

Supernova 测试仪 报文字段跳变配置手册

网测科技

2021-01-27

目录

1. 文档说明.....	3
2. 功能介绍.....	3
3. 配置报文跳变.....	4
4. 创建用例测试.....	7
5. 用例运行测试.....	9
6. 抓包验证.....	9

1. 文档说明

本文档主要介绍报文字段跳变的配置使用过程。随着需求的不断改变，可能会对用例配置进行修改和升级，从而改变配置过程，所以有任何问题，请联系我们的售前或售后支持人员。

2. 功能介绍

Supernova 支持对报文设置跳变，即指对 Pcap 报文的字段进行一些固定、递增、递减、列表和随机等有规则的变化，此功能可以在 TCP 流重放测试和流量重放测试中使用。

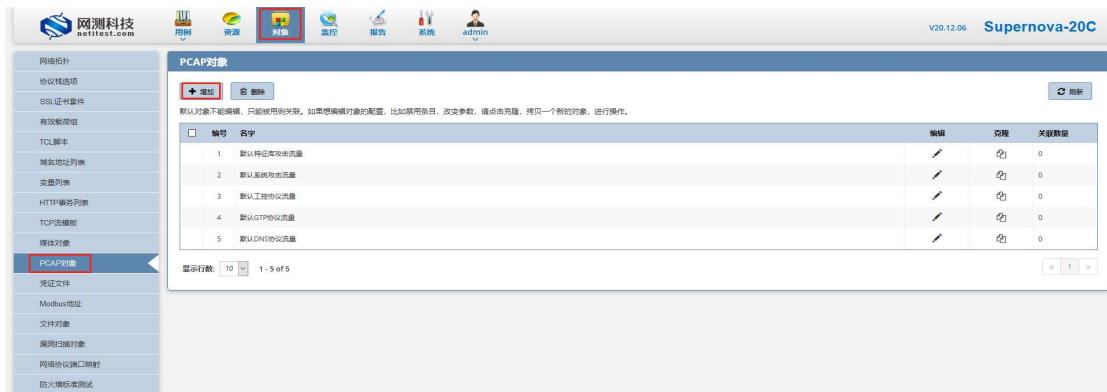
Supernova 通过配置 TCP 流模板重放 TCP 流，TCP 流模板中只能对 TCP 报文载荷设置跳变。

Supernova 支持使用 PCAP 文件生成流，进行流量重放特定格式的 pcap 文件。PCAP 对象可以对报文的任何字段进行跳变设置。

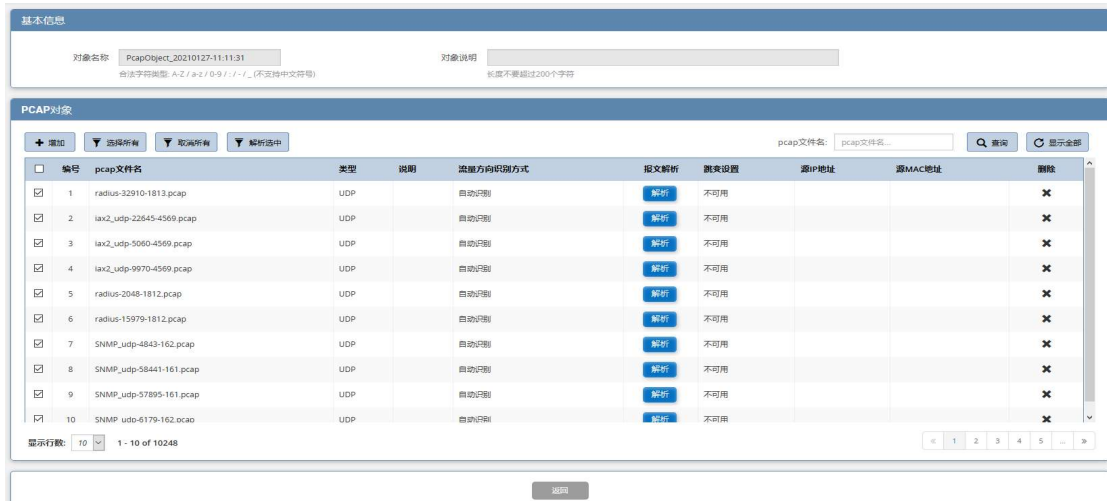
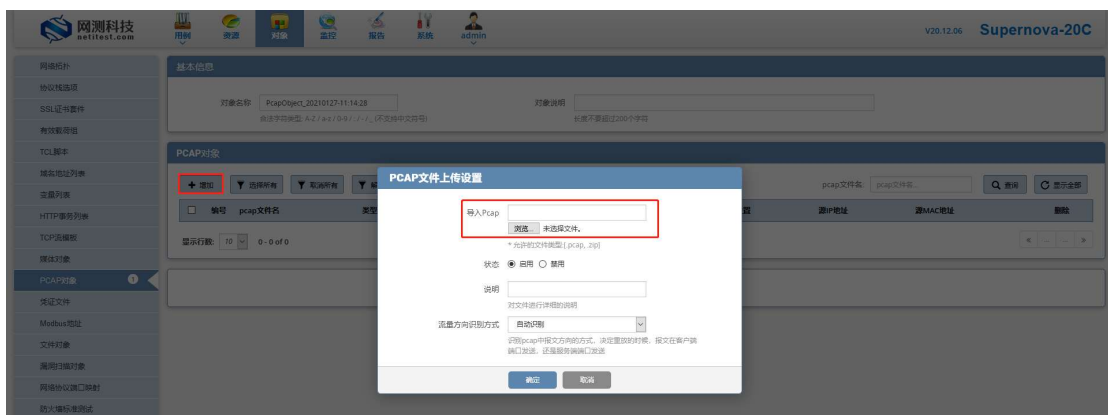
3. 配置报文跳变

