Supernova 测试仪

防火墙恶意代码检测配置手册

网测科技

2021/01/22

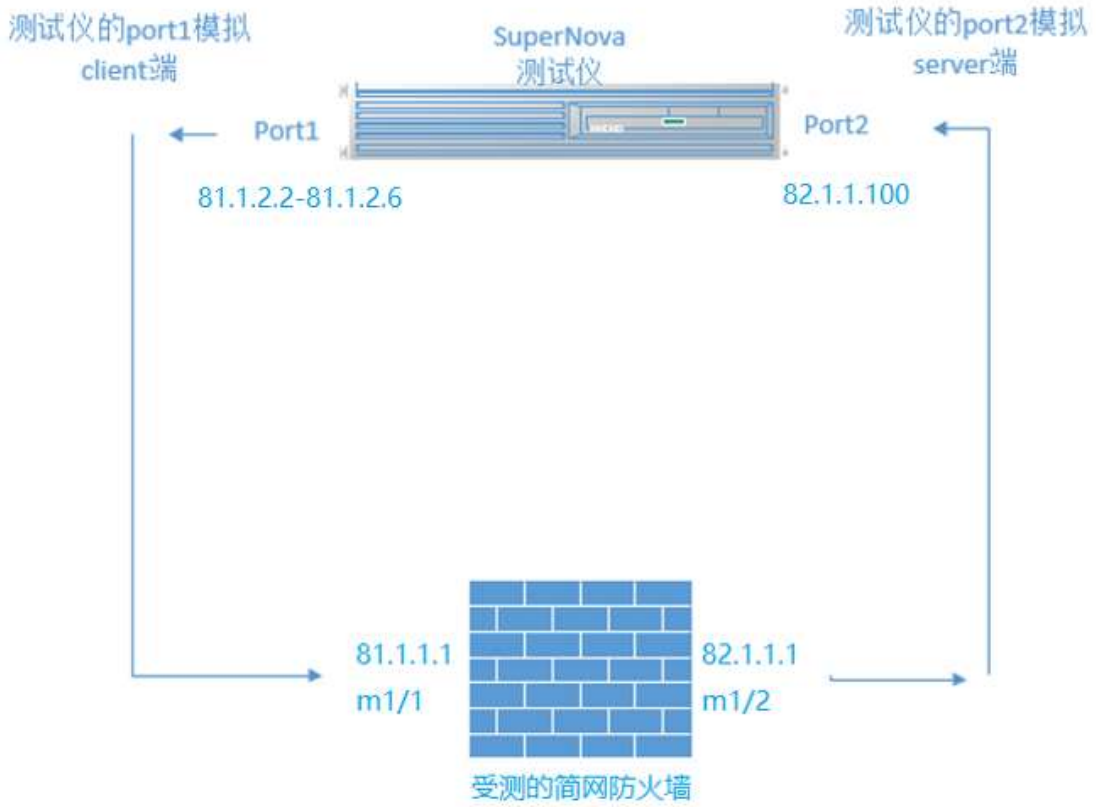
目　　录

1. 文档说明

本文档介绍配置防火墙恶意代码检测的配置过程，此文档使用一台简网防火墙配置举例，不同品牌的防火墙操作配置存在差异性，而且随着系统版本升级和接口变化，需要不断对配置用例进行修改和升级，所以有任何问题，请联系我们的售前或售后支持人员。

