宿“监控告警服务”适用于政府网站、企事业单位网站、电商网站、金融网站、社交网站和信息咨询网站等各行业站点。

2.3. 技术架构

网宿监控告警平台的架构如下图所示：



3.监控告警服务功能

网宿“监控告警服务”提供可用性监控告警、DNS 监控、网站弱点监控告警、内容安全检测、攻击监控告警、业务流量指数监测等服务。

3.1. 可用性监控告警

通过周期性模拟访客请求访问被监控站点，基于分布在全球各地的监控节点实时获取站点的响应状态和请求详情，如发现网站出现响应异常情况，将通过邮件、短信等方式告知站点相关人员，帮助运维人员第一时间察觉网站异常。

3.2. DNS 监控告警

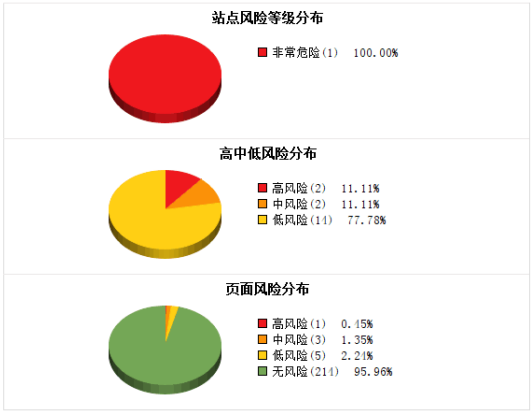
对域名解析服务器的可用率、响应时间及解析结果进行监控，在可用率、响应时间超出阈值、解析结果与指定不匹配时发出告警时，能即时通知运维人员。

3.3. 网站弱点监控告警

网宿安全团队通过自主挖掘与行业共享相结合的方式搜集漏洞信息并更新漏洞库，通过扫描等手段对网站的脆弱性进行检测，提供 SQL 注入、XSS、CSRF 等各类 Web 漏洞和第三方开源程序漏洞扫描服务，以及弱口令检测、安全配置错误检测，敏感信息检测等，挖掘 Web 应用中可能影响业务正常运行、敏感信息泄露等的漏洞，并对漏洞风险进行评级，输出网站弱点检测报告。

网站弱点检测报告如下：

任务名称	扫描[http://w[redacted]]
网络风险	风险值：9.8
信息统计	已发现链接数：375 已扫描链接数：173 已发现文件数：223 有漏洞文件数：33
下达任务的用户	zhangyc
站点统计	已扫描站点数：1 未扫描站点数：0 非常危险站点数：1
时间统计	开始：2017-02-17 16:03:25 结束：2017-02-17 16:33:17 耗时：29分钟52秒
版本信息	系统版本：V6.0R03F01SP09 插件版本：V6.0R03F00.67
任务说明	



3.4. 内容安全监测告警

对网页响应内容进行检测和分析，如发现敏感信息泄露、暗链、页面内容被篡改等，将生成告警消息。如下图所示：

时间	攻击IP	域名	URL	攻击类型	处理动作	详细信息
2017-08-23 18:25:59	[redacted]	www[redacted]cn	/t[redacted]n...	敏感信息泄露防护	报警	
2017-08-23 18:25:59	[redacted]	www[redacted]cn	/t[redacted]g/[redacted]...	敏感信息泄露防护	报警	
2017-08-23 18:22:36	[redacted]	www[redacted]cn	/t[redacted]ng[redacted]..	敏感信息泄露防护	报警	
2017-08-23 18:22:36	[redacted]	www[redacted]cn	/[redacted]m[redacted]	敏感信息泄露防护	报警	
2017-08-23 18:20:26	[redacted]	www[redacted]cn	[redacted]	敏感信息泄露防护	报警	
2017-08-23 18:20:25	[redacted]	www[redacted]cn	[redacted]	敏感信息泄露防护	报警	
2017-08-23 18:20:18	[redacted]	www[redacted]cn	[redacted]	敏感信息泄露防护	报警	
2017-08-23 18:20:18	[redacted]	www[redacted]cn	[redacted]	敏感信息泄露防护	报警	
2017-08-23 18:17:40	[redacted]	www[redacted]cn	[redacted]/r[redacted]	敏感信息泄露防护	报警	
2017-08-23 18:17:40	[redacted]	www.[redacted]cn	[redacted]sc[redacted]	敏感信息泄露防护	报警	

