

HTTP 正向代理配置手册

网测科技

2021-01-20

目 录

1. 文档说明	3
2. 网络拓扑图	3
3. 设置防火墙	4
3.1 设置接口 ip 地址	4
3.2 开启代理	5
3.3 添加附加 ip 地址	6
3.4 网络代理的设置	9
3.5 添加策略	10
4. 设置 Supernova 测试仪	12
4.1 HTTP 的正向代理实例	12
4.2 启动实例	13
4.4 启动后正常运行界面	14

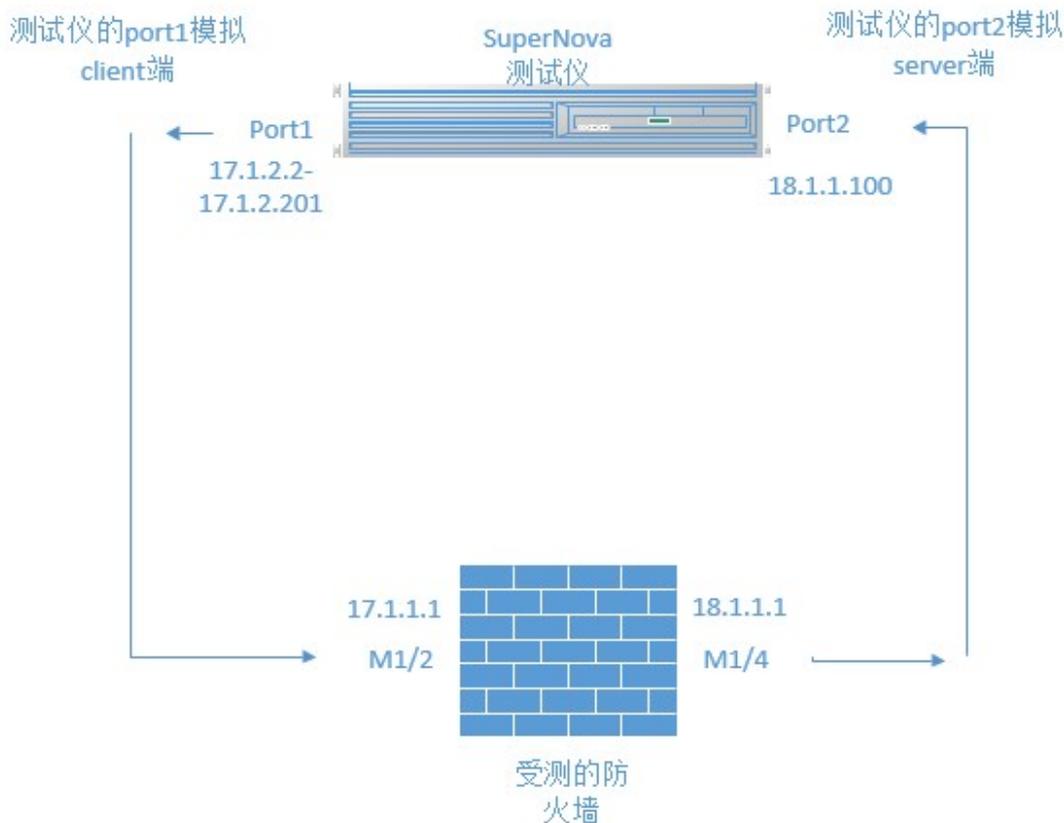
1. 文档说明

本文档介绍配置 HTTP 正向代理的配置过程，但 HTTP 正向代理的配置涉及到 HTTP 协议的专业知识、Web 应用的研发逻辑、正则表达式的应用，而且随着 Web 服务器的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