2. 网络拓扑图

本次测试的网络拓扑图如下



判断方法：
通过 HTTP 协议，Get 一个病毒文件或者恶意程序，通过响应的成功与否，判断防火墙对恶意代码的检查结果。

3. 设置防火墙

3.1 设置接口 ip 地址

进入防火墙系统网络接口配置页面

我这里用的是 m1/1 和 m1/2 端口

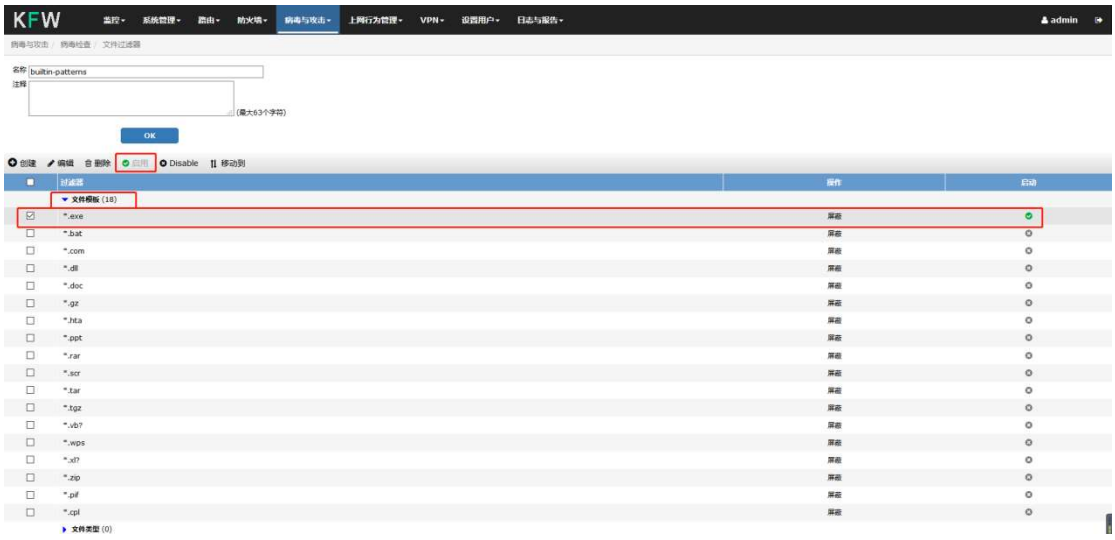
3.2 配置防火墙病毒检测

3.2.1 配置防火墙病毒文件过滤器

进入防火墙病毒文件过滤器配置界面

点击文件过滤器模板进行编辑

文件过滤器中，启动对 .exe 文件模板的屏蔽



3.2.2 配置防火墙病毒检测配置模板

进入防火墙病毒检测配置模板界面

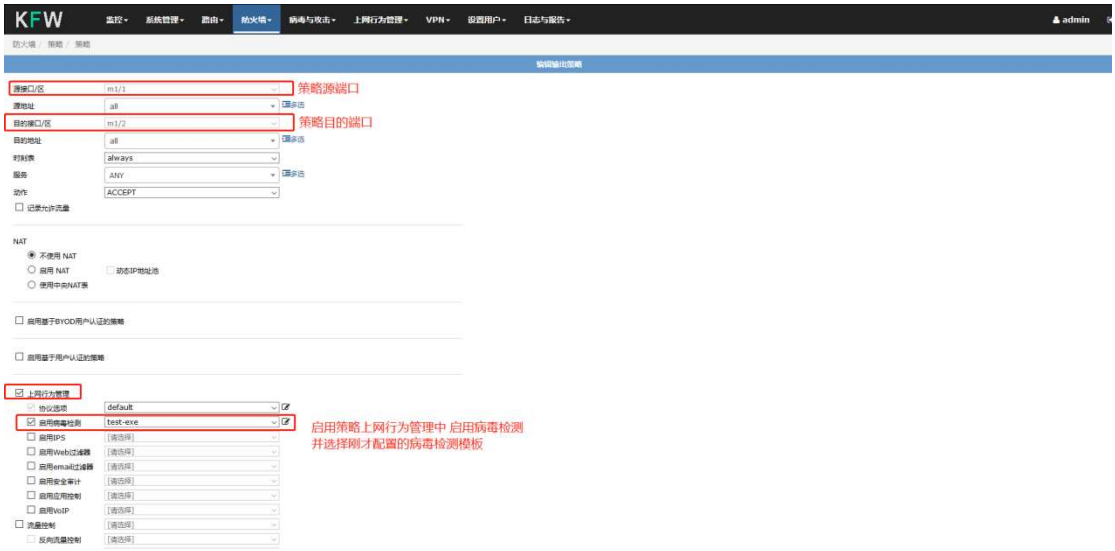
