Supernova 测试仪

NAT 模式 VLAN 配置手册

网测科技

2021/11/09

目　　录

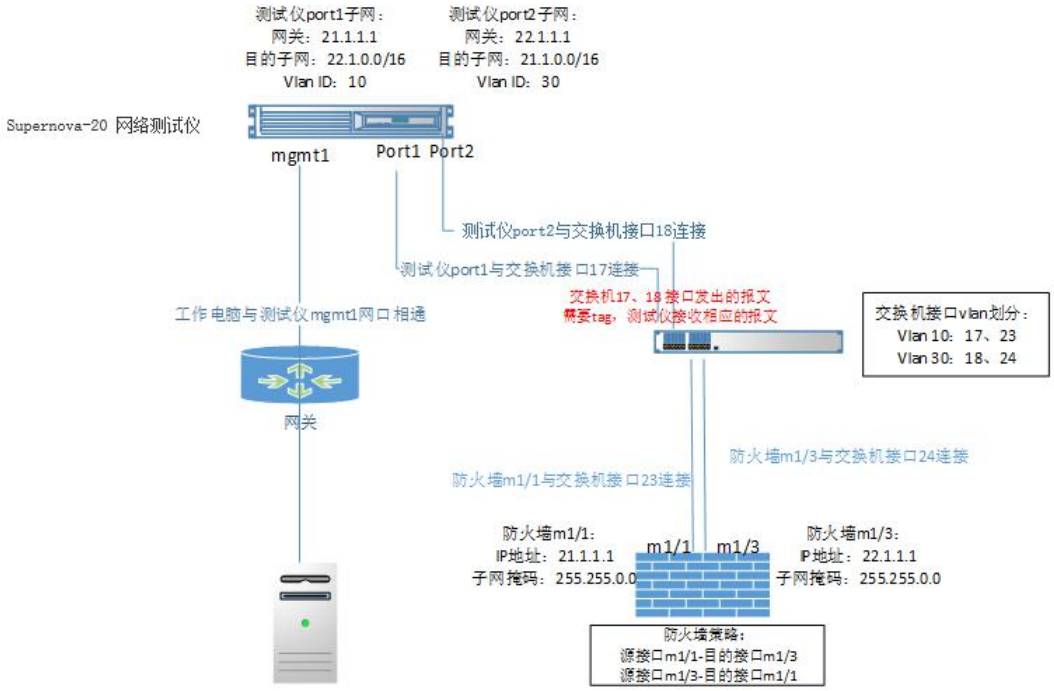
目录

1. 文档说明

本文档介绍受测设备为 NAT 工作模式时，测试仪支持 VLAN 的部署配置过程。随着版本的不断更新升级，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

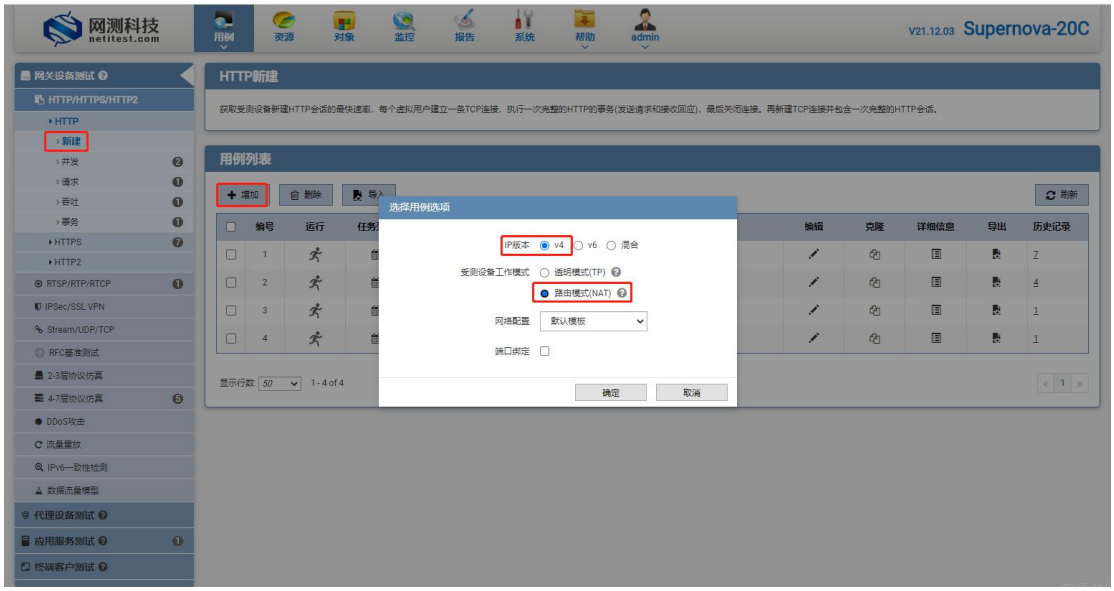
Supernova-网络测试仪 mgmt1 网口与工作电脑通过网关相通，Port1 模拟客户端，属于 VLAN 10，通过交换机同一 VLAN 与受测设备防火墙 m1/1 相连，Port2 模拟服务器，属于 VLAN 30，通过交换机同一 VLAN 与受测设备防火墙 m1/3 相连。网络拓扑图如下：