本次以测试防火墙的
正向代理为例：



3. 设置防火墙

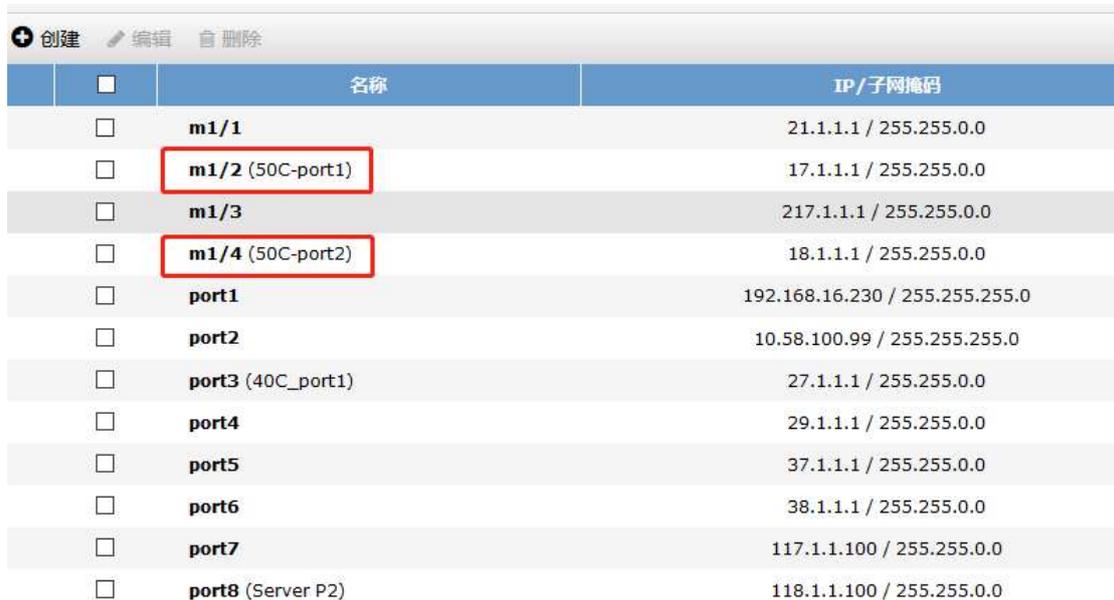
3.1 设置接口 ip 地址



The screenshot shows the KFW web management interface. The top navigation bar includes '系统管理', '路由', '防火墙', '病毒与攻击', and '上网行为管理'. The '系统管理' menu is expanded, showing '网络' and '接口' options. The '网络' menu is further expanded, showing 'DHCP服务器', '配置', '管理员设置', '证书', and '维护'. The '接口' menu is also expanded, showing '区', '选项', 'DNS 服务器', and '网络代理'. Below the navigation, a table lists network interfaces with their IP addresses and subnets.

	名称	IP/子网掩码
<input type="checkbox"/>	m1/1	21.1.1.1 / 255.255.0.0
<input type="checkbox"/>	m1/2 (50C-port1)	17.1.1.1 / 255.255.0.0
<input type="checkbox"/>	m1/3	217.1.1.1 / 255.255.0.0
<input type="checkbox"/>	m1/4 (50C-port2)	18.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port1	192.168.16.230 / 255.255.255.0
<input type="checkbox"/>	port2	10.58.100.99 / 255.255.255.0
<input type="checkbox"/>	port3 (40C_port1)	27.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port4	29.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port5	37.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port6	38.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port7	117.1.1.100 / 255.255.0.0
<input type="checkbox"/>	port8 (Server P2)	118.1.1.100 / 255.255.0.0

我这里用的是 m1/2 和 m1/4 端口



The screenshot shows a table of network interfaces in the KFW web interface. The table has columns for '名称' (Name) and 'IP/子网掩码' (IP/Subnet Mask). The interfaces m1/2 (50C-port1) and m1/4 (50C-port2) are highlighted with red boxes.

	名称	IP/子网掩码
<input type="checkbox"/>	m1/1	21.1.1.1 / 255.255.0.0
<input type="checkbox"/>	m1/2 (50C-port1)	17.1.1.1 / 255.255.0.0
<input type="checkbox"/>	m1/3	217.1.1.1 / 255.255.0.0
<input type="checkbox"/>	m1/4 (50C-port2)	18.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port1	192.168.16.230 / 255.255.255.0
<input type="checkbox"/>	port2	10.58.100.99 / 255.255.255.0
<input type="checkbox"/>	port3 (40C_port1)	27.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port4	29.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port5	37.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port6	38.1.1.1 / 255.255.0.0
<input type="checkbox"/>	port7	117.1.1.100 / 255.255.0.0
<input type="checkbox"/>	port8 (Server P2)	118.1.1.100 / 255.255.0.0

3.2 开启代理

进入到 m1/2 口下将接口的 ip 地址改为和拓扑图一致并将 web 代理开启：

接口名称	m1/2 (00:60:E0:67:72:B9)		
别名	<input type="text" value="50C-port1"/>		
连接状态	已启用		