点击创建新增配置模板

3.3 配置防火墙策略

进入到防火墙策略配置界面：

点击创建增加策略：

配置策略内容：

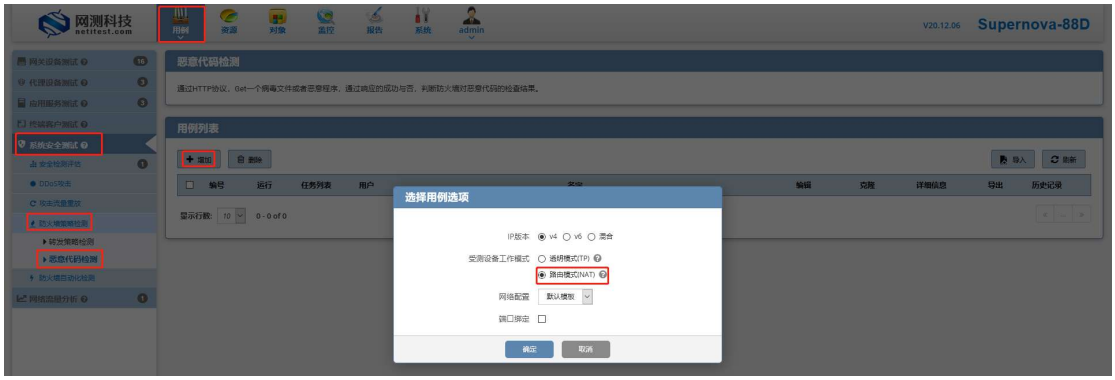


最后的效果如下：

4. 设置 Supernova 测试仪

4.1 防火墙恶意代码检测用例配置

新增防火墙恶意代码检测测试用例，点击用例→系统安全测试→防火墙策略检测→恶意代码检测→增加，创建测试用例，受测设备工作模式选择 NAT 模式。

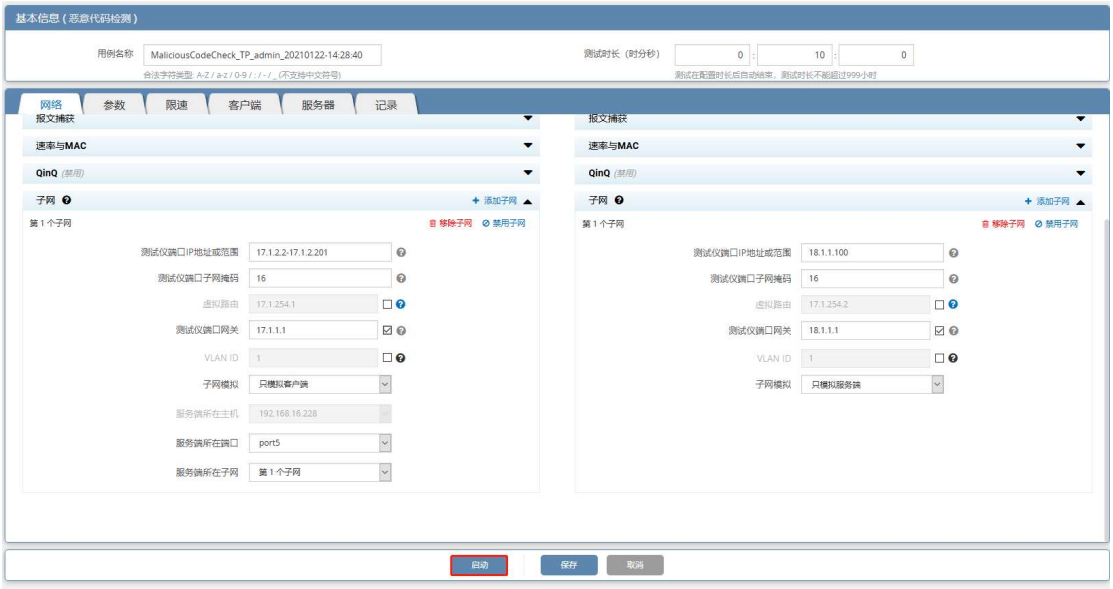


设置填写用例配置中 IP 地址（此处 ip 地址与拓扑中一致）：

配置请求的病毒文件：