3.5. 攻击监控告警

包括网络层 DDoS 攻击、应用层 DDoS 攻击和 Web 应用攻击监控告警。

3.5.1.网络层攻击监控告警

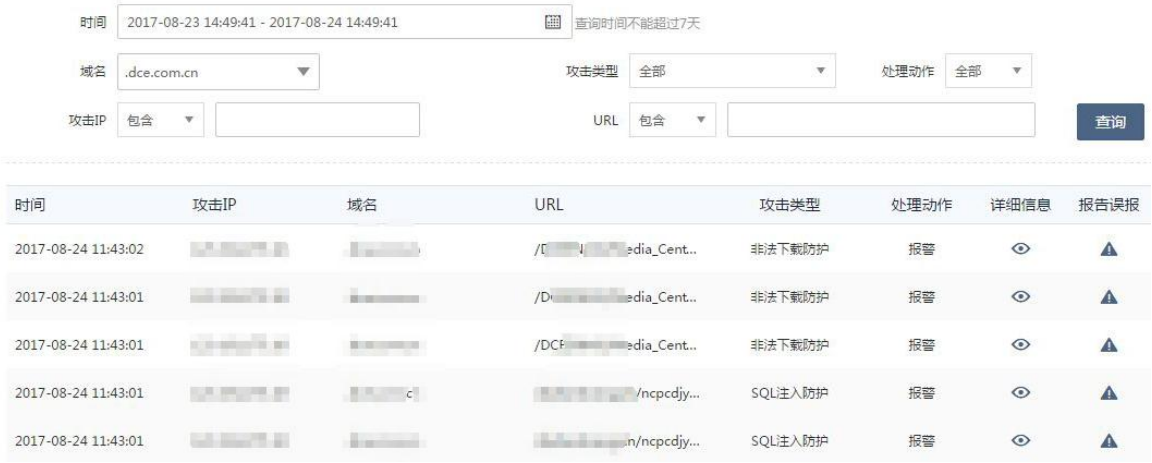
网宿云安全能够以域名为粒度实时采集并统计对应服务 IP 的网络层攻击带宽，当网络层攻击到达预先设置的攻击带宽阈值时，将通过邮件/短信等形式向运维人员发出告警消息，告警信息包括攻击时间、攻击峰值等。

3.5.2.应用层 DDOS 监控告警

各安全节点通过动态学习网站的历史访问日志（如：每个域名的访问量、行为特征等），建立动态基线。通过动态基线学习和日志分析，识别出攻击特征，当检测到异常访问时，根据告警规则（如：QPS 设置的阈值）发送相应攻击告警。