地址模式	为Client端的网关地址		
<input checked="" type="radio"/> 自定义	<input type="radio"/> DHCP	<input type="radio"/> PPPoE	
IP地址/子网掩码:	<input type="text" value="17.1.1.1/255.255.0.0"/>		
IPv6地址:	<input type="text" value="3ffe:1:7:1::1/64"/>		

<input type="checkbox"/> 开启端口监控功能			
<input checked="" type="checkbox"/> 开启显式Web代理功能			
<input type="checkbox"/> 开启IPMAC绑定功能			
<input type="checkbox"/> 启用DDNS			
<input type="checkbox"/> 分解大于MTU的输出包	<input type="text" value="1500"/>	(字节)	
<input checked="" type="checkbox"/> 启用DNS查询	<input type="text" value="recursive"/>	v	
管理访问	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input checked="" type="checkbox"/> HTTP
	<input checked="" type="checkbox"/> SSH	<input checked="" type="checkbox"/> SNMP	<input checked="" type="checkbox"/> TELNET
	<input checked="" type="checkbox"/> WEBAPI-HTTP	<input checked="" type="checkbox"/> WEBAPI-HTTPS	
IPv6端口访问权限	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input checked="" type="checkbox"/> HTTP
	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input checked="" type="checkbox"/> TELNET
	<input checked="" type="checkbox"/> WEBAPI-HTTP	<input checked="" type="checkbox"/> WEBAPI-HTTPS	

<input checked="" type="checkbox"/> 检测网关的接口状况			
检测服务器	<input type="text"/>		
检测协议	<input checked="" type="checkbox"/> Ping	<input checked="" type="checkbox"/> TCP Echo	<input checked="" type="checkbox"/> UDP Echo
权值	<input type="text" value="0"/>		
链路超载阈值	<input type="text" value="0"/>	KBps	

3.3 添加附加 ip 地址

在此页面下方选择附加 ip 地址并添加：

接口名称	m1/2 (00:60:E0:67:72:B9)
别名	<input type="text" value="50C-port1"/>
连接状态	已启用

地址模式

自定义 DHCP PPPoE

IP地址/子网掩码：

IPv6地址：

开启端口监控功能

开启显式Web代理功能

开启IPMAC绑定功能

启用DDNS

分解大于MTU的输出包。 (字节)

启用DNS查询

管理访问	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input checked="" type="checkbox"/> HTTP
	<input checked="" type="checkbox"/> SSH	<input checked="" type="checkbox"/> SNMP	<input checked="" type="checkbox"/> TELNET
	<input checked="" type="checkbox"/> WEBAPI-HTTP	<input checked="" type="checkbox"/> WEBAPI-HTTPS	
IPv6端口访问权限	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input checked="" type="checkbox"/> HTTP
	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input checked="" type="checkbox"/> TELNET
	<input checked="" type="checkbox"/> WEBAPI-HTTP	<input checked="" type="checkbox"/> WEBAPI-HTTPS	

检测网关的接口状况

检测服务器

检测协议 Ping TCP Echo UDP Echo

权值

链路超载阈值 KBps

▾ 附加的IP地址

+ 添加

编辑接口

IP地址 / 子网掩码: 17.2.1.1/16 为client端子网2的网关地址

检测网关的接口状况

检测服务器:

检测协议: Ping TCP Echo UDP Echo

管理访问: HTTPS PING HTTP
 SSH SNMP TELNET

OK 取消

进入到 m1/4 口下，设置方法和设置 m1/2 的一致：

接口名称: m1/4 (00:60:E0:67:72:BB)

别名: 50C-port2

连接状态: 已启用

地址模式: 自定义 DHCP PPPoE

IP地址/子网掩码: 18.1.1.1/255.255.0.0 为Server的网关地址

IPv6地址: 3ffe:1:2:2::1/64 址

开启端口监控功能

开启显式Web代理功能

开启IPMAC绑定功能

启用DDNS

分解大于MTU的输出包: 1500 (字节)