报文字段跳变功能的使用，根据需要运行的流量重放或者 TCP 流重放测试用例，先新增创建一个 PCAP 对象或者 TCP 流模板，在 PCAP 对象或者 TCP 流模板进行报文字段跳变配置，然后在用例中引用配置完成的对象。下面以攻击流量重放用例使用报文跳变功能举例说明。

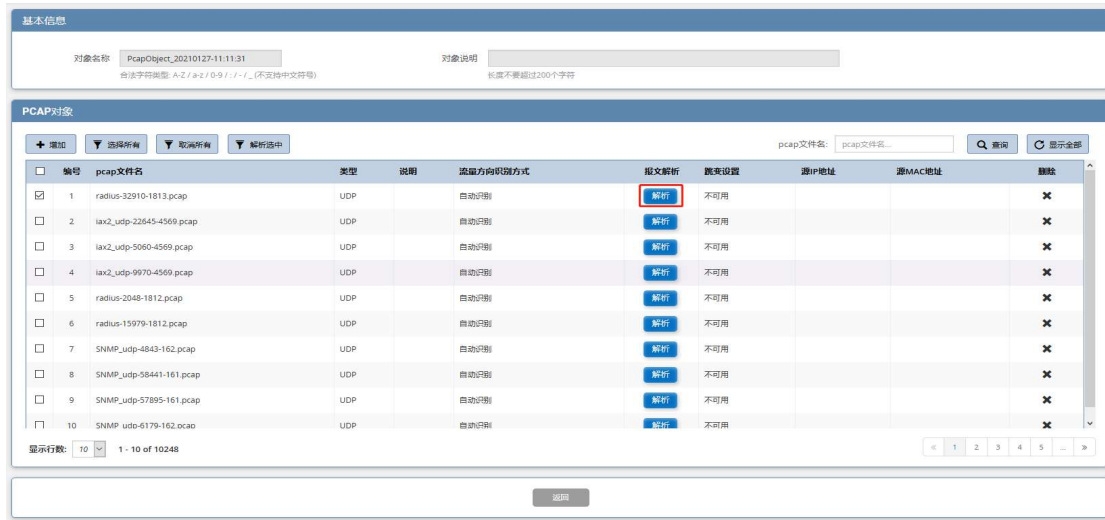
1) 点击对象→PCAP 对象→新增，创建 PCAP 对象。



2) 点击增加→导入 Pcap，导入 pcap 文件。



3) 解析 PCAP 报文，选中需要设置跳变的 Pcap 报文，点击解析。



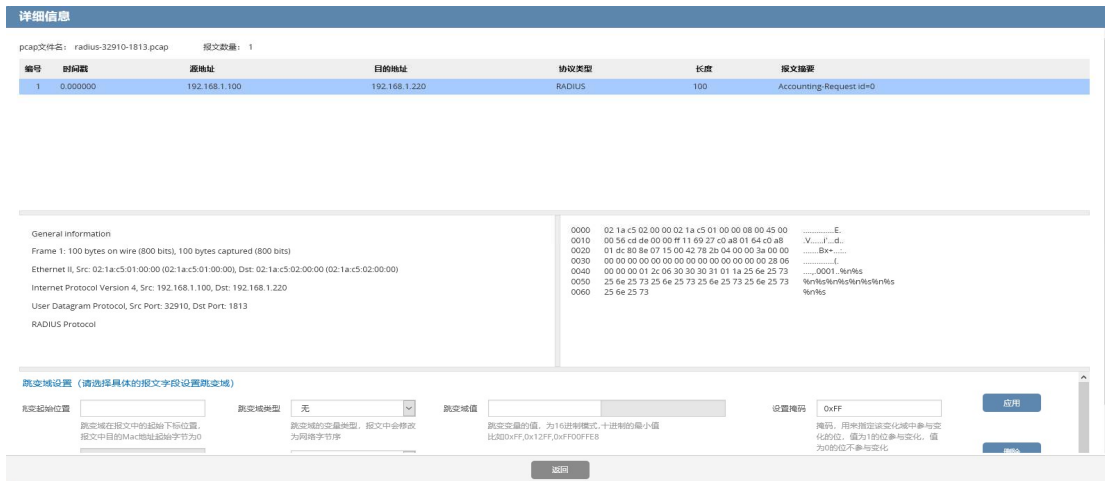
基本信息

对象名称: PcapObject_20210127-11:11:31
 对象说明: [空]

PCAP对象

编号	pcap文件名	类型	说明	流量方向识别方式	报文解析	跳变设置	源IP地址	源MAC地址	删除
1	radius-32910-1813.pcap	UDP		自动识别	解析	不可用			✕
2	iax2_udp-22645-4569.pcap	UDP		自动识别	解析	不可用			✕
3	iax2_udp-5060-4569.pcap	UDP		自动识别	解析	不可用			✕
4	iax2_udp-9970-4569.pcap	UDP		自动识别	解析	不可用			✕
5	radius-2048-1812.pcap	UDP		自动识别	解析	不可用			✕
6	radius-15979-1812.pcap	UDP		自动识别	解析	不可用			✕
7	SNMP_udp-4843-162.pcap	UDP		自动识别	解析	不可用			✕
8	SNMP_udp-58441-161.pcap	UDP		自动识别	解析	不可用			✕
9	SNMP_udp-57895-161.pcap	UDP		自动识别	解析	不可用			✕
10	SNMP_udp-6179-162.pcap	UDP		自动识别	解析	不可用			✕

显示行数: 10 / 1 - 10 of 10248



详细信息

pcap文件名: radius-32910-1813.pcap 报文数量: 1

编号	时间戳	源地址	目的地址	协议类型	长度	报文摘要
1	0.000000	192.168.1.100	192.168.1.220	RADIUS	100	Accounting-Request id=0

General information

Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)