3.5.3.Web 应用攻击监控告警

对 Web 应用程序客户端的各类请求进行内容检测和验证，如发现异常请求，则告警。如图所示：

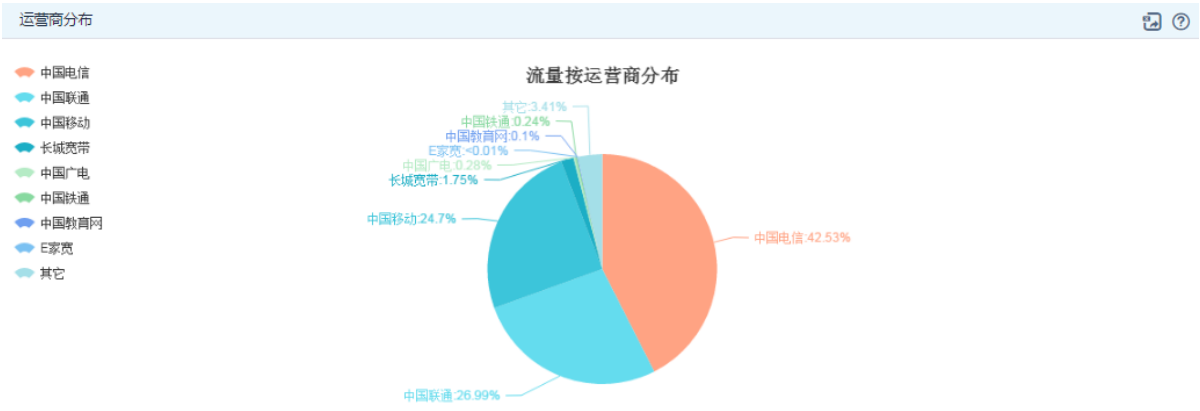


3.6. 业务流量指数监测

提供业务访问数据分析，如：访客分布、PV、访问来源等指标展示，帮助运营人员全面了解线上业务的运营情况。

- 访客按区域（按省/按地区）分布情况：

➢ 访客按运营商情况分布情况：



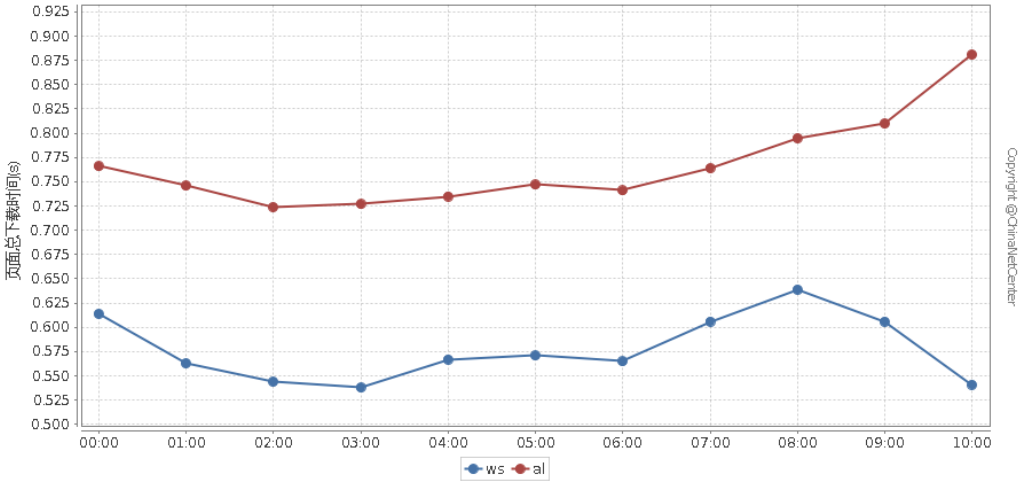
访客运营商分布情况

➢ PV 按省份/地区排行：

PV 排行

3.7. 加速效果监控

直观展示网站加速前与加速后的效果对比，使运维人员了解使用服务后的价值：



4.服务价值

4.1. 自定义设置告警阈值

根据不同业务的需求，灵活自定义各类监控告警服务的检测周期和告警阈值。如可用性小于 98%的时候触发告警、HTTP 请求响应时间大于 5s 时触发告警、攻击达到 20Gbps 时触发告警等。

4.2. 实时掌控网站情况

周期性全自动化监测，能够对网站的可用性、脆弱性、攻击情况、内容安全等进行监测，发现问题可立即告警，并生成告警报告及可视化图表，使运维人员对网站的安全状态一目了然，并对网站安全状况作出正确的评估。

4.3. 了解网站弱点，风险预警

网宿云安全团队通过自主挖掘与行业共享相结合的方式搜集漏洞信息并更新漏洞库，网站弱点监控告警不仅可对常见 Web 漏洞进行扫描，还可以扫描第三方开源软件漏洞以及 0 day 漏洞等，尽早发现可能影响业务正常运行、敏感信息泄露等的漏洞，进行风险预警。

4.4. 降低风险影响

监控告警服务一旦发现网站出现安全问题或安全事件，将及时自动通过电子邮件、短信等方式发送告警信息给网站运维人员，以便相关人员及时作出响应和处理，第一时间降低风险影响。

关于网宿

网宿科技 始创于 2000 年 1 月，主要提供互联网内容分发与加速（CDN）、云计算、云安全、全球分布式数据中心(IDC) 等服务。

2009 年 10 月，网宿科技在深交所上市，股票代码 300017。

网宿科技拥有遍布全球的 1000+ CDN 加速节点，在北京、上海、广州、深圳等地设有分公司，在美国、香港、印度、爱尔兰、马来西亚、济南、南京、杭州等地建有多家全资子公司，并在厦门及美国硅谷设立了研发中心。现有员工 3000 多名，研发以及技术人员占总人数 60% 左右。客户群覆盖各类互联网门户网站、视音频网站、网络游戏公司、电子商务网站、政府网站、企业网站以及运营商等，公司服务的客户超过 3000 家，是市场同类公司中拥有客户数量较多、行业覆盖面较广的公司。