

Dotouch XPRO 云测网络仿真测试工具



V2.0R3



声明

Copyright © 2022 北京触点互动信息技术有限公司及其许可者版权所有,保留一切权利。

未经北京触点互动信息技术有限公司书面许可,任何单位和个人不得擅自摘抄、复制本书内容的部分或全部,并 不得以任何形式传播。

Dotouch Dotouch及图标 ^{触 点 互 动} 北京触点互动信息技术有限公司的商标。对于本手册出现的其他公司的商标、产 品标识和商品名称,由各自权利人拥有。

除非另有约定,本手册仅作为使用指导,本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改, 恕不另行通知。

目录

第1章	Ī	前言	5
1.1	-	文档介绍	5
1.2	j	声明	5
1.3	-	文档约定	5
1.4	Ę	技术支持	6
第2章		基本概念	7
2.1	-	关于 XPRO 云测网络仿真测试工具	7
2.2		测试场景与拓扑	7
	2.2.1	串接测试场景	7
	2.2.2	并接测试场景	7
	2.2.3	单臂测试场景	8
2.3	,	客户端概念说明	8
2.4	J	服务端概念说明	9
第3章	Ī	配置指南	10
3.1		工程	10
3.2		系统配置	13
	3.2.1	开放平台	13
	3.2.2	用户管理	13
	3.2.3	外部攻击库	14
	3.2.4	L3 回放库管理	15
	3.2.5	病毒库管理	15
	3.2.6	L7 回放库管理	16
	3.2.7	系统信息	16
3.3		接入配置	17
	3.3.1	PPPoE	17
	3.3.2	DHCP	20
3.4		网口设置	22
3.5	7	变量设置	24
3.6	ţ	媒体对象	25
3.7		客户端	26
	3.7.1	客户端子网配置	26
	3.7.2	客户端网络配置	27
	3.7.3	客户端负载配置	28
	3.7.4	客户端动作配置	29
3.8)	服务端	48
	3.8.1	服务端子网配置	48
	3.8.2	服务端网络配置	49
	3.8.3	服务端 Profiles 配置	49
3.9	-	关联	61
	3.9.1	服务端和客户端关联	61
	3.9.2	添加测试订单	62

_			Dotouch XPRO 云测网络仿真测试工具 v2.0R3
3.	9.3	协议篡改规则配置	
3.10	测试	订单	
3.11	报表		70
3.	11.1	网口报表	
3.	11.2	测试用例报表	
3.	11.3	URL 统计报表	
3.	11.4	应用统计报表	71
3.	11.5	RTCP 报表	
3.	11.6	RTP 报表	
3.	11.7	RTP 详细报表	
3.	11.8	RTSP 报表	
3.	11.9	CUSP 报表	
3.	11.10	CUSP 用户接入报表	74
3.	11.11	用户接入报表	74
3.12	终端		75
箆4音	13 T	proughout 配置指南	76
بر 4 1	工程		76
4.1		设置	76
4.3	13 T	proughput	76
4.4	运行	noughput	
4.5	订单	列表	78
4.6	报表		80
4.7	终端		80
		·	
第5章	L2 re	play 配置指南	
5.1	工程		
5.2	図口	设置	
5.3	报び	〔捕获	
5.4	报文	资源管理	
5.5	回放		
5.6	运行		
5.7	测试	订单	
5.8	报表		
5.	8.1	网口报表	
5.	8.2	测试用例报表	
5.9	终端		
第6章	Atta	k 配置指南	
6.1	工程		86
6.2	系统	配置	86
6.3	接入	 配置	86
6.4	図口	一 <u>一</u> 配置	88
6.5	- 1	设置	88
6.6 6.6	入 里	☆ <u>↓</u>	۵۵ ۹۶
6.7	<i>沐</i> 仲 安 白	13 25 ·····	30
0.7	日ノ	۲IU •••••••	

			Dotouch XPRO 云测网络仿真测试工具 v2.0R3		
6.7.′	1	客户端子网配置			
6.7.2	2	客户端网络配置			
6.7.3	3	客户端负载配置			
6.7.4	4	客户端动作配置			
6.8	关联				
6.9	测试	订单			
6.10	报表				
6.11	包构	建器			
6.12	终端				
弗 / 早 ■ ·		,2544			
7.1	上程				
7.2	系统	配置			
7.3	接入	配置			
7.4	网口	配置			
7.5	变量	设置			
7.6	媒体	对象			
7.7	客户	端			
7.7.2	1	客户端子网配置			
7.7.2	2	客户端网络配置			
7.7.3	3	客户端负载配置			
7.7.4	4	客户端动作配置			
7.8	关联				
7.9	测试订单				
7.10	报表				