Ethernet II, Src: 02:1a:c5:01:00:00 (02:1a:c5:01:00:00), Dst: 02:1a:c5:02:00:00 (02:1a:c5:02:00:00)

Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.220

User Datagram Protocol, Src Port: 32910, Dst Port: 1813

RADIUS Protocol

跳变域设置 (请选择具体的报文字段设置跳变域)

跳变域起始位置: [空] 跳变域类型: 无 跳变域值: [空] 设置掩码: 0x0F

4) 设置跳变字段，报文字段跳变类型支持单字节数值、双字节数值、四字节数值、单字符类型，跳变方式支持固定、递增、递减、随机、列表。



详细信息

编号	时间戳	源地址	目的地址	协议类型	长度	报文摘要
1	0.000000	192.168.1.100	192.168.1.220	IAX2	64	IAX, source call# 1, timestamp 0ms NEW
2	0.276033	192.168.1.220	192.168.1.100	IAX2	60	IAX, source call# 1, timestamp 2ms ACCEPT
3	0.736562	192.168.1.100	192.168.1.220	IAX2	60	IAX, source call# 1, timestamp 24ms ACK
4	1.003480	192.168.1.220	192.168.1.100	IAX2	60	Control, source call# 1, timestamp 54ms ANSWER
5	1.250212	192.168.1.100	192.168.1.220	IAX2	60	IAX, source call# 1, timestamp 55ms ACK
6	1.305397	192.168.1.100	192.168.1.220	IAX2	60	IAX, source call# 1, timestamp 67ms LAGRQ

选择报文中跳变条目

> Ethernet II, Src: 02:1a:c5:01:00:00 (02:1a:c5:01:00:00), Dst: 02:1a:c5:02:00:00 (02:1a:c5:02:00:00)

配置具体跳变字段及跳变设置

跳变域设置 (请选择具体的报文字段设置跳变域)

跳变域起始位置: 0 跳变域类型: 无 跳变域值: [空] 设置掩码: 0x0F

跳变域长度: 14 跳变方式: 无

举例说明:

1. 跳变类型单字节数值, 跳变方式固定:

设置跳变位置为 0, 跳变类型为单字节数值, 跳变方式为固定, 跳变域值为 0x00 (0x 表示后边为 16 进制数字), 掩码为 0xFF (掩码, 用来指定该变化域中参与变化的位, 值为 1 的位参与变化, 值为 0 的位不参与变化, 参考掩码位的值, 0xFF 表示两位都参与变化)。使用此跳变设置时, 此报文中第一位字节变为 00。



报文中payload的第一个字节变为00

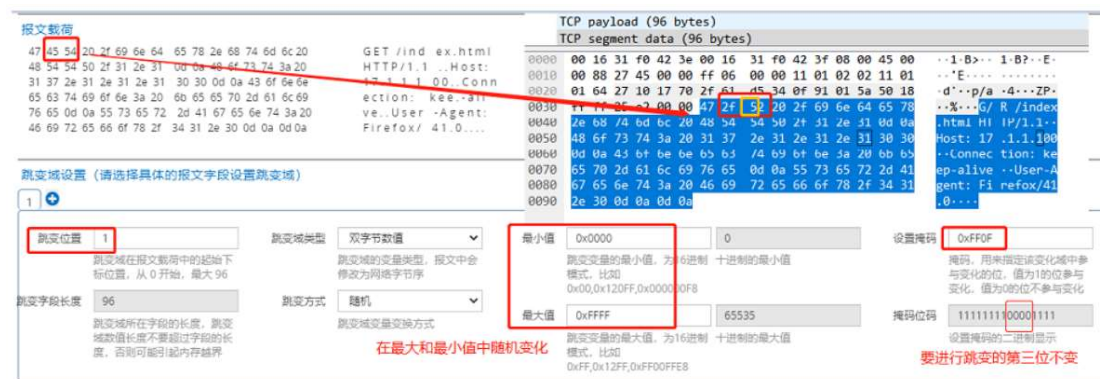
0表示第一个字节

两位都参与变化

设置掩码 0xFF

2. 跳变类型双字节数值, 跳变方式随机:

设置跳变位置为 1, 跳变类型为双字节数值, 跳变方式为随机, 跳变域最小值为 0x0000 (0x 表示后边为 16 进制数字, 两位代表一个字节), 跳变域最大值 0xFFFF, 掩码为 0xFF0F (掩码, 用来指定该变化域中参与变化的位, 值为 1 的位参与变化, 值为 0 的位不参与变化, 参考掩码位的值, 0xFF0F 表示要进行跳变的第三位不参与变化)。使用从跳变设置时, 此报文中第二位、第三位字节在跳变域范围内变化。

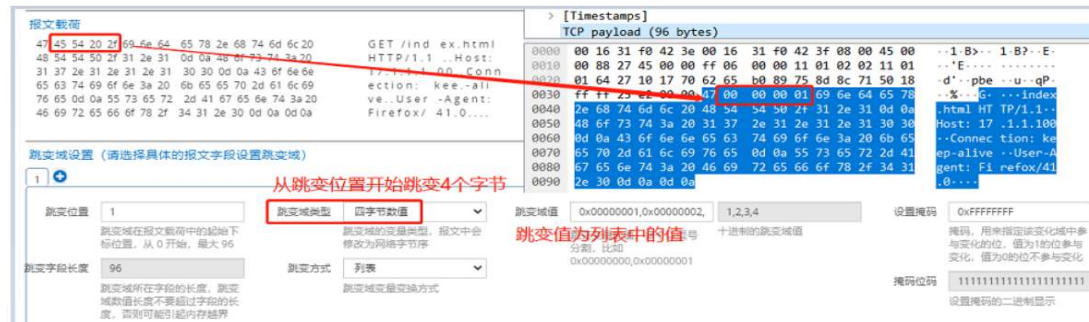


在最大和最小值中随机变化

要进行跳变的第三位不变

3. 跳变类型四字节数值, 跳变方式列表:

设置跳变位置为 1, 跳变类型为四字节数值, 跳变方式为列表, 跳变域值为 0x00000001, 0x00000002, 0x00000003, 0x00000004, 掩码为 0xFFFFFFFF。使用此跳变设置时, 此报文中第二位、第三位、第四位、第五位字节在跳变域列表内变化。