启用DNS查询: recursive

管理访问: HTTPS PING HTTP
 SSH SNMP TELNET
 WEBAPI-HTTP WEBAPI-HTTPS

接口名称 m1/4 (00:60:E0:67:72:BB)
别名 50C-port2
连接状态 已启用

地址模式

自定义 DHCP PPPoE

IP地址/子网掩码: 18.1.1.1/255.255.0.0

IPv6地址: 3ffe:1:2:2::1/64

开启端口监控功能

开启显式Web代理功能

开启IPMAC绑定功能

启用DDNS

分解大于MTU的输出包. 1500 (字节)

启用DNS查询 recursive

管理访问 HTTPS PING HTTP
 SSH SNMP TELNET
 WEBAPI-HTTP WEBAPI-HTTPS

IPv6端口访问权限 HTTPS PING HTTP
 SSH SNMP TELNET
 WEBAPI-HTTP WEBAPI-HTTPS

检测网关的接口状况

检测服务器

检测协议 Ping TCP Echo UDP Echo

权值 0

链路超载阈值 0 Kbps

附加的IP地址
+ 添加



3.4 网络代理的设置



下图序号 1 中的 m1/2 和 m1/4 接口开启 web 代理后会在此处显示监听；
序号 2 中的端口号可以是任意，默认是 80；而 8080 也比较常用；
序号 3 中选择阻止；（如果选择放行下一步将不需要设置，直接跳过即可）



3.5 添加策略

在防护墙中添加允许策略：（防火墙的默认策略是全部阻止）



KFW 监控 系统管理 路由 防火墙 病毒

防火墙 / 策略 / 策略

+ 创建 编辑 删除 移动到 插入 检查

序号 源

防火墙 / 策略 / 策略

源接口/区: m1/2(50C-port1)

源地址: all 多选

目的接口/区: m1/4(50C-port2)

目的地址: all 多选

时刻表: always

服务: ANY 多选

动作: ACCEPT

记录允许流量

源接口/区: m1/4(50C-port2)

源地址: all 多选

目的接口/区: m1/2(50C-port1)

目的地址: all 多选

时刻表: always

服务: ANY 多选

动作: ACCEPT

记录允许流量

源接口/区

源地址 多选

目的接口/区

目的地址 多选

动作

记录允许流量

启用基于BYOD用户认证的策略

最后的效果如下：

策略名称	源地址	目的地址	动作	状态
m1/2(S0C-port1) -> m1/4(S0C-port2) (1)	all	all	ACCEPT	启用
m1/4(S0C-port2) -> m1/2(S0C-port1) (1)	all	all	ACCEPT	启用
web-proxy -> m1/4(S0C-port2) (1)	all	all	ACCEPT	启用