第1章前言

1.1文档介绍

本手册对北京触点互动信息技术有限公司的 XPRO 云测网络仿真测试工具系列产品的安装及配置方法进行说明。

1.2声明

本手册面向具备一定技术能力的软件开发工程师/测试工程师使用,使用人员至少具备基本的 Linux 系统操作能力 及基础的网络技术知识。

1.3文档约定

约定	描述
<u> </u>	注意事项.
条目	描述/全称
DUT	Device Under Test 被测设备
DPDK	Data Plane Development Kit 数据平面开发套件
Client	业务层面的客户端,如 HTTP Client, FTP Client
Server	业务层面的服务端,如Web Server,FTP Server
HTTP	Hyper Text Transfer Protocol 超文本传输协议
FTP	File Transfer Protocol 文件传输协议
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer 基于安全套接层的 HTTP
SSL	Secure Sockets Layer 安全套接层
TLS	Transport Layer Security 传输层安全
DNS	Domain Name System 域名系统
RTSP	Real Time Streaming Protocol 实时流传输协议
MODBUS	串行通信协议
NETCONF	网络配置协议
OPCUA	通信接口协议
L2TP	工业标准的 Internet 隧道协议
HANDLE	工控协议
SMTP	电子邮件传输协议

POP3	Post Office Protocol - Version 3 邮局协议
IPSEC	Internet Protocol Security 安全协议包
SIP	Session Initiation Protocol,会话初始协议
MQTT	Message Queuing Telemetry Transport 消息队列遥测传输
COAP	Constrained Application Protocol 受限应用协议

1.4技术支持

Email: support@dotouch.com.cn

第2章 基本概念

2.1关于 XPRO 云测网络仿真测试工具

XPRO 云测网络仿真测试工具(是一款面向 4~7 层网络协议仿真的专业测试仪表,用来仿真各类网络协议及应用、网络攻击的流量,同时具备高性能、高可扩展性的特点,目前业内同类型产品为 Spirent 的 Avanlanche 与 IXIA 的 BreakPoint System。

2.2测试场景与拓扑

2.2.1串接测试场景

串接测试作为测试过程中最常见的测试场景,一般用来测试如 DUT 的带业务转发性能、行为封堵、流量管理, 典型测试对象是网关/网桥模式部署下的防火墙、负载均衡、VPN、上网行为管理、流控管理等类型设备,典型测 试拓扑如下:



》试时客户端与服务端可位于同一台服务器之上,此时仪表相当于自环状态,也可分布在两台不同的服务器之上,如服务器 A 充当 HTTP 客户端,服务器 B 充当 Web 服务端,这样客户端和服务端可以独占各自服务器硬件的 CPU 资源与内存资源,提升性能。

2.2.2并接测试场景

并接测试作为测试过程中最常见的测试场景,通过分光器件、交换机/路由器镜像等将仪表产生的流量复制后送 至被测设备,一般用来测试如 DUT 的协议识别准确性,典型的测试对象是运营商 DPI 设备, APM/NPM 等无需进 行流量转发的设备,也可用来测试并接模式下的行为审计等类型设备。典型测试拓扑如下:



别试时客户端与服务端可位于同一台服务器之上,此时仪表相当于自环状态,也可分布在两台不同的服务
 器之上,如服务器 A 充当 HTTP 客户端,服务器 B 充当 Web 服务端,这样客户端和服务端可以独占各自服务器硬
 件的 CPU 资源与内存资源,提升性能。

2.2.3单臂测试场景

在串接测试与并接测试场景下,都是使用仪表来充当业务的 Client 端与 Server 端,但在单臂测试场景下,仪表一般仅充当 Client 端或者 Server 端,用来测试目标服务的功能与性能,如使用仪表充当 DNS 客户端,向客户自有的 DNS 服务器发起海量的 DNS 请求,测试 DNS 服务器的极限性能,因此单臂测试模式测试对象往往是业务系统,如 DNS 服务、Web 服务等等,典型测试拓扑如下:



🥼 单臂模式部署时,仪表既可充当客户端,也可充当服务端。

2.3客户端概念说明

在仪表仿真业务时,会仿真业务的客户端与服务端,如仿真 HTTP 业务时,会模拟海量 HTTP Get 向 Server 发起请 求,因此客户端与服务端是站在业务的角度来定义的。

Client 端作为业务请求的发起方,在测试时,根据所配置 Testcase 仿真所需业务流量,客户端的定义是应用的发 起端,如发起 HTTP 请求的 HTTP Client,发起 FTP 请求的 FTP Client,发起域名解析请求的 DNS Client。

在定义客户端时,需要定义客户端发起请求时的源/目 IP 范围,传输层端口(源端口范围/访问的目的端口范围),应用层的请求参数以及业务发起模型。

在配置客户端时有如下关键步骤:

- 定义客户端的子网范围,如仿真 10000 个用户向服务端发起业务请求,这 10000 个用户的源/目 IP 范围就是客 户端的子网,在配置时,对应的是"客户端"的"客户端子网"配置项,从协议栈的角度看,子网配置的是 客户端发起请求时的 IP 层信息。
- 定义客户端的在发起业务请求的传输层端口信息,如仿真 10000 个用户向服务端发起业务请求,这 10000 个用 户在发起业务请求时,传输层所使用的源端口及将要访问的目的端口,在配置时,对应的是"客户端"的 "客户端网络"配置项,从协议栈的角度看,客户端网络配置的是客户端发起请求时的传输层信息。
- 定义客户端的在发起业务请求的业务模型,包括定义新建速度,并发规模,新建与并发的优先级,以及流量的
 爬坡时间,稳定测试时间,下坡时间。
- 定义客户端的在发起业务请求的应用层信息,如仿真 10000 个用户向服务端发起业务请求,此处定义具体发起的业务类型,如发起的是 HTTP 业务还是 FTP 业务抑或是 DNS 业务,用户可自定义应用层的详细参数,如 HTTP 头部字段,Method 类型,POST 内容等等,在配置上对应的是"客户端动作"配置项,从协议栈的角度看,客户端动作配置的是客户端发起请求时的应用层信息。
- 仪表在进行仿真业务时,为了提高配置的灵活性,将 IP 层信息,传输层信息,应用层信息,业务模型解耦,

各个部分独立配置,以便用户通过自由组合生成不同的客户端配置,因此当完成客户端子网、客户端网络、 客户端负载、客户端动作配置后,还需完成最后一个步骤,将子网配置、网络配置、负载配置、动作配置进 行组合,最终生成一个完整的客户端配置。

2.4服务端概念说明

Server 端作为请求的响应端,在测试时,按照所配置规则响应客户端请求。 在定义服务端时,需要定义服务端提供服务的 IP 范围,提供服务的端口以及响应客户端请求时应用层参数。 在配置服务端时有如下关键步骤:

- 定义服务端的子网范围,如服务端仿真 1 个或多个 Web Server, Web Server 的 IP 范围就是服务端的子网,在 配置时,对应的是"服务端"的"服务端子网"配置项。从协议栈的角度看,子网配置的是服务端的 IP 层 信息。
- 定义服务端的的传输层端口信息,如服务端仿真 1 个或多个 Web Server, Web Server 提供 web 服务的四层端 口范围就是服务端的网络,在配置时,对应的是"服务端"的"服务端网络"配置项,从协议栈的角度看, 服务端网络配置的是服务端对外提供服务的四层端口,服务端将在此处所配置的端口上监听业务请求。
- 定义服务端的在响应业务请求时的应用层信息,如服务端响应客户端的 HTTP 请求,用户可自定义服务端响应时的应用层的详细参数,如 HTTP 响应码是 200 OK 还是 404 Not Found 等等,在配置上对应的是 "Profiles" 配置项,从协议栈的角度看,服务端 Profiles 配置的是服务响应请求时的应用层信息。
- 仪表在进行应用仿真时,为了提高配置的灵活性,将服务端 IP 层信息,传输层信息,应用层信息解耦,各个部分独立配置,以便用户通过自由组合生成不同的服务端配置,因此当完成服务端子网、服务端网络、服务端 Profiles 配置后,还需完成最后一个步骤,将子网配置、网络配置、业务配置进行组合,最终生成一个完整的服务端配置。