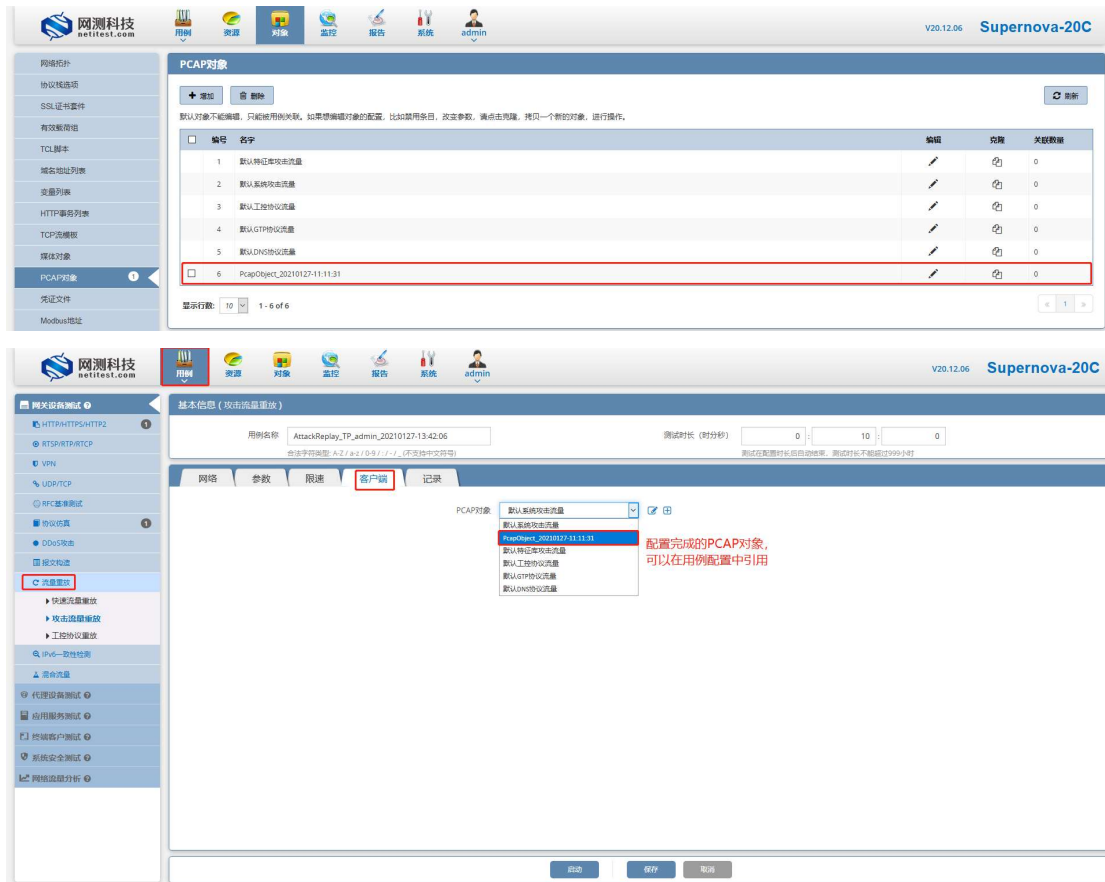


从跳变位置开始跳变4个字节

跳变域值为列表中的值

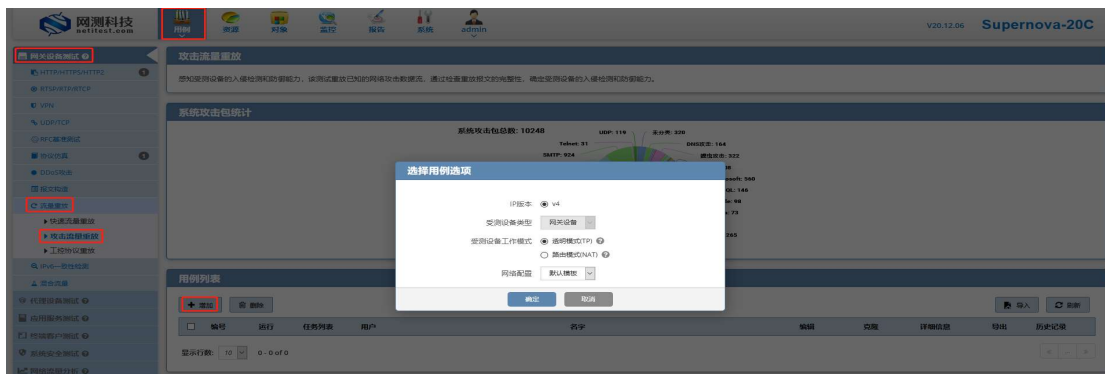
5) 设置完成后, 返回自动保存对象配置, PCAP 对象报文字段配置完成。

配置完成的 PCAP 对象可以在流量重放功能用例中设置引用。

