**{{company}}**

**山石网科防火墙{{year}}年第{{quarter}}度巡检报告**



**报告日期: {{report\_date}}**

**目 录**

[**一、** **系统巡检总结** 3](#_Toc166509077)

[**二、** **基础信息** 4](#_Toc166509078)

[2.1 保内与过保设备统计 4](#_Toc166509081)

[2.2 设备型号统计 5](#_Toc166509082)

[2.3 软件版本统计 6](#_Toc166509083)

[2.4 防火墙基础状态 6](#_Toc166509084)

[2.5 与上季度巡检对比 9](#_Toc166509085)

[**三、** **安全评估** 10](#_Toc166509086)

[3.1 配置检查 10](#_Toc166509091)

[3.2 安全日志分析 11](#_Toc166509092)

[3.3 策略规范性 11](#_Toc166509093)

[**四、** **HA可靠性检查** 12](#_Toc166509094)

[1. 硬件部分 13](#_Toc166509095)

[1.1 机房要求 13](#_Toc166509096)

[1.2 电源检查 13](#_Toc166509097)

[1.3 风扇检查 13](#_Toc166509098)

[1.4 指示灯检查 13](#_Toc166509099)

[1.5 模块及数据接口检查： 14](#_Toc166509100)

[2. 系统部分 14](#_Toc166509101)

[2.1 软件版本检查 14](#_Toc166509102)

[2.2 设备温度和风扇及电源检查 14](#_Toc166509103)

[2.3 运行时间检查 15](#_Toc166509104)

[2.4 并发会话检查 15](#_Toc166509105)

[2.5 CPU利用率检查 16](#_Toc166509106)

[2.6 内存使用率检查 16](#_Toc166509107)

[2.7 日志统计审计 16](#_Toc166509108)

[2.8 路由检查 17](#_Toc166509109)

[2.9 查看系统信息 17](#_Toc166509110)

[3. HA部分 17](#_Toc166509111)

[3.1 查看HA状态 17](#_Toc166509112)

[3.2 查看HA Monitor监控对象 17](#_Toc166509113)

[3.3 查看HA是否开启抢占 18](#_Toc166509114)

[3.4 配置同步检查 18](#_Toc166509115)

[4. 防火墙整体配置及策略检查 18](#_Toc166509116)

[5. 巡检命令参考： 18](#_Toc166509117)

1. **系统巡检总结**

**本次针对现网运行的{{set\_number}}台设备进行巡检，通过分析统计设备的版本与型号、资源利用率、系统日志、安全告警、HA 状态等相关信息，确认{{normal\_number}}台设备系统运行正常，{{abnormal\_number}}台存在安全风险，具体如下:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 序列号 | 发生时间 | 具体问题 | 解决方案 | 风险等级 |
| {{for\_start}} |  |  |  |  |  |  |
| {{row\_id}} | {{row\_name}} | {{row\_sn}} | {{row\_occurrence\_time}} | {{row\_concrete\_issue}} | {{row\_solution}} | {{row\_risk\_grade}} |
| {{for\_due}} |  |  |  |  |  |  |

备注：风险等级描述

* 高：会引起严重业务影响，建议尽快整改；
* 中：概率性影响业务，建议安排时间窗口整改；
* 低：不影响业务；

1. **基础信息**
3. 1. 保内与过保设备统计

本次巡检共计{{set\_number}}台防火墙，其中{{under\_warranty}}台在保，{{over\_insured}}台已经过保，以下为过保设备列表，建议联系销售续保。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备名称 | S/N | 设备过保时间 |
| {%tr for row in record\_list %} |  |  |  |
| {{row.table\_id}} | {{row.device\_name}} | {{row.device\_sn}} | {{row.lic\_expiration\_time}} |
| {%tr endfor %} |  |  |  |