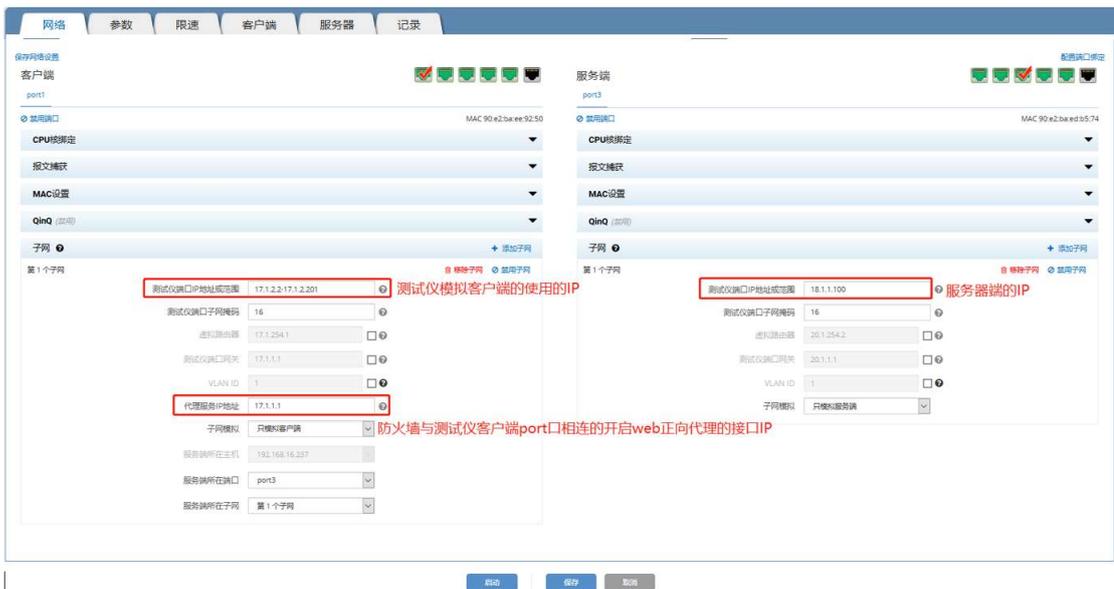
4. 设置 Supernova 测试仪

4.1 HTTP 的正向代理实例

1) 登录系统，依次点击，用例->代理设备测试->HTTP->新建服务->增加，单击增加，在弹出的选择用例选项中，编辑用例网络选项，根据需要修改配置参数，然后点击确定，进入用例配置页面。