3. 创建测试用例

创建一个 HTTP 新建用例，受测设备是 NAT 工作模式，支持 VLAN，并修改配置参数，比如端口的 IP 地址以及虚拟用户的数量。

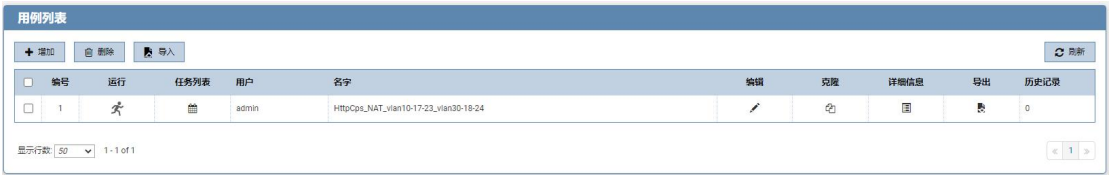
1）通过 web 登录测试仪，依次点击用例 -> 网关设备测试 -> HTTP -> 新建，单击添加，在弹出的选择用例选项中，做如下选择，然后点击确定，进入用例配置页面。



2）输入 HTTP 新建用例的名称，设置用例名称和测试时长，用例保存后也可修改为便于识别的的名称，测试时长可以根据自己的需求需改。

3）根据网络拓扑，配置端口和 IP 地址，子网配置勾选 VLAN ID，根据测试需求选择抓包协议类型和数量。

4）设置虚拟用户数量，虚拟用户数量不能大于客户端子网 IP 地址的数量，可以根据客户端子网 IP 地址的数量修改虚拟用户数量，点击保存，保存 HTTP 新建用例的配置。



4. 配置防火墙

以简网科技的防火墙为例进行说明。让防火墙的 m1/1 端口通过交换机与测试仪的客户端 port1 连接，作为客户端 port1 的网关；让防火墙的 m1/3 端口通过交换机与测试仪的服务器 port2 连接，作为服务器 port2 的网关。

4.1 设置防火墙工作模式

通过 web 登录防火墙，系统管理->控制面板->状态，查看操作模式，运行模式设置为 NAT。

4.2 设置接口 ip 地址

1）系统管理->网络->接口，m1/1 设置为客户端网关，m1/3 设置为服务器网关。

2）编辑防火墙的 m1/1 端口，输入别名，配置为测试用例中客户端 port1 子网的网关地址，点击 OK 保存。

3）编辑防火墙的 m1/3 端口，输入别名，配置为测试用例中服务器 port2 子网的网关地址，点击 OK 保存.

4.3 设置防火墙策略

1）IP 地址配置好之后，开始配置防火墙访问策略，让测试流量在 m1/1 端口和 m1/3 端口之间进行转发。进入防火墙策略管理界面，点击创建，添加新的访问策略。

2）第一条策略为，允许从 m1/1 端口到 m1/3 端口的所有流量转发；第二条策略为，允许从 m1/3 端口到 m1/1 端口的所有流量转发。点击返回首页，可查看新建策略接口流向。


KFW
监控
系统管理
路由
防火墙
病毒与攻击
上网行为管理
VPN
设置用户
日志与报告
防火墙 / 策略 / 策略
编辑输出策略
源接口/区
port3(server_port2)
源地址
all
多选
目的接口/区
port1(client_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
紧急
NAT
不使用 NAT
启用 NAT
动态IP地址池
使用中央NAT表


KFW
监控
系统管理
路由
防火墙
病毒与攻击
上网行为管理
VPN
设置用户
日志与报告
admin
防火墙 / 策略 / 策略
创建
编辑
删除
移动到
复制
插入
冲突检查
有效性检查
进入批处理
[列设定]
基于接口查看
清单式查看
序号
源地址
目的地址
时刻表
服务
动作
状态
port1(client_port1) -> port3(server_port2) (1)
port3(server_port2) -> port1(client_port1) (1)
隐形 (1)