设备过保/在保比例：{{timing\_separation}}设备许可过保比例

{{over\_chart}}

* 1. 设备型号统计

{{product\_chart}}

* 1. 软件版本统计

{{software\_chart}}

* 2. 防火墙基础状态

因表单信息较多，分成多个表格：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 基础信息 | | | | | | | |
| 设备名称 | SN | 设备型号 | 软件版本 | LIC到期时间 | 主备状态 | 运行天数 | 机房位置 |
| {%tr for row in record\_list%} |  |  |  |  |  |  |  |
| {{row.device\_name}} | {{row.device\_sn}} | {{row.device\_model}} | {{row. software\_version}} | {{row. lic\_expiration\_time}} | {{row.ha\_state}} | {{row.uptime}} | {{row. machine\_room}} |
| {%tr endfor %} |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 环境指标 | | | | | | |
|  | 电源状态 | | | 板卡状态 | | |
| SN | 巡检值 | 参考范围 | 风险评估 | 巡检值 | 参考范围 | 风险评估 |
| {%tr for row in record\_list %} |  |  |  |  |  |  |
| {{row.device\_sn}} | {{row.ps\_status}} | Fine | {{row.power\_status}} | {{row.module\_status}} | Fine | {{row.board\_status}} |
| {%tr endfor %} |  |  |  |  |  |  |
|  | 风扇状态 | | | 温度状态 | | |
| SN | 巡检值 | 参考范围 | 风险评估 | 巡检值 | 参考范围 | 风险评估 |
| {%tr for row in record\_list %} |  |  |  |  |  |  |
| {{row.device\_sn}} | {{row.fan\_status}} | Fine | {{row.fan\_evaluation}} | {{row.env\_cpu\_temperature}} | 0-90 | {{row.env\_cpu\_evaluation}} |
| {%tr endfor %} |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 性能指标 | | | | | | |
|  | CPU利用率（平均） | | | 整机吞吐（可选） | | |
| SN | 巡检值 | 参考范围 | 风险评估 | 巡检值 | 参考范围 | 风险评估 |
| {%tr for row in record\_list %} |  |  |  |  |  |  |
| {{row.device\_sn}} | {{row.cur\_cpu}} | 0-70% | {{row.cpu\_assess}} | {{row.throughput}} |  |  |
| {%tr endfor %} |  |  |  |  |  |  |
|  | CP利用率 | | | DP利用率 | | |
| SN | 巡检值 | 参考范围 | 风险评估 | 巡检值 | 参考范围 | 风险评估 |
| {%tr for row in record\_list %} |  |  |  |  |  |  |
| {{row.device\_sn}} | {{row.cp\_memory}} | 0-70% | {{row.cp\_assess}} | {{row.dp\_memory}} | 0-70% | {{row.dp\_assess}} |
| {%tr endfor %} |  |  |  |  |  |  |
|  | 会话新建数 | | | 会话并发数 | | |
| SN | 巡检值 | 参考范围 | 风险评估 | 巡检值 | 参考范围 | 风险评估 |
| {%tr for row in record\_list %} |  |  |  |  |  |  |
| {{row.device\_sn}} | {{row.alloc\_session}} |  |  | {{row.session\_info}} |  |  |
| {%tr endfor %} |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 资源利用率指标 | | | | | | |
|  | 地址簿利用率 | | | 服务簿利用率 | | |
| SN | 巡检值 | 参考范围 | 风险评估 | 巡检值 | 参考范围 | 风险评估 |
| {%tr for row in record\_list %} |  |  |  |  |  |  |
| {{row.device\_sn}} | {{row.address\_rate}} |  |  | {{row.server\_rate}} |  |  |
| {%tr endfor %} |  |  |  |  |  |  |
|  | SNAT条目利用率 | | | DNAT条目利用率 | | |
| SN | 巡检值 | 参考范围 | 风险评估 | 巡检值 | 参考范围 | 风险评估 |
|  |  |  |  |  |  |  |
| {%tr for row in record\_list %} |  |  |  |  |  |  |
| {{row.device\_sn}} | {{row.snat\_rate}} |  |  | {{row.dnat\_rate}} |  |  |
| {%tr endfor %} |  |  |  |  |  |  |
|  | 策略利用率 | | | 路由条目利用率 | | |
| SN | 巡检值 | 参考范围 | 风险评估 | 巡检值 | 参考范围 | 风险评估 |
| {%tr for row in record\_list %} |  |  |  |  |  |  |
| {{row.device\_sn}} | {{row.policy\_rate}} |  |  | {{row.route\_entry}} |  |  |
| {%tr endfor %} |  |  |  |  |  |  |

* 2. 与上季度巡检对比

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 季度 | 设备名称 | 运行天数 | 软件版本 | 板卡状态 | 温度'C |
| {%tr for record in quarterly\_list %} |  |  |  |  |  |  |
| {{record.table\_id}} | {{record.quarterly\_data.date\_tag}} | {{record.quarterly\_data.device\_model}} | {{record.quarterly\_data.uptime}} | {{record.quarterly\_data.software\_version}} | {{record.quarterly\_data.board\_status}} | {{record.quarterly\_data. env\_cpu\_temperature}} |
| {{record. date\_tag}} | {{record.device\_model}} | {{record.uptime}} | {{record.software\_version}} | {{record. board\_status}} | {{record. env\_cpu\_temperature}} |
| {%tr endfor %} |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 季度 | 设备名称 | 主备状态 | session新建 | session并发 | CPU | CP内存（%） | DP内存（%） |
| {%tr for record in quarterly\_list %} |  |  |  |  |  |  |  |  |
| {{record.table\_id}} | {{record.quarterly\_data.date\_tag}} | {{record.quarterly\_data.device\_model}} | {{record.quarterly\_data.ha\_state}} | {{record.quarterly\_data.alloc\_session}} | {{record.quarterly\_data.session\_info}} | {{record.quarterly\_data.cur\_cpu}} | {{record.quarterly\_data.cp\_memory}} | {{record.quarterly\_data.dp\_memory}} |
| {{record. date\_tag}} | {{record.device\_model}} | {{record.ha\_state}} | {{record.alloc\_session}} | {{record.session\_info}} | {{record.cur\_cpu}} | {{record.cp\_memory}} | {{record.dp\_momory}} |
| {%tr endfor %} |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 季度 | 设备名称 | 地址簿使用率 | 服务簿数量 | 策略数量 | snat条目数 | dnat条目数 |
| {%tr for record in quarterly\_list %} |  |  |  |  |  |  |  |
| {{record.table\_id}} | {{record.quarterly\_data.date\_tag}} | {{record.quarterly\_data.device\_model}} | {{record.quarterly\_data.address\_rate}} | {{record.quarterly\_data.server\_rate}} | {{record.quarterly\_data.policy\_rate}} | {{record.quarterly\_data.snat\_rate}} | {{record.quarterly\_data.dnat\_rate}} |
| {{record. date\_tag}} | {{record.device\_model}} | {{record.address\_rate}} | {{record.server\_rate}} | {{record.policy\_rate}} | {{record.snat\_rate}} | {{record.dnat\_rate}} |
| {%tr endfor %} |  |  |  |  |  |  |  |