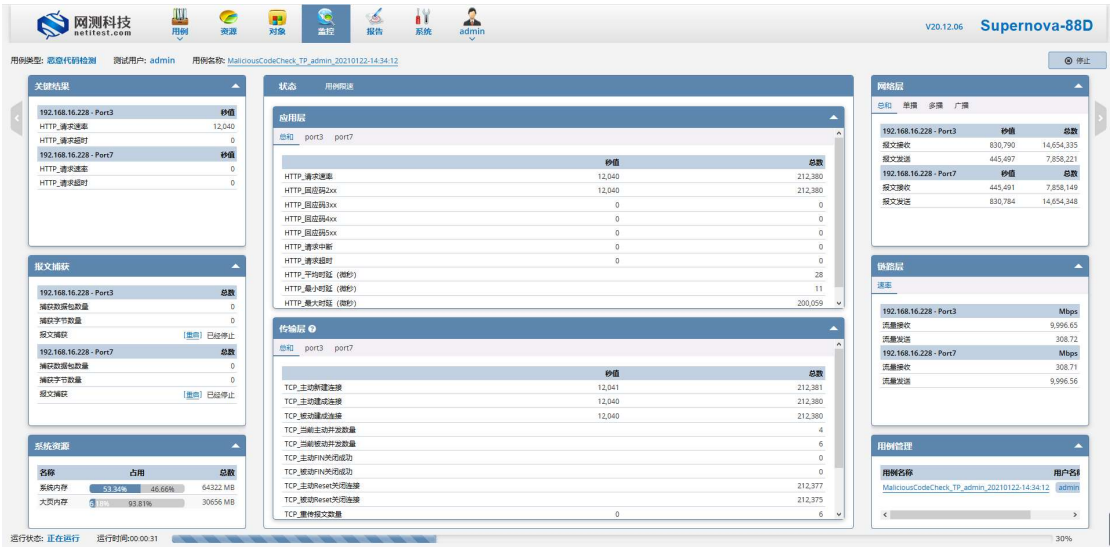
4.2 启动测试用例

用例配置后，可点击【启动】直接运行测试用例：

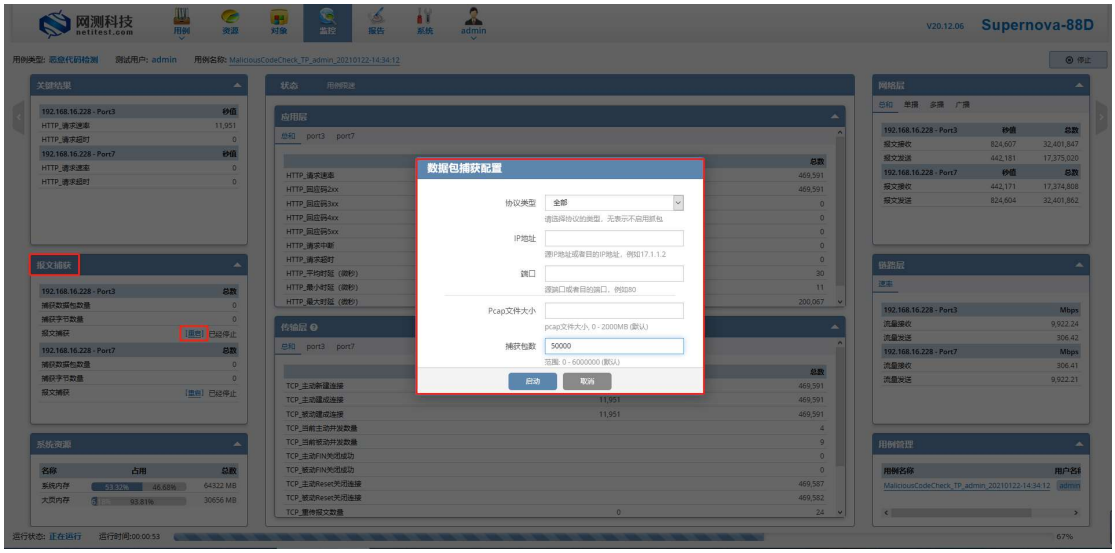


4.3 运行用例

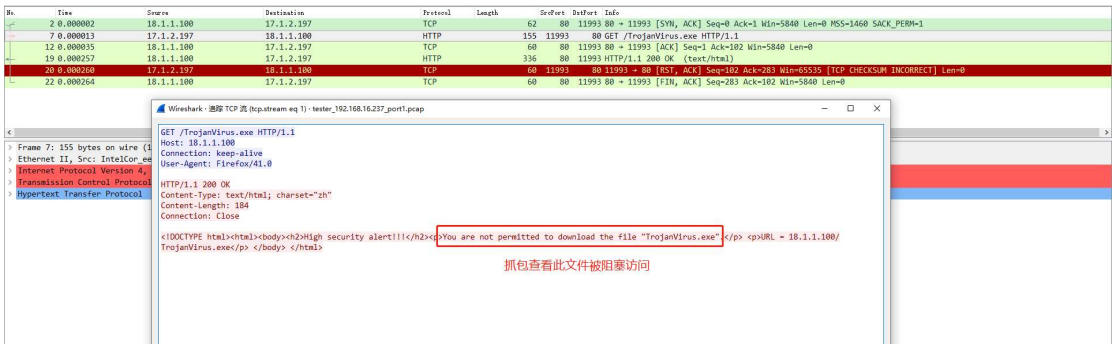
用例启动后，正常运行界面如下：



用例运行中，可点击【报文捕获】进行抓包查看运行报文：

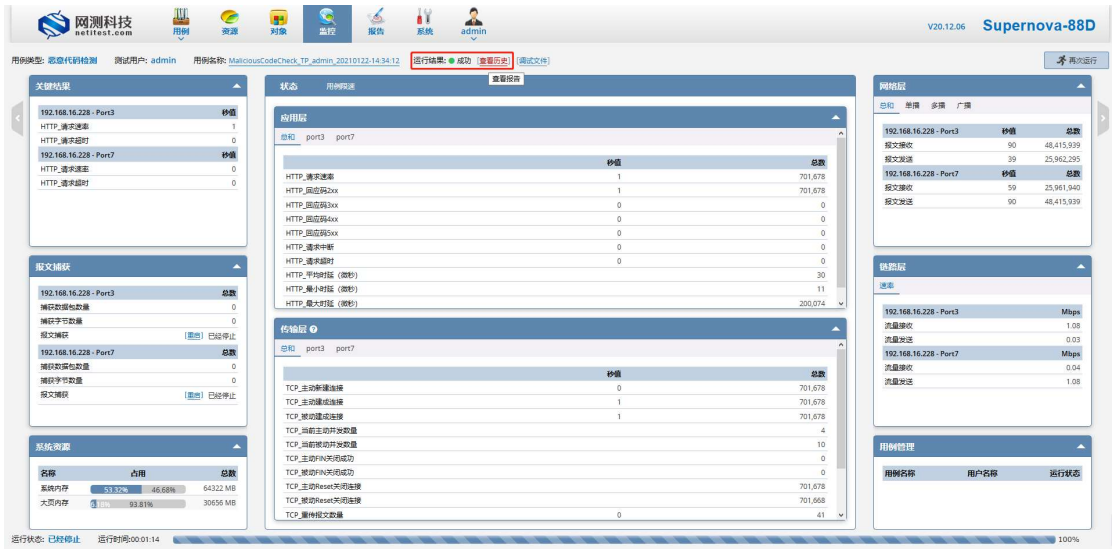


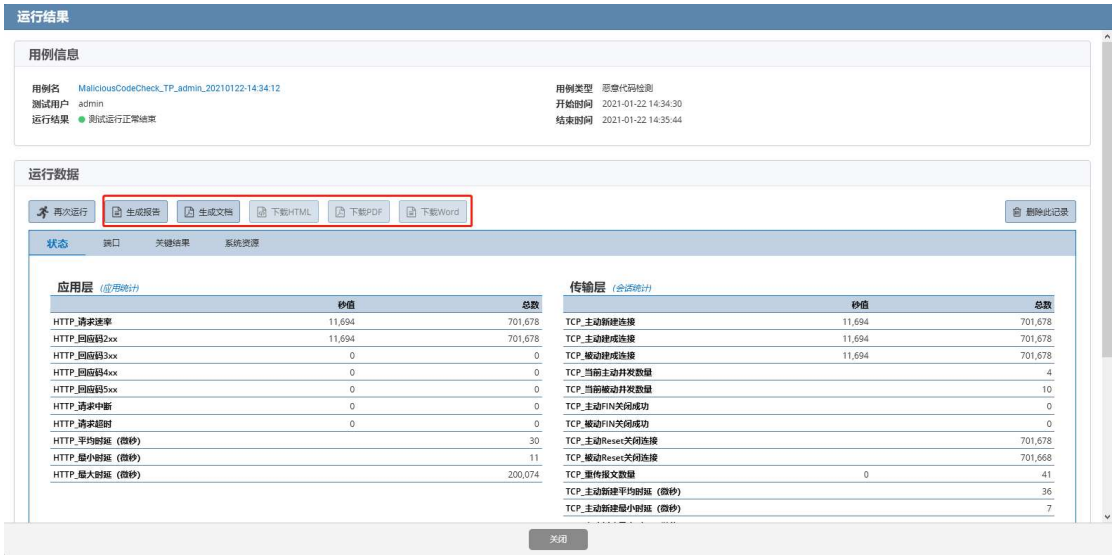
查看报文捕获到的交互报文，可以看到防火墙对此病毒文件进行了访问阻断：



4.4 查看运行报告

用例运行结束可以生成报告数据及 HTML/PDF/Word 报告，报告生成后，可以下载 HTML/PDF/Word 格式测试报告。




运行结果
用例信息
用例名 MaliciousCodeCheck_TP_admin_20210122-14:34:12
测试用户 admin
运行结果 测试运行正常结束
用例类型 恶意代码检测
开始时间 2021-01-22 14:34:30
结束时间 2021-01-22 14:35:44
运行数据
再次运行
生成报告
生成文档
下载HTML
下载PDF
下载Word
删除此记录
状态
端口
关键结果
系统资源
应用层 (应用统计)
传输层 (会话统计)
关闭


运行结果
用例信息
报告生成进度
摘要
图表
HTML
PDF
Word
已完成
关闭
下载HTML
下载PDF
下载Word