Hillstone下一代智能防火墙技术白皮书之主动检测篇

关键词： 主动检测、风险预知、威胁防护、全网健康指数、风险对象

摘要： 本文介绍了Hillstone下一代智能防火墙中独创的专利技术：主动检测分析引擎和全网健康评分体系。主动检测技术通过对设备资源使用状态、关键网络节点的网络连通性、关键业务服务可用性、内网对象风险分析和威胁状态的检测，给出全网健康分数和详尽的检测报告，帮助用户防御已知和未知威胁，提前预知网络风险，快速排除网络故障，保障网络安全运行。

概述

在安全威胁复杂化、持续化、隐藏化的发展趋势下，企业面临的信息化风险越来越突出，企业业务的可用性作为保证企业正常运转的重要指标，其信息化的程度也非常高，所以，企业业务的可用性是企业信息化风险的重要组成部分。业务的可用性由多种因素构成，网络因素和威胁因素是其中很重要的两个方面，网络因素中主要涵盖了关键网络节点（例如路由器、交换机）和关键业务服务（例如ERP、Mail等业务服务系统）。威胁因素则主要是指人为的无意失误、人为的恶意攻击、网络软件系统的漏洞和“后门”三个方面的因素，它会对网络核心资产造成直接的危害。

伴随着云计算、移动应用、社交网络等新技术、新应用的发展，企业的商业模式也逐步发生了变化。业务可用性不再单纯代表业务不中断，还要求业务的服务质量达到一定的标准，如业务服务的响应速度应在一定的时间范围之内，但当前的网络安全设备大都是在问题发生后才能通知管理员，而在问题发生之前，业务服务质量变差时则无法给出预警；同时，网络安全设备主要采用多模块分开管理和呈现的方案，问题发生后，管理员需要逐个模块分别查看，这意味着需要花更长时间定位问题。主动检测功能则能够提供更加快捷、直观的问题响应和处理机制。

Hillstone 主动检测技术

Hillstone主动检测技术通过对设备资源使用状态、关键网络节点和关键业务服务的网络连通性、业务可用性、内网对象的风险分析以及威胁状况的检测，利用具备专利技术的主动检测分析引擎和网络健康评分体系进行关联分析，给出网络的综合健康评价，即全网健康指数。管理员通过全网健康指数能够实时掌握网络的健康和运行状况，业务的可用性状况以及威胁发生状况，从而在业务中断不可用之前就能够提前获知问题和风险的发生；同时在业务发生不可用的问题后，还能够利用设备提供的健康报告，一次性获取与健康相关联的所有内容，从而更加准确和快速的定位问题。

2.1 检测内容

主动检测的检测对象主要包括关键网络节点、关键业务服务、设备资源，我们将检测对象称为检测单元，针对每一个检测单元又包含了具体的检测项。

- 网络关键节点检测单元

检测内容：关键网络节点的网络连通状态和延迟情况

举例：路由器、交换机的网络联通状态和延迟值

- 关键业务服务检测单元

检测内容：关键业务服务真实的业务服务延迟和网络层连通状态

举例：Mail服务的实际收发邮件的响应时长和服务器网络连通状态

- 设备资源检测单元

检测内容：设备自身的资源使用情况

举例：CPU、内存、磁盘使用率

- 风险对象分析单元

检测内容： 特征无法识别的0-Day攻击和静态阈值内未知DDoS攻击行为等未知威胁和异常

举例：DDoS、0-Day、网络环路故障等未知威胁和网络异常

- 威胁检测单元

检测内容：网络中发生的已知威胁情况

举例：应用层攻击行为、网络层攻击行为、Web攻击行为等

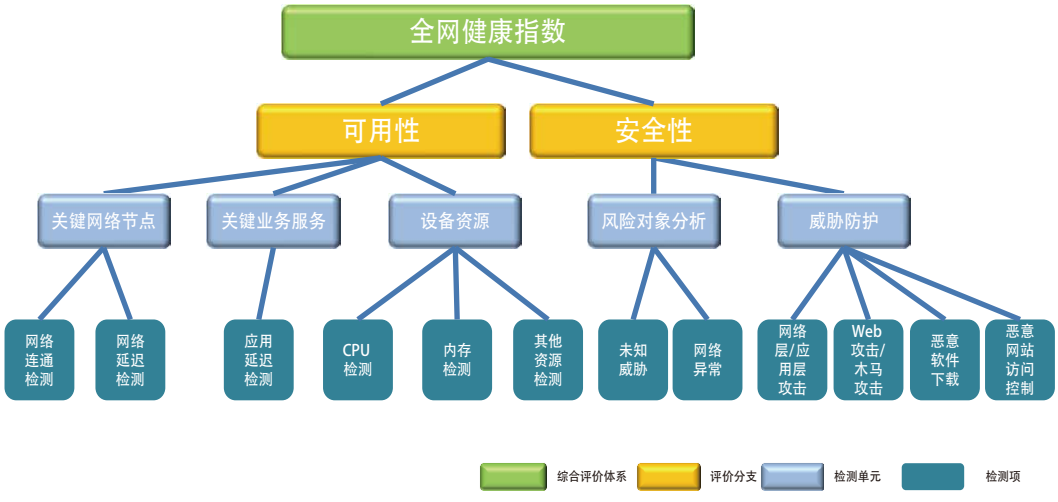

图1 主动检测检测内容

2.2 全网健康评分体系

主动检测的结果通过全网健康指数体现，全网健康指数代表着网络和业务的健康状态，全网健康状态分为三级，分别为健康、亚健康、危险。当全网健康状态发生变迁时，可以通过短信、邮件等多种方式通知管理员，便于管理员及早的关注隐患和进行问题的排查。