1. **安全评估**


5. 1. 配置检查

|  |  |
| --- | --- |
| 巡检内容 | **主备设备配置对比** |
| 操作步骤 | 执行命令 show config，对比主备设备配置是否相同。 |
| 异常设备 | {{compare\_main\_baseconfig\_equipment}} |
| 分析建议 | {{compare\_main\_baseconfig\_suggest}} |

|  |  |
| --- | --- |
| 巡检内容 | **口令长度与复杂度** |
| 操作步骤 | 对于采用静态口令认证技术的设备：应支持口令长度及复杂度验证机制（强制要求口令应由数字、大写字母、小写字母和特殊符号4类字符构成，自动拒绝用户设置不符合复杂度要求的口令。）； |
| 异常设备 | {{password\_policy\_equipment}} |
| 分析建议 | {{password\_policy\_suggest}} |

|  |  |
| --- | --- |
| 巡检内容 | **账号锁定策略** |
| 操作步骤 | 应为设备配置用户连续认证失败次数上限，当用户连续认证失败次数超过上限时，设备自动断开该用户账号的连接，并在一定时间内禁止该用户账号重新认证。admin lockout-duration xxxx |
| 异常设备 | {{admin\_lockout\_duration\_equipment}} |
| 分析建议 | {{admin\_lockout\_duration\_suggest}} |

|  |  |
| --- | --- |
| 巡检内容 | **关闭不安全的管理方式** |
| 操作步骤 | 接口下关闭telnet、http登录设备方式 |
| 异常设备 | {{unsafe\_interface\_equipment}} |
| 分析建议 | {{unsafe\_interface\_suggest}} |

|  |  |
| --- | --- |
| 巡检内容 | **配置可信主机** |
| 操作步骤 | 配置可信主机，只允许授权的IP登录设备。 |
| 异常设备 | {{admin\_host\_equipment}} |
| 分析建议 | {{admin\_host\_suggest}} |

* 1. 安全日志分析

|  |  |
| --- | --- |
| 巡检内容 | **查看事件日志、告警日志、配置日志、操作日志、威胁日志是否开启。** |
| 操作步骤 | 通过show logging 命令 |
| 异常设备 | {{logging\_status\_equipment}} |
| 分析建议 | {{logging\_status\_suggest}} |

|  |  |
| --- | --- |
| 巡检内容 | **Threat安全威胁日志分析** |
| 操作步骤 | 分析show logging threat日志，查看是否有威胁事件、攻击日志、端口扫描等。 |
| 异常设备 | {{log\_threat\_equipment}} |
| 分析建议 | {{log\_threat\_suggest}} |

|  |  |
| --- | --- |
| 巡检内容 | **告警日志分析** |
| 操作步骤 | 分析show logging alarm日志，查看是否有告警事件。 |
| 异常设备 | {{log\_alarm\_equipment}} |
| 分析建议 | {{log\_alarm\_suggest}} |

* 1. 策略规范性

|  |  |
| --- | --- |
| 巡检内容 | **检查是否有全通策略** |
| 操作步骤 | 分析show policy，查看是否有全通策略。 |
| 异常设备 | {{all\_passrlue\_equipment}} |
| 分析建议 | {{all\_passrlue\_suggest}} |

1. **HA可靠性检查**

|  |  |
| --- | --- |
| 巡检内容 | **HA配置检查** |
| 操作步骤 | 执行命令show ha group 0或者1  执行命令show ha group config |
| 异常设备 | {{ha\_group\_equipment}} |
| 结果分析 | {{ha\_group\_suggest}} |

|  |  |
| --- | --- |
| 巡检内容 | **HA 同步统计信息检查** |
| 操作步骤 | 执行命令show ha sync statistic |
| 异常设备 | {{synced\_equipment}} |
| 分析建议 | {{synced\_suggest}} |

|  |  |
| --- | --- |
| 巡检内容 | **HA会话同步信息检查** |
| 操作步骤 | 执行命令show session {sync|unsync} |
| 异常设备 | {{poor\_equipment}} |
| 分析建议 | {{poor\_suggest}} |