5. 交换机 VLAN 划分

5.1 交换机接口规划

以华为交换机为例，根据交换机的接口来划分 VLAN。华为定义了 Access 接口、Trunk 接口、Hybrid 接口，各类型接口对数据帧的处理方式如表 1：

表 1：各类型接口对数据帧的处理方式

接口类型	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理	发送帧处理过程
Access 接口	接收该报文，并打上缺省的 VLAN ID。	1）当 VLAN ID 与缺省 VLAN ID 相同时，接收该报文。 2）当 VLAN ID 与缺省 VLAN ID 不同时，丢弃该报文。	先剥离帧的 PVID Tag，然后再发送。
Trunk 接口	1）打上缺省的 VLAN ID，当缺省 VLAN ID 在允许通过的 VLAN ID 列表里时，接收该报文。 2）打上缺省的 VLAN ID，当缺省 VLAN ID 不在允许通过的 VLAN ID 列表里时，丢弃该报文。	1）当 VLAN ID 在接口允许通过的 VLAN ID 列表里时，接收该报文。 2）当 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，丢弃该报文。	1）当 VLAN ID 与缺省 VLAN ID 相同，且是该接口允许通过的 VLAN ID 时，去掉 Tag，发送该报文。 2）当 VLAN ID 与缺省 VLAN ID 不同，且是该接口允许通过的 VLAN ID 时，保持原有 Tag，发送该报文。
Hybrid 接口	1）打上缺省的 VLAN ID，当缺省 VLAN ID 在允许通过的 VLAN ID 列表里时，接收该报文。 2）打上缺省的 VLAN ID，当缺省 VLAN ID 不在允许通过的 VLAN ID 列表里时，丢弃该报文。	1）当 VLAN ID 在接口允许通过的 VLAN ID 列表里时，接收该报文。 2）当 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，丢弃该报文。	当 VLAN ID 是该接口允许通过的 VLAN ID 时，发送该报文。可以通过命令设置发送时是否携带 Tag。

根据各类型接口对数据帧的处理方式不同（见表 1）及网络拓扑需求，将交换机接口 17、18、23、24 规划如表 2 所示：

表 2：接口规划

交换机接口	接口类型	VLAN ID	PVID	TAG
接口 17（与测试仪相连）	Hybrid 接口	10	10	10
接口 18（与测试仪相连）	Hybrid 接口	30	30	30
接口 23（与防火墙相连）	Access 接口	10	10	10
接口 24（与防火墙相连）	Access 接口	30	30	30