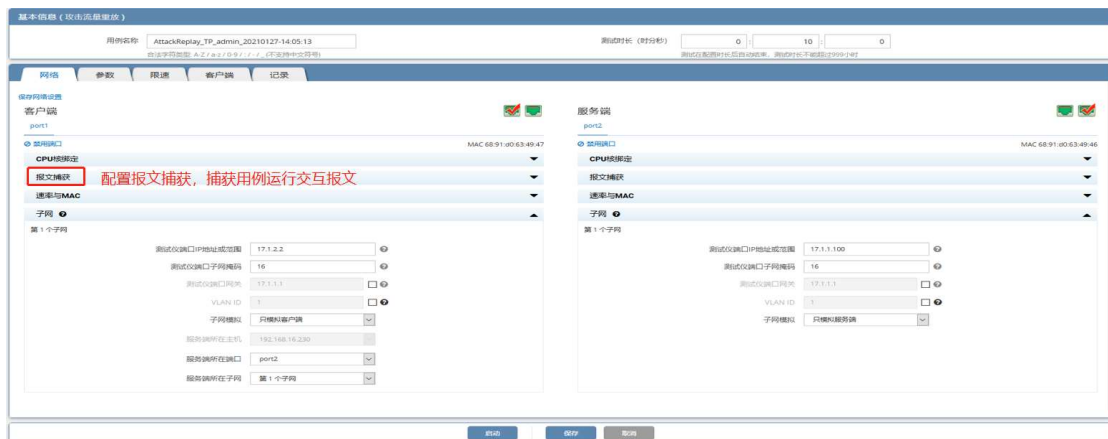


4. 创建用例测试

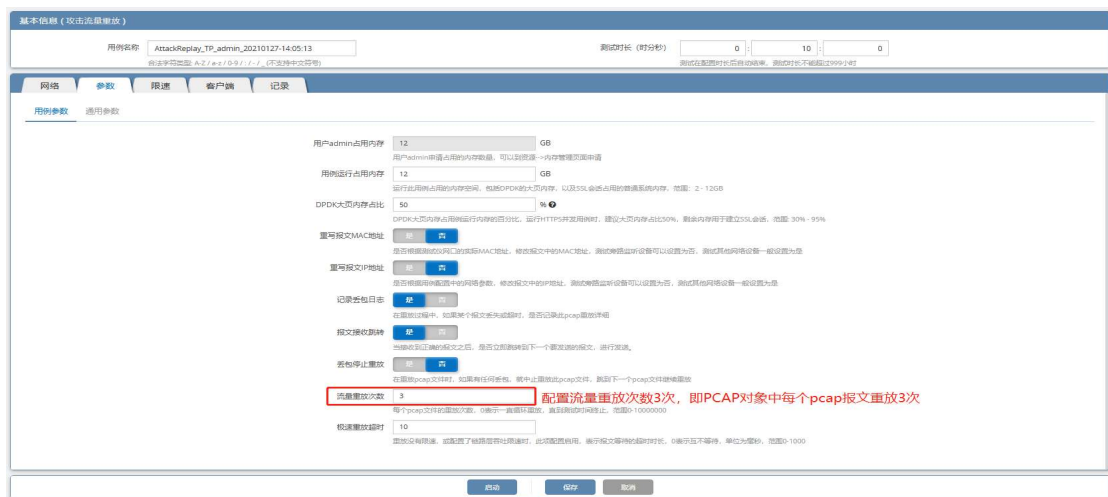
1) 登录系统, 依次点击, 用例->网关设备测试->流量重放->攻击流量重放->单击增加, 在弹出的选择用例选项中, 编辑用例网络选项, 根据需要修改配置参数, 然后点击确定, 进入用例配置页面。