第3章 配置指南

3.1工程

工程作为测试任务最高的组织形式,定义了一个完整的测试任务。

xpro_ns	至	
工程	首页 / 工程	
系統配置		
接入协议 🗸 🔻	工程 example-test v 日	
网口设置	模式 双单错	
交量设置		
媒体对象		
客户端 🔻		
服务端 🔻	用户 dotouch@dotouch.com.cn / 機式 语选择 🔺	
关联		
测试订单	今入工程 単年 近近 近世	
报表 🔻	法得文件 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
终端		
	导出工程(请勿修改导出文件名,否则会导致导入工程先为) 立即使交	
	<u>Фалта</u>	
xpro_ns	至 ● example-test 授权剩余时间:14天12小时48分 时间编移:0.000	dotouch@dotouch.com.cn 🔻 🚦
xpro_ns 工程	正 ● example-test 授权剩余时间: 14天12小时48分 时间篇版: 0.000 首页 / 工程	dotouch@dotouch.com.cn 🔻 🚦
xpro_ns 工程 系统配置 v	王 ● example-test 授权利余时间:14天12小时48分 时间隔移:0000 首页 / 工程	dotouch@dotouch.com.cn ♥ 🕴
xpro_ns 工程 系统配置 ~ 接入协议 ~	正 example-test 授収到余时间: 14天12小时48分 时间偏移: 0 000 首页 / 工程	dotouch@dotouch.com.cn 👻 🚦
xpro_ns 工程 系统配置 ・ 接入协议 ・ 阿口设置	こ ● example-test 授权 教令前同: 14天12小时48分 町同業務: 0.000 首次 / 工程 ・ 工程 ・ ・ 工程 ・ ・ 構成 双母音 ・ ・	dotouch/gidotouch.com.cn 💌 🚦
Xpro_ns 工程 系統配置 並入助议 マ 阿口设置 支星设置	正 example-test 授权转命询问: 14天12小时48分 时间编辑8: 0.000 首页 / 工程 工程 ************************************	dolauch/gidalouch.com.cn 💌 👎
xpro_ns 工程 系統配置 ・ 接入协议 ・ 网口设置 ・ 支量设置 煤休对象	正 example-test 授权剩余时间: 14天12小时48分 时间编8: 0 000 首页 / 工程 工程 ************************************	dotouch@dotouch.com.cn ♥ 🕴
xpro_ns 工程 系統配置 ・ 接入协议 ・ 网口设置 ・ 突星设置 ・ 煤休功像 ・	正 example-test 提权联合时间: 14天12小0148分 目前電路8: 0.000 首次/工程 「工程 「工程 「工程 「工程名 ①	dotouch@dotouch.com.cn ♥ 🕴
Xpro_ns 工程 系統配置 後入协议 第 接入协议 第 支星设置 媒体対象 客户論 販売論	正 example-test 授权制分时间: 14天12小2148分 即回編8: 0.000 首次/工程 「工程 ************************************	dotouch@dotouch.com.cn ♥ 🕴
Xpro_ns 工程 系統配置 並入助议 学 遊入助议 マロジョ 変量设置 家体対象 富户端 美戦	Image: Completest 授权转分词目: 14天12小2148分 Explanae: Completest Comp	dotouch/gidotouch.com.cn.♥ 1
XPIO_IIS 工程 系統配置 東京公司 成入助収 マ 別口设置 支量设置 媒体対象 宮戸橋 堅労橋 実駅 剤応订単	Image: 1988 1989 1989 1989 1989 1989 1989 198	dotouch@dotouch.com.cn ♥ 🕴
XPIO_IS 工程 系統配置 ・ 接入协议 ・ 接入协议 ・ 闭口设置 ・ 支量设置 ・ 炭休对象 ・ 室門端 ・ 影洗論 ・ 炭防油 ・ 規志订单 ・ 报表 ・	Image: Completes 股权制分相同: 14天12/12148分 Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes Image: Completes <	dotouch@idotouch.com.cn ♥
XPIO_IS 工程 系統配置 後入协议 第 接入协议 プロ设置 支星设置 探体对象 客户職 影話訂单 搬表 火服 搬載	Image: 2 example:est BUSH-chill: 14,512/15/14/85/ BUSH-BERGE: 2000 Image: 128 Image: 2000 Image: 2000 Image: 1280 Image: 2000 Image: 2000	dotouch/ġłdotouch com cn ♥ 🕴
XPIO_IIS 工程 系統配置 協入助议 学 協入助议 受量设置 家体对法 富户端 学 服劣論 关联 期応订单 报表 终端	Image: Complete: 授权转分相: 4天12/bl482 Examplete: 1000000000000000000000000000000000000	dotouch/gidotouch.com.cn ♥