5.2 交换机 vlan 划分

使用串口线连接交换机与工作电脑相连，通过 SecureCRT 连上交换机，输入用户名和密码，登录成功。

5.2.1 创建 VLAN

1）system-view　　//进入系统视图。

2）vlan 10　　//创建 VLAN 10 并进入 VLAN 10 视图。如果 VLAN 已经创建，则直接进入 VLAN 视图。

3）quit　　//返回系统视图。

4）vlan 30　　//创建 VLAN30 并进入 VLAN 30 视图。如果 VLAN 已经创建，则直接进入 VLAN 视图。

5）quit　　//返回系统视图。

5.2.2 接口加入 VLAN

根据 5.1 章节的接口规划，执行如下命令：

1.规划为 Access 接口：

接口 23 配置

1）interface XGigabitEthernet 0/0/23 //进入需要加入 VLAN 的以太网接口 23 视图。

2） port link-type access　　//配置接口类型为 access。

3）port default vlan 10　　//配置接口的缺省 VLAN 并将接口加入到指定 VLAN。

4） quit　　//返回系统视图

接口 24 配置

1）interface XGigabitEthernet 0/0/24 //进入需要加入 VLAN 的以太网接口 24 视图。

2） port link-type access　　//配置接口类型为 access。

3）port default vlan 30　　//配置接口的缺省 VLAN 并将接口加入到指定 VLAN。

4） quit　　//返回系统视图

2.规划为 Hybrid 接口：

接口 17 配置

1）interface XGigabitEthernet 0/0/17 //进入需要加入 VLAN 的以太网接口 17 视图。

2） port link-type hybrid　　//配置接口类型为 hybrid。

3） port hybrid pvid vlan 10　　//配置 Hybrid 接口的缺省 VLAN。

4） port hybrid tagged vlan 10　　//将 Hybrid 接口以 Tagged 方式加入 VLAN

5） quit　　//返回系统视图

接口 18 配置

1）interface XGigabitEthernet 0/0/18//进入需要加入 VLAN 的以太网接口 18 视图。

2）port link-type hybrid　　//配置接口类型为 hybrid。

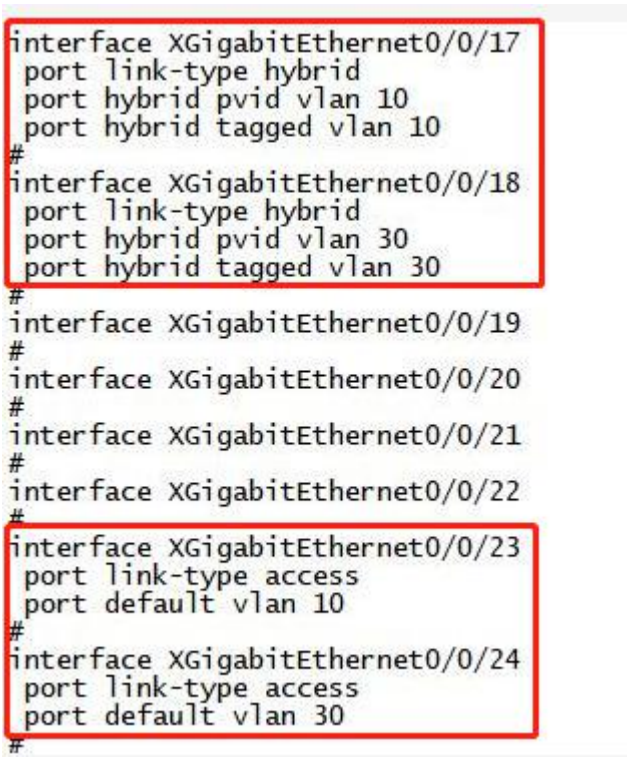
3）port hybrid pvid vlan 30　　//配置 Hybrid 接口的缺省 VLAN。