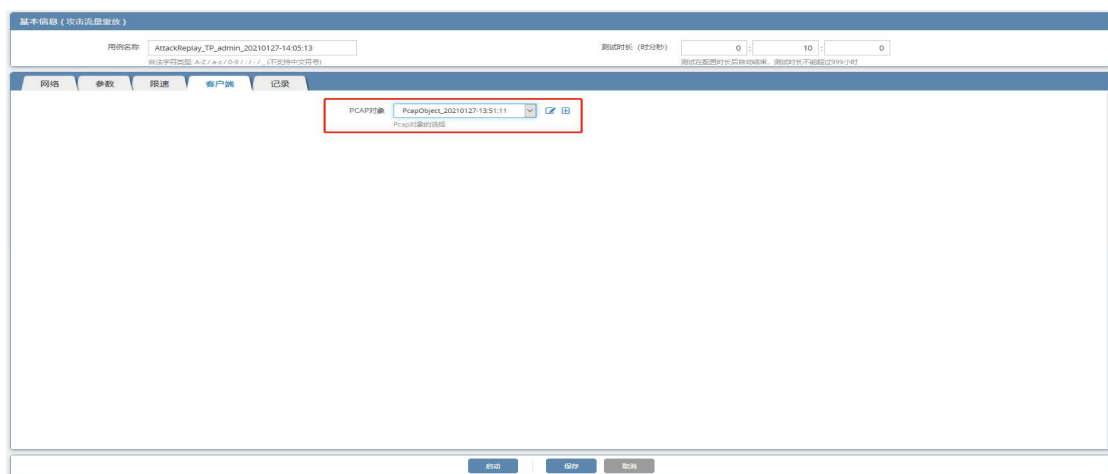
2) 点击确定，进入用例配置界面，配置测试端口、子网信息及报文捕获。



3) 进行参数配置，比如流量重放次数、丢包停止重放、重写报文 IP 地址等配置。配置完成后，保存用例。



4) 引用 PCAP 配置对象，选择编辑完成的报文跳变 PCAP 对象。

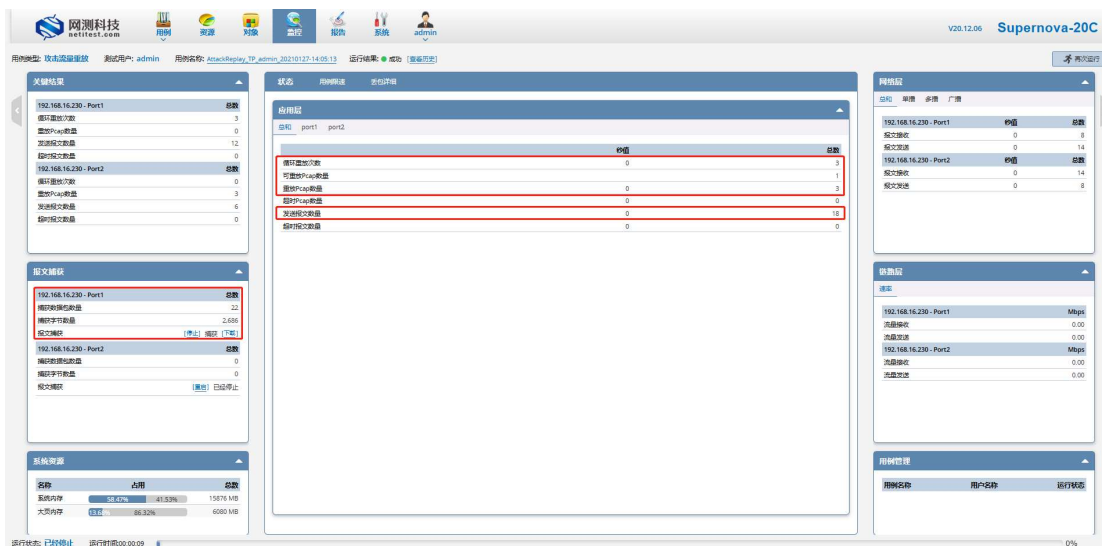


5. 用例运行测试

1) 用例保存后自动返回主页面，点击运行配置保存的攻击流量重用用例。



2) 用例启动后进入运行状态，监控页面显示循环重放次数、重放 PCAP 数量、发送报文数量等运行数据。

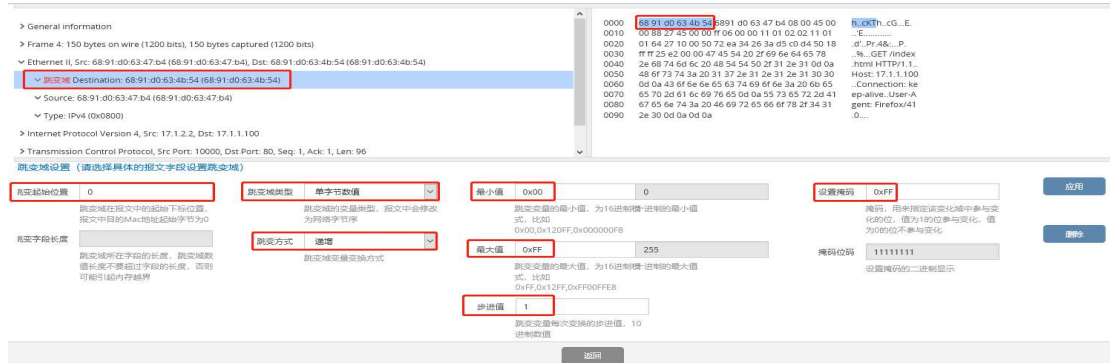


6. 抓包验证