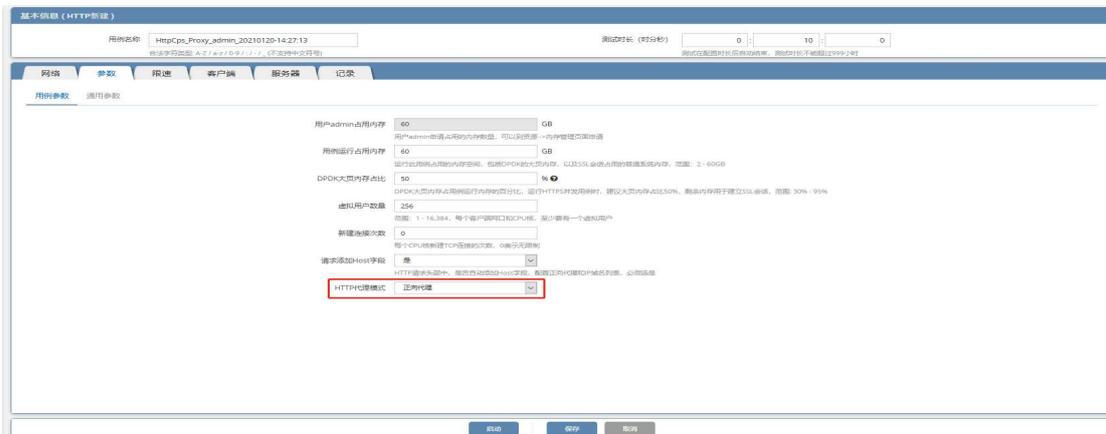


2) 点击确定，进入用例配置界面，配置子网信息。

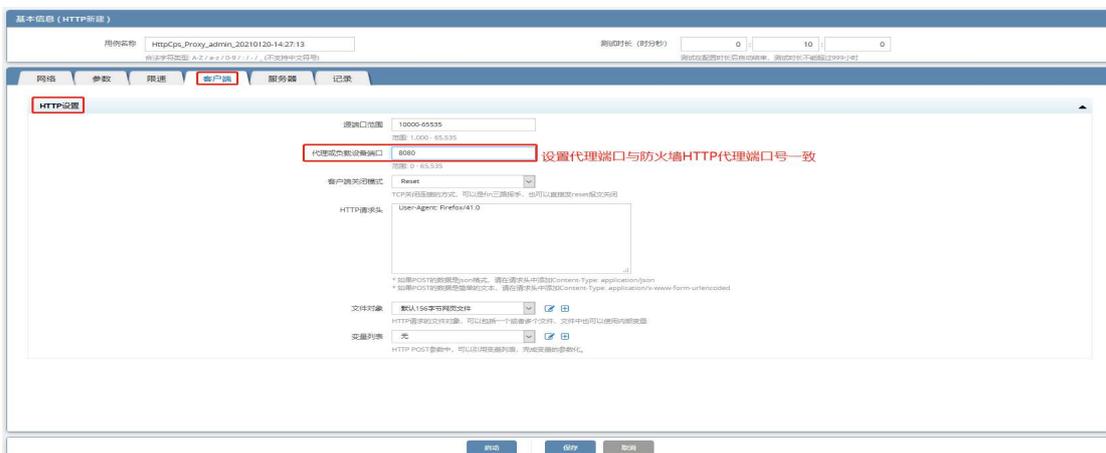


4.2 启动实例

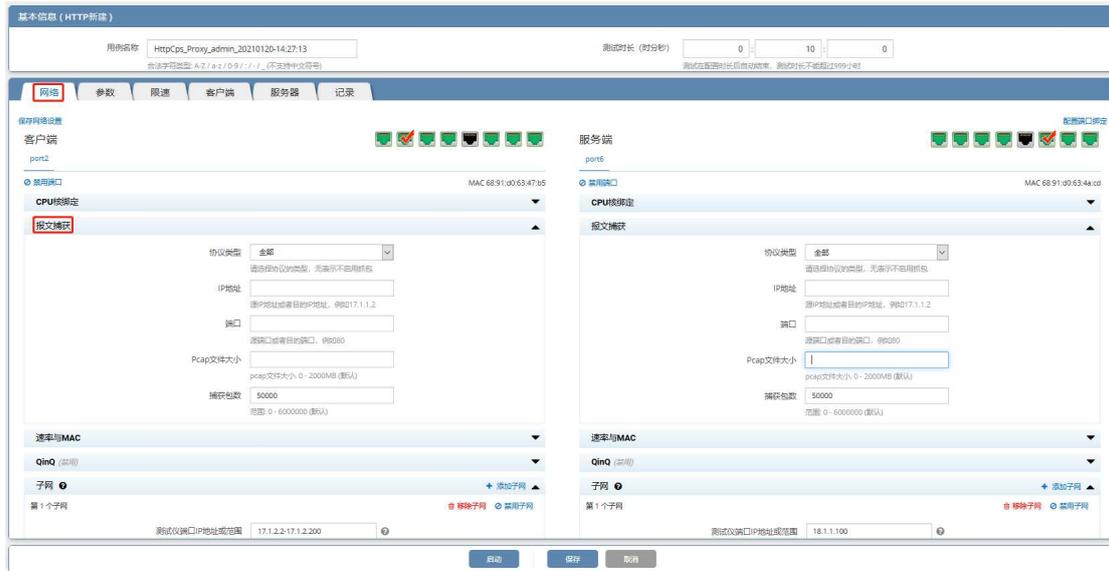
用例参数配置中选择正向代理：



选择代理端口号：



配置报文捕获查看用例运行报文交互过程：

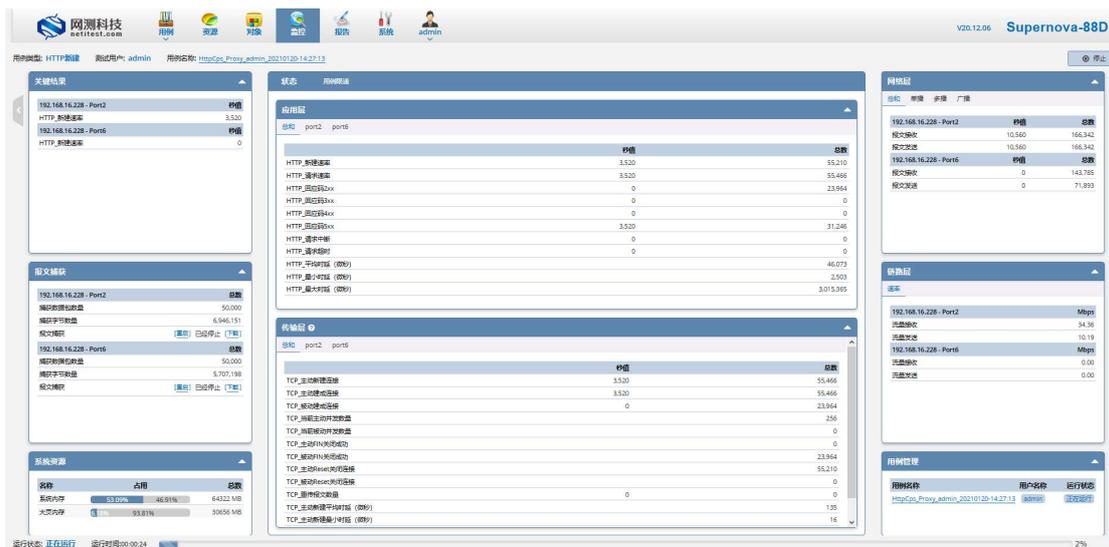


4.4 启动后正常运行界面

用例编辑保存后，点击运行按钮运行测试用例



用例运行监控数据页面：



用例运行结束，可以点击下载报告查看用例运行中报文交互



客户端报文：