4）port hybrid tagged vlan 30　　//将 Hybrid 接口以 Tagged 方式加入 VLAN

5）quit　　//返回系统视图

5.2.3 查看接口配置信息

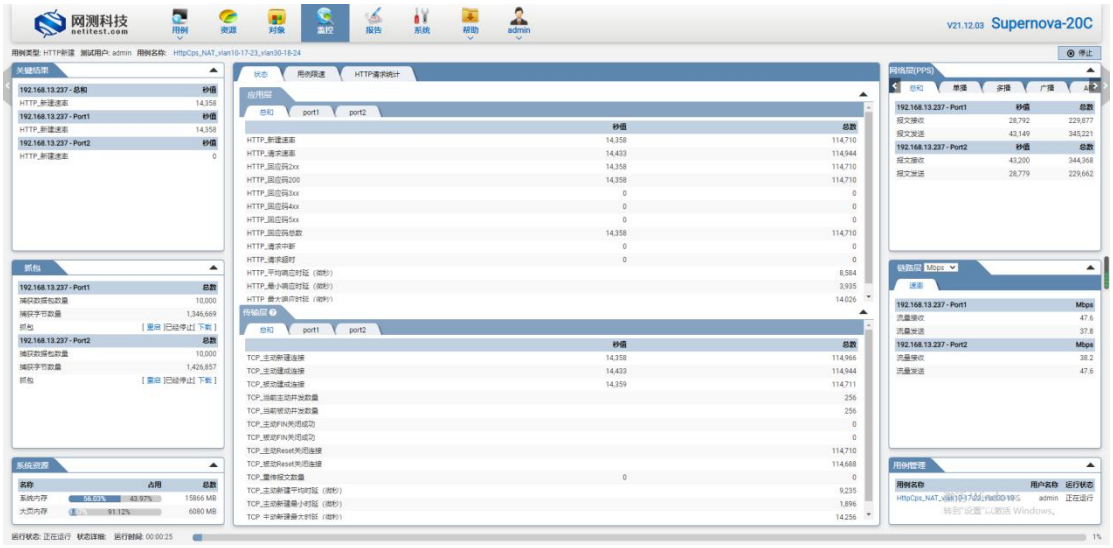
执行命令 display current-configuration



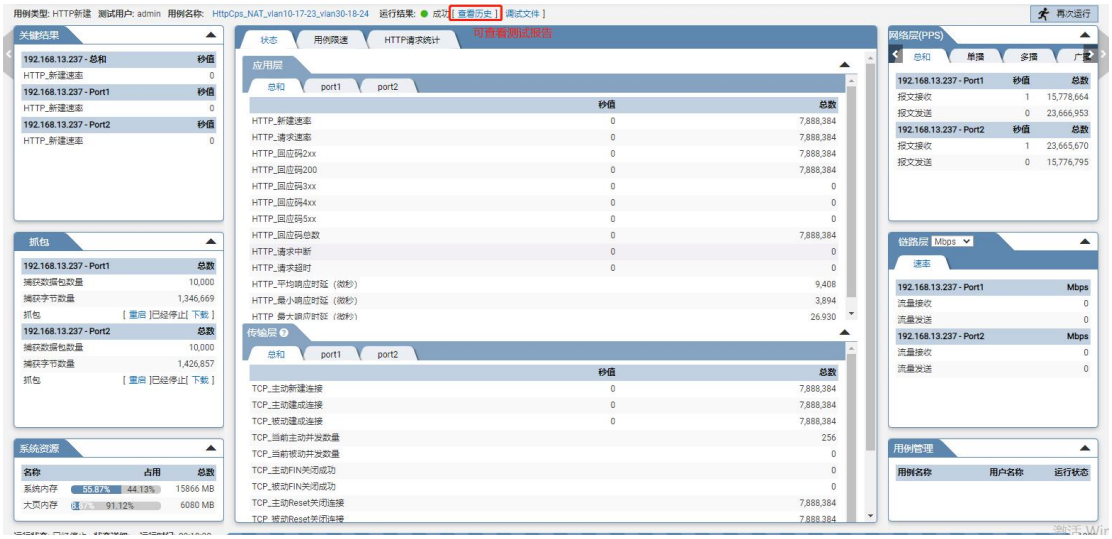
6. 运行用例

1）回到测试仪的用例管理界面，点击运行启动 HTTP 新建测试用例。

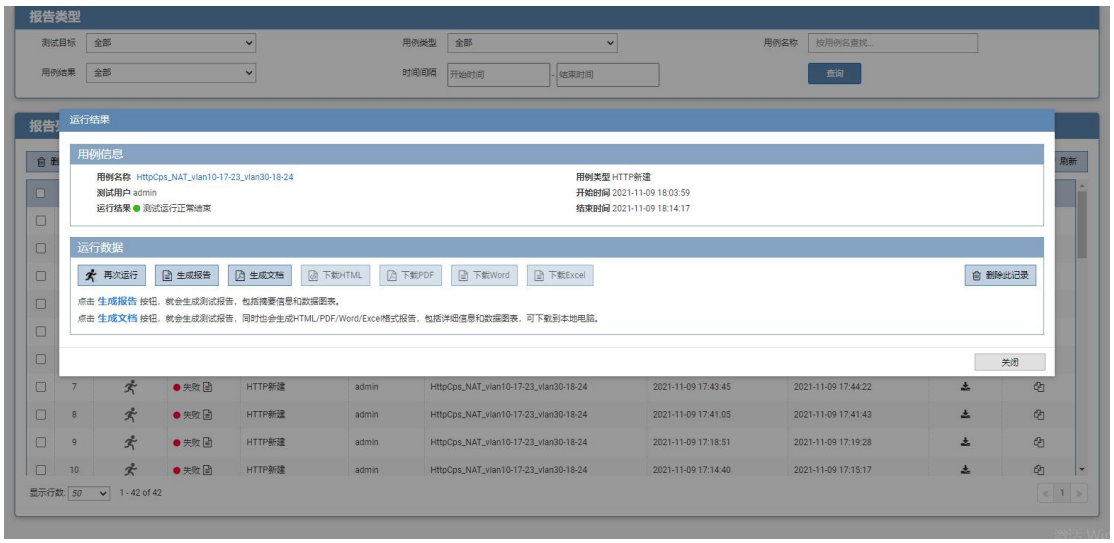
2）用例运行启动后，可以在监控页面查看运行详细数据

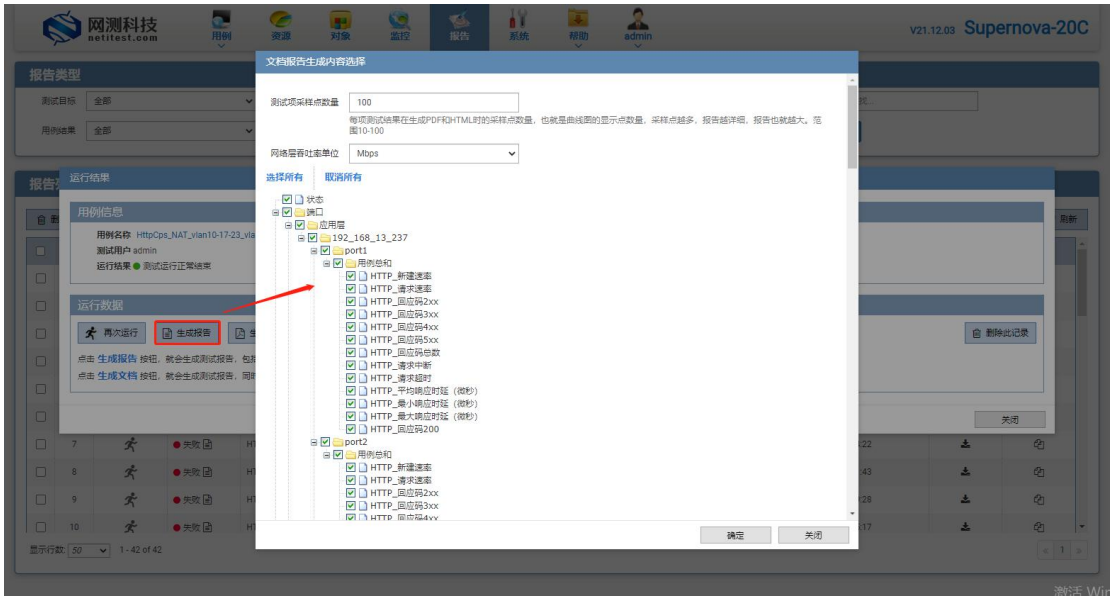


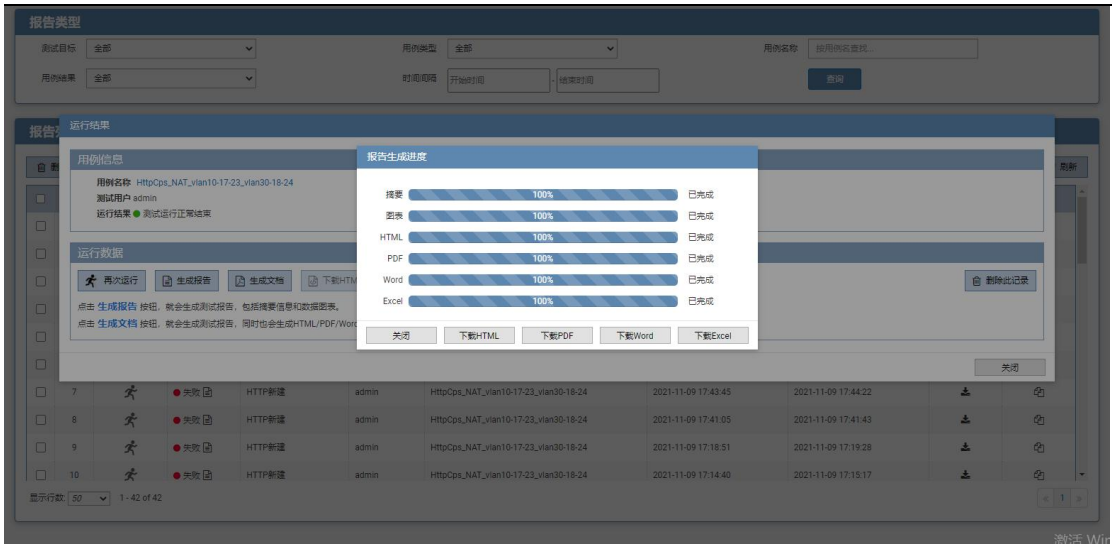
3）用例运行结束，点击查看历史，可以查看测试报告。

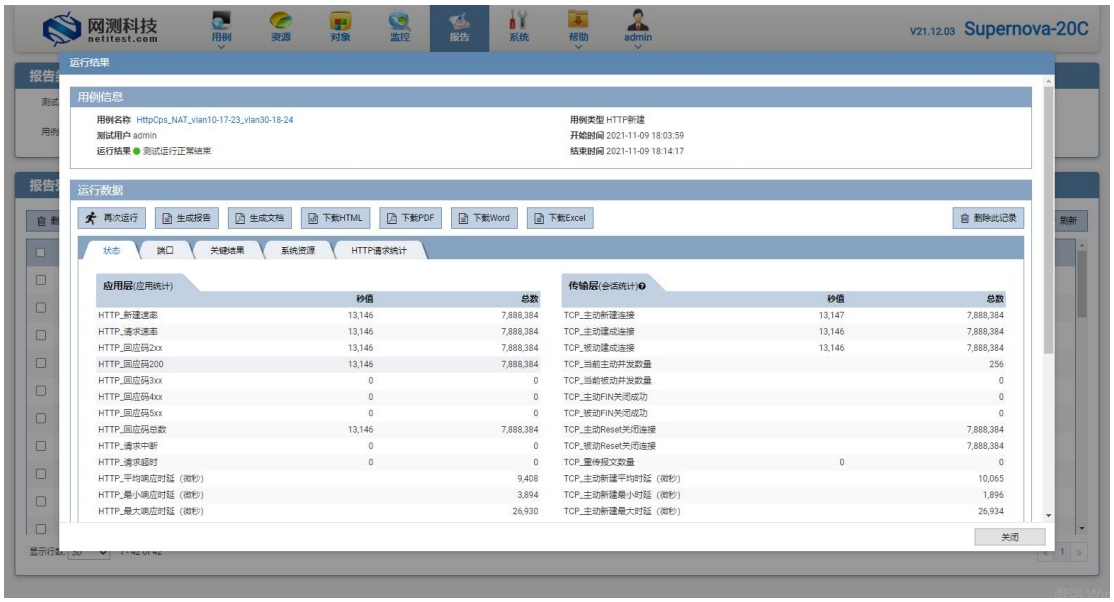


4）生成报告数据及 HTML/PDF/Word 报告，报告生成后，可以下载 HTML/PDF/Word 格式测试报告

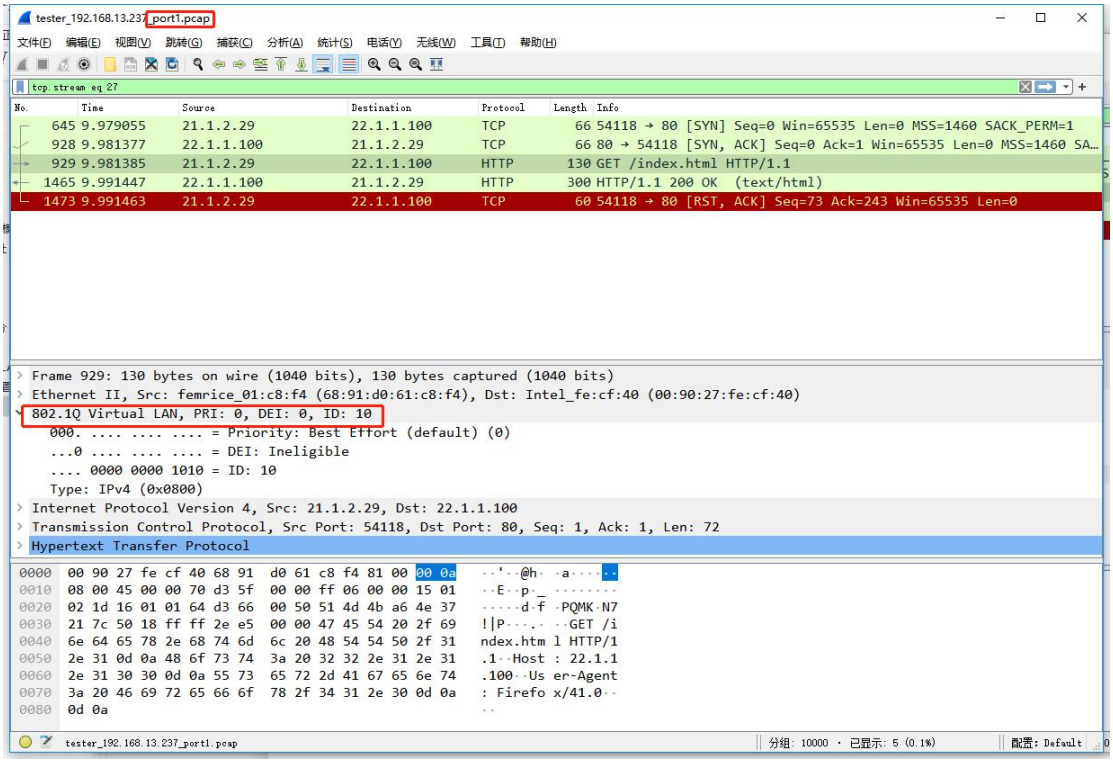


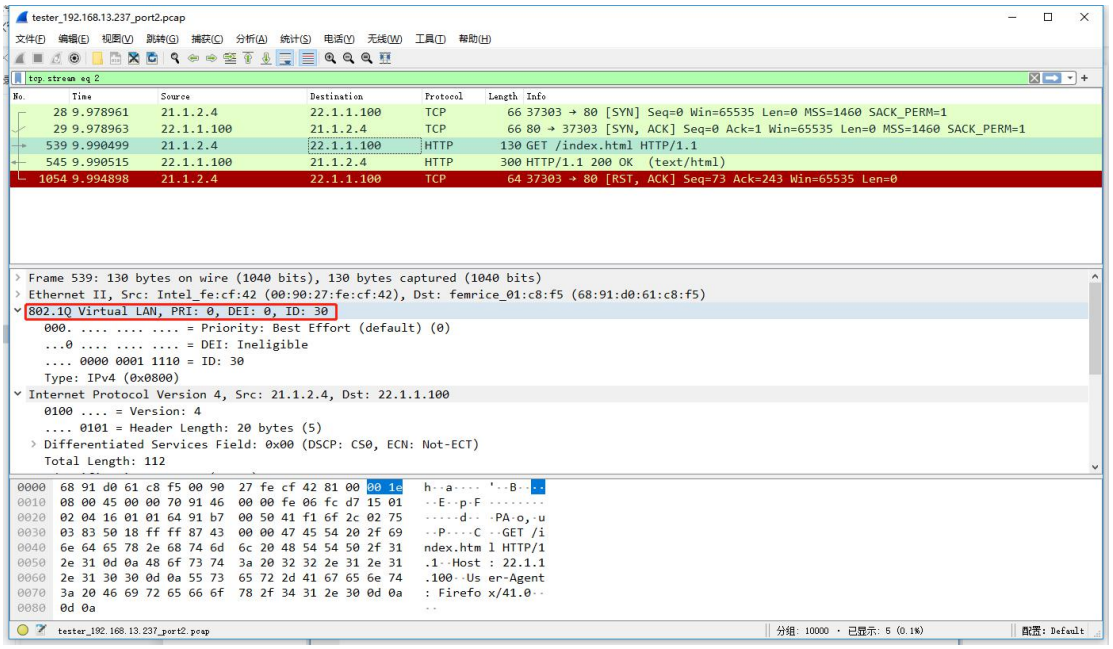






5）抓包可查看 vlan 标志，比对是否符合用例运行前的配置。


tester_192.168.13.237_port1.pcap
tcp.stream eq 27
No. Time Source Destination Protocol Length Info
645 9.979055 21.1.2.29 22.1.1.100 TCP 66 54118 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