在工程菜单页,管理员可自行添加、删除及编辑测试工程。

- 点击图标 + , 新增工程, 根据业务需求选择对应的模式和类型
- 点击图标 / , 编辑指定工程
- 点击图标 💼 , 删除指定工程

AA 第一次使用时,必须在新建工程后方可配置其他功能模块。

点击图标 ④ 导出工程 可以将指定工程导出。支持同时导出多个工程。 导出的工程在资源管理器里,鼠标右键可以下载到本地。

类型

互联网

 \times





点击 导入工程下面的"选择文件"输入框,可以选择 已导出的工程,若需要导入的工程不在资源管理器中,可以点击资源管理器中的 上传 按钮,将工程出上传到资源管理器中,再点击 **•** 我钮,可以将选择的工程导入。



xpro_ns		<u> </u>	PPOE	授权剩余时间:	12天10小时5分	时间偏移: 0.000						
工程		首页 / 工程										
系统配置												
接入协议		工程	PPPOE		导入工程 (tar)							~
网口设置		+=										^
<u> 变量设置</u>		1#14	从平肖		✓ ☆ 我的文档					X 1		
媒体对象		类型	互联网		> desktop	名称	T 17	0B/不限制 类型	大小	修改时间		• • •
客户端		描述	PPPOEN	接防火墙测试	> dump	🕨 🔄 mci		文件夹		2021/01/26 16:0	9:05	
		用户	dotouch@	odotouch.com.cn	> ftp pcap-builder	testcase	2012 datauah Odatau	文件夹	500 GM	2021/05/11 15:2	9:14	
助汉尹立场而					tools	202108041443	4592_dotouch@dotou	tar 文件	522.0W	2021/08/04 14:4	4:59	
关联				_	✓ <mark></mark> ✓ 公共目录	TAR 202108111019	9142_dotouch@dotou	tar 文件	14.8M	2021/08/11 10:1	9:15	
测试订单		导入工程			> doc	TAR 202108161418	8042_dotouch@dotou	. tar 文件	14.8M	2021/08/16 14:1	8:05	
报表		选择文件		▲台	nsvi-2.0.0-SVN_100	202108171028	8022_dotouch@dotou	tar 文件	14.8M	2021/08/17 10:2	8:02	
终端					share	TAR 202100101033	2132_001000011@001000		14.00	2021/00/13 13:3	2.15	
		导出工程 (请勿修改	如导出文件名	3, 否则会导致导入工	> system							
					virus							
		(1) 守田上柱				8个项目						
											備定	取消
	首页 /	工程										
系統配置 ▼				导入工程 (.tar)				×				
接入协议 ▼		工程 PPPOE		 收藏夹 	< > 🖾 📑 public de		* *	Q				
网口设置		模式 双单嵴		> desktop	■ 新建文件英 ▼ 1 上传 ▼ 名称	0B/不限制	89	×				
		美型 互联网		> dump	mci	本地上传离	线下载					
☆户端 ▼		描述 PPPOE对接防火场	意测试	pcap-builder	202108041443012_dotouch@c	otou 选择文件 -	打开					>
		用户 dotouch@dotouch	n.com.cn	· 100/s ~ 100 公共目录	202108051354592_dotouch@d 202108111019142_dotouch@d 202108111019142_dotouch@d	otou	← → ✓ ↑ → 此 组织 ▼ 新建文件夹	电脑 〉 Desktop 〉 主程序	>	~ Ö	搜索"主程序"	م ۱۱۱۱ • ۱۱۱
				custom-cve	202108161418042_dotouch@c	lotou	↓下載 ★ ^	名称	^	(92	女日期	类型
	导入	工程		nsvi-2.0.0-SVN_1	202108171028022_dotouch@c	lotou	handle-tcp-\$1	中间件 202105170102182_dd	otouch@dotouch	202 .com.cn_rfc254 202	1/8/17 9:50	文件夹 WinRAR 压缩文 WinPAR 压缩文
	送	释文件	▲导入	> share			工作	xpro-ns-1565-3.0.1-h	ikey-gm ikey-gmta	202 202 202	21/6/8 0:00	1-HKEY-GM 文 1-HKEY-GMTA
				> upload			OneDrive	xpro-ns-1577-2.9.6	-	202 202	21/6/8 14:37 21/6/10 18:30	6 文件 6 文件
	导出	工程 (请勿修改导出文件名,否则)	会导致导入工		8个项目		WPS网盘 UPB脑	xpro-ns-1738-3.0.1-h	ikey	202	1/6/30 17:56 1/7/19 8:21	1-HKEY 文件 7 文件
) 导出工程					3D 对象 Desktop	xpro-ns-18/0-3.0.1-h	ikey	202 202 202	1/7/26 10:59 21/7/27 14:27	1-HKEY 文件 1-HKEY 文件 1 文件
							→ 測试共享文件 (C ■ +0145 V	xpro-ns-1964-3.0.1		202	1/8/5 16:21	1 文件
							文件名	S(N): 202105170102182_dc	otouch@dotouch.	com.cn_rfc2544_c ~	所有文件 (*.*)	~
											引ガ(O)	取消