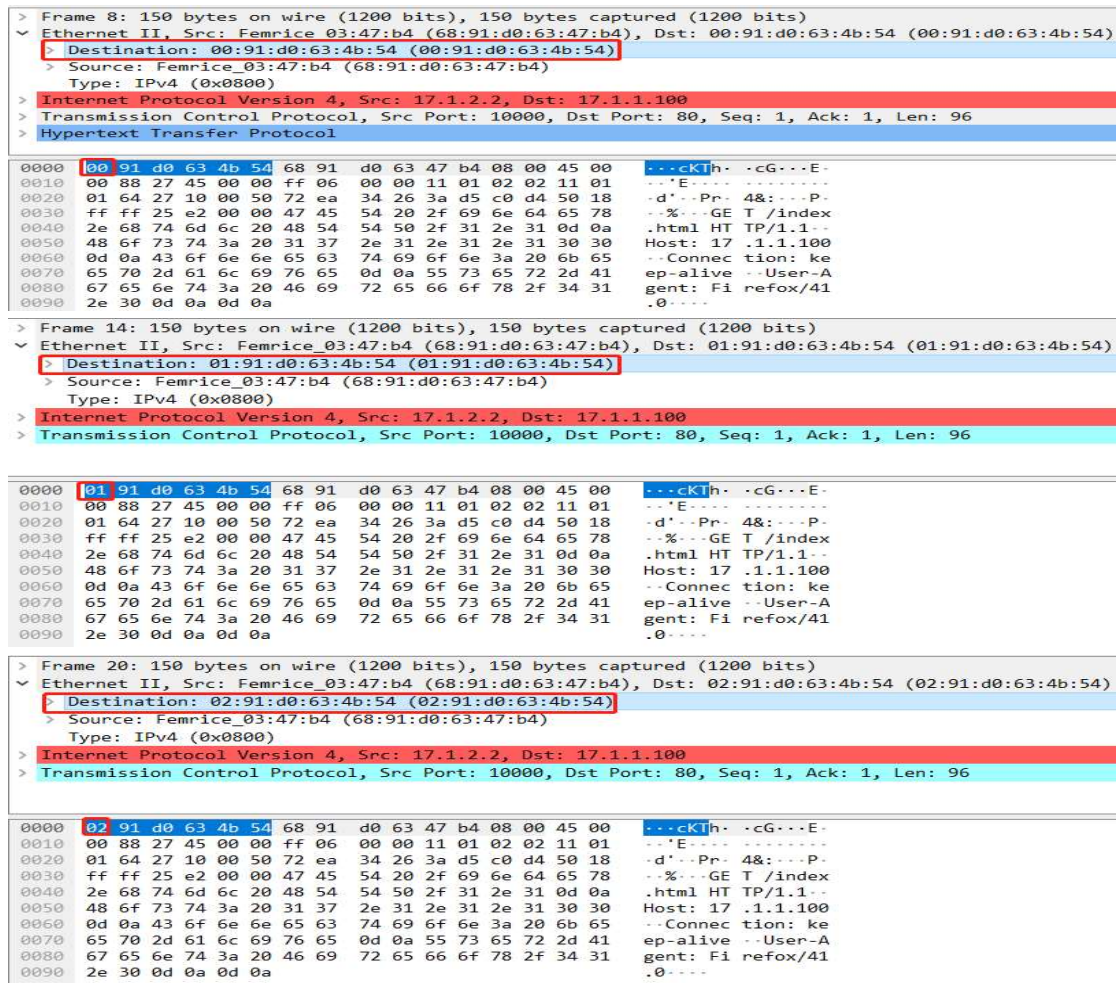
用例运行结束，点击下载打开用例运行中报文捕获的抓包文件，查看校验报文交互信息。



PCAP 对象，我们设置的报文跳变配置，设置跳变位置为 0，跳变类型为单字节数值，跳变方式为递增，跳变最小值为 0x00（0x 表示后边为 16 进制数字），跳变最大值为 0xFF，步进值为 1，掩码为 0xFF（掩码，用来指定该变化域中参与变化的位，值为 1 的位参与变化，值为 0 的位不参与变化，参考掩码位的值，0xFF 表示两位都参与变化）。因此报文中，设置跳变的字段值应该从 00、01、02 依次递增跳变。



通过 Wireshark 打开下载的用例运行报文，查看报文跳变字段。



通过查看用例运行抓包文件，交互报文中跳变值结果与配置一致。