928 9.981377 22.1.1.100 21.1.2.29 TCP 66 80 → 54118 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SA…
929 9.981385 21.1.2.29 22.1.1.100 HTTP 130 GET /index.html HTTP/1.1
1465 9.991447 22.1.1.100 21.1.2.29 HTTP 300 HTTP/1.1 200 OK (text/html)
1473 9.991463 21.1.2.29 22.1.1.100 TCP 60 54118 → 80 [RST, ACK] Seq=73 Ack=243 Win=65535 Len=0
Frame 929: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
Ethernet II, Src: femrice_01:c8:f4 (68:91:d0:61:c8:f4), Dst: Intel_fe:cf:40 (00:90:27:fe:cf:40)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
.... 0000 0000 1010 = ID: 10
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 21.1.2.29, Dst: 22.1.1.100
Transmission Control Protocol, Src Port: 54118, Dst Port: 80, Seq: 1, Ack: 1, Len: 72
Hypertext Transfer Protocol
0000 00 90 27 fe cf 40 68 91 d0 61 c8 f4 81 00 00 0a
0010 08 00 45 00 00 70 d3 5f 00 00 ff 06 00 00 15 01
0020 02 1d 16 01 01 64 d3 66 00 50 51 4d 4b a6 4e 37
0030 21 7c 50 18 ff ff 2e e5 00 00 47 45 54 20 2f 69
0040 6e 64 65 78 2e 68 74 6d 6c 20 48 54 54 50 2f 31
0050 2e 31 0d 0a 48 6f 73 74 3a 20 32 32 2e 31 2e 31
0060 2e 31 30 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74
0070 3a 20 46 69 72 65 66 6f 78 2f 34 31 2e 30 0d 0a
0080 0d 0a


tester_192.168.13.237_port2.pcap
tcp.stream eq 2
No. Time Source Destination Protocol Length Info
28 9.978961 21.1.2.4 22.1.1.100 TCP 66 37303 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
29 9.978963 22.1.1.100 21.1.2.4 TCP 66 80 → 37303 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1
539 9.990499 21.1.2.4 22.1.1.100 HTTP 130 GET /index.html HTTP/1.1
545 9.990515 22.1.1.100 21.1.2.4 HTTP 300 HTTP/1.1 200 OK (text/html)
1054 9.994898 21.1.2.4 22.1.1.100 TCP 64 37303 → 80 [RST, ACK] Seq=73 Ack=243 Win=65535 Len=0
Frame 539: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
Ethernet II, Src: Intel_fe:cf:42 (00:90:27:fe:cf:42), Dst: femrice_01:c8:f5 (68:91:d0:61:c8:f5)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 30
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
.... 0000 0001 1110 = ID: 30
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 21.1.2.4, Dst: 22.1.1.100
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 112
0000 68 91 d0 61 c8 f5 00 90 27 fe cf 42 81 00 00 1e
0010 08 00 45 00 00 70 91 46 00 00 fe 06 fc d7 15 01
0020 02 04 16 01 01 64 91 b7 00 50 41 f1 6f 2c 02 75
0030 03 83 50 18 ff ff 87 43 00 00 47 45 54 20 2f 69
0040 6e 64 65 78 2e 68 74 6d 6c 20 48 54 54 50 2f 31
0050 2e 31 0d 0a 48 6f 73 74 3a 20 32 32 2e 31 2e 31
0060 2e 31 30 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74
0070 3a 20 46 69 72 65 66 6f 78 2f 34 31 2e 30 0d 0a
0080 0d 0a