工程导入仅支持相同版本,或是高版本导入低版本导出的工程。低版本导入高版本导出的工程会出现导入 失败的情况。

3.2系统配置

系统配置中的参数对所有的工程都生效

3.2.1开放平台

开放平台中可以配置第三方的 url 接口,系统可以在测试时向指定的 url 推送测试输出的数据

xpro_ns	三 🔮 example-test 授权剩余时间:14天12小时44分 时间编移:0.000	dotouch@dotouch.com.cn 👻 🕴
工程	首页 / 开放平台	
系統配置		
开放平台	居用数据推进 🔵 启用 💿 关闭	
用户管理	URL(限务器地比) https://192.168.2.142/api/order/notify	
外部攻击库		
L3回放车管理	立即建立	
病毒库管理		
して四放车管理		
按入协议 ▼	*	
网口沿署		
本母沿署		
<u>这里说出</u>		
太白柴 -		
127 Jan .		
1802251845 ▼		
天联		
测试订单		
报表 ▼	*	
终端		

此功能默认为关闭,根据需要进行配置。

3.2.2用户管理

用户管理页面可以给系统添加新用户,并且对用户账户进行编辑管理。

xpro_ns	三 @ example-test 授权剩余时间: 14天12小时			dotouch@dotouch.com.cn 🔻 🗄
工程	首页 / 用户管理			
系統配置				
开放平台	Name: Ema	il: Q		
用户管理				
外部攻击库	添加			
L3回放车管理	57 (P)	西寻如故	色话	58.4%
病毒库管理	michela	michela@qmail.com	普通用户	Seal -
L7回放库管理	admin	admin@dotouch.com.cn	管理员(可通过api修改普通用户密码)	Setting Token
系统信息	< 1 > 到第 1 页 确定 共2条 10条页 >			
接入协议 🗸 👻				
网口设置				
变量设置				
媒体对象				
客户端 🔻				
服务端 🔫				
关联				
测试订单				
报表 ▼				
终端				
				27 0 + 32.5
		版权所有:北京触点互动信息技	术有限公司 京ICP备19037780号	订単未运行
点击页面上	的 添加 按钮,打开新增用	用户的编辑页面		

	Ξ ● example-test 授权剩余时间:14天12小时36		
工程	首页 / 用户管理		
系统配置			
开放平台	Name: Email:	Q	
用户管理			4
外部攻击库	添加	add-user X	4
L3回放库管理		*名称	1
病毒库管理	名校	*Email	ł
L7回放库管理	michela		
系统信息		* 25.99	0
接入协议		立即提交	
网口设置			
变量设置			I
媒体对象			I
客户端			
关联			_