- 健康状态：表示网络运行状态良好，业务可用；
- 亚健康状态：表示网络运行状态存在隐患，虽然当前没有造成严重的影响，但是需要管理员关注或是排查，避免问题的发生，例如业务服务没有中断但是其服务响应较慢；
- 危险状态：表示网络运行状态存在问题，已经造成了业务不可用的影响，此时需要管理员进行排查和解决。

2.3 全网健康报告

主动检测的结果通过全网健康指数体现，全网健康指数代表着网络和业务的健康状态，全网健康状态分为三级，分别为健康、亚健康、危险。当全网健康状态发生变迁时，可以通过短信、邮件等多种方式通知管理员，便于管理员及早的关注隐患和介入问题的排查。

- 健康状态：表示网络运行状态良好，业务可用；
- 亚健康状态：表示网络运行状态存在隐患，虽然当前没有造成严重的影响，但是需要管理员关注或是排查，避免问题的发生，例如业务服务没有中断但是其服务响应较慢；
- 危险状态：表示网络运行状态存在问题，已经造成了业务不可用的影响，此时需要管理员进行排查和解决。

下一代智能防火墙不仅提供针对全网的健康报告，同时也会提供针对每一个检查项的检测报告，使得管理员在掌握全局信息的同时也能够得到每个检测项的详细信息。从而管理员可以通过检测报告迅速的从完整的信息中找到故障的原因，而无需再到各个功能模块中多次获取。

- 全网健康报告

包括全网健康状态、全网健康趋势以及各检测单元的健康趋势、所有亚健康检测项和危险检测项。

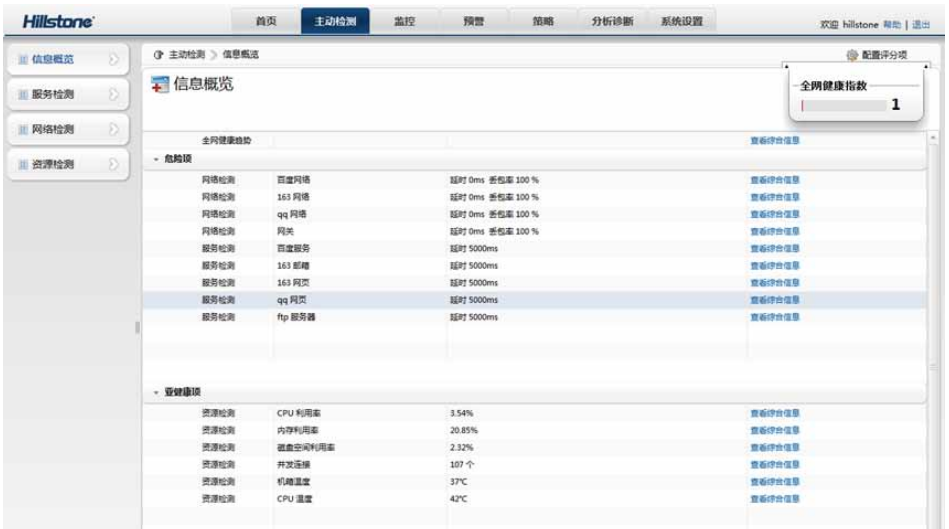

图2 全网健康报告

- 检测项健康报告

包括检测项的健康状态，以及影响该检测项健康状态的全部信息，包括相关的流量、用户、应用的监控信息以及预警信息。

图3 检测项健康报告

Hillstone 主动检测技术用户价值

- **主动检测，预知风险**

在日常的网络管理中，Hillstone业务可用性保障解决方案通过对业务服务、关键网络节点、设备资源进行主动的定期巡检，而Hillstone安全性保障解决方案通过对网络中的威胁信息进行实时检测防御，从而能够实时管控网络健康状态的变化，当业务服务质量下降而问题还未发生前就能及时的感知，并通知管理员，从而帮助管理员提前预知风险，尽早干预和排除隐患。

- **全网健康报告，提升运维效率**

当网络发生问题时，Hillstone业务可用性保障解决方案不仅能够通过主动的检测发现可能的问题点，同时还针对每个问题点提供详尽的分析报告，极大的降低了管理员排查问题的难度和缩短了排查问题的时间。

文档编号：EX-09.01-SG0000-5.0R4-0314-Ch-02