名称:自定义的账户名称

Email:新增的账户登录用的邮箱,无需校验

密码:账户的登录密码

提交保存后就可以使用新的账户登录系统了。页面上同时还可以编辑和删除已有账户。

🔪 dotouch@dotouch.com.cn 是默认系统账户,不在"用户管理"页面展示,可在右上角 账号位置 修改密码

3.2.3 外部攻击库

本页面可以导入用于网络安全的测试的攻击库文件,攻击库文件由我司制作更新。

xpro_ns	프 🛭 example-test 授	权剩余时间: 14天6小时49分	时间编移: 0.000			c	lotouch@dotouch.com.cn ▼ :
工程	首页 / 外部攻击库						*
系統配置							
开放平台	ID	文件名	文件大小字节	版本	备注	上传时间	授作
用户管理	1	nsat-1.0.0-3925.tar.bz2	294663	1.0.0		2021-07-02 15:17:59	升级 回滾 清空
外部攻击库							
L3回放库管理							
病毒库管理							
L7回放库管理							
系统信息							
接入协议 🗸 👻							
网口设置							
变量设置							

上传后可在 Attack 子系统中模拟网络攻击行为的测试中调用上传的攻击库文件,同时页面还有回滚和清空的功能。

3.2.4 L3 回放库管理

点击 添加 按钮打开添加页面

xpro_ns		example-test 授权剩余时间:14天							
工程	首页 / L3[且放库管理							
系統配置									
开放平台	添加								
用户管理	ID	文件名	文件大					上传时间	操作
外部攻击库	74	601f62aee4b89-1-clean.pcap	5640	漆加又件			×	021-02-07 11:47:35	「「「「」」」 「「」」 「「」」 「「」」 「」」 「」」 「」」 「」」
L3回放库管理	76	603f062ca8f70-11282-4-clean.pcap	864	上传文件	▲ 选择文件			021-03-03 11:45:56	下乾編組 調除
病毒库管理	79	6045d718d9c42-11277-4-clean.pcap	864	源IP段				:021-03-08 15:50:11	11日
L7回放库管理	80	6045d913bb5cb-11277-4-clean.pcap	864	目的旧段				021-03-08 15:58:24	下我 编辑 删除
系统信息	81	6045dd304ae4b-port0-dump-clean.pcap	61344					021-03-08 16:15:57	金融 銀澤
接入协议 🗸 🔻	82	6045e8da188f5-11277-4-clean.pcap	864	音注:				:021-03-08 17:06:29	下乾編組 調除
网口设置	97	607eabcec5d7f-mysql3-clean.pcapng	53788					021-04-20 18:28:45	1983年1983年1983年1983年1983年1983年1983年1983年
变量设置	102	607f8bfb0710b-mysql-1-clean.pcap	53788			li		021-04-21 10:20:50	· · · · · · · · · · · · · · · · · · ·
媒体对象	103	609de65d31786-CNVD-2021-09650-clean.pcap	5124		立即提交			:021-05-14 10:54:51	下我 编辑 删除
案戸端 ▼									
服务端 🔻									
关联									

上传 pcap 文件后,可以输入源 ip 和目的 ip 地址段,然后提交。系统会按照填写的地址段范围过滤上传的 pcap 包中的报文,然后生成新的 pcap 文件并保存。支持上传多个文件,也可以将文件下载到本地,或者编辑、删除 已有文件。

3.2.5 病毒库管理

本页面可以导入用于网络安全的测试的病毒库文件,病毒库文件由我司制作更新。

xpro_ns	☲ ⊕ example-test 🚦						dotouch@dotouch.com.cn 👻 🗄
工程	首页 / 病毒库管理						•
系統配置							_
开放平台	ID	文件名	文件大小字节	版本	告注	上传时间	操作
用户管理	2	nsvi-1.0.0-SVN_10.tar.bz2	95869	1.0.0		2021-06-23 14:42:01	升级 回滾 清空
外部攻击库							
L3回放库管理							
病毒库管理							
L7回放库管理							
系统信息							
接入协议 🔫							
网口设置							
变量设置							
媒体对象							

上传后可在 Attack 子系统中模拟网络病毒攻击行为的测试中调用上传的攻击库文件,同时页面还有回滚和清空的功能。

3.2.6 L7 回放库管理

此页面可以导入本地的 pcap 报文,目前只支持单条流的 pcap 文件上传,上传的 pcap 文件在 replay 协议中以回 放文件-选择 L7 回放样包进行引用

xpro_ns	Ξ	 example-test 授权剩余时间: 14分 	天6小时21分 时间偏移: 0.000				dotouch@dotouch.com.cn 👻 🗄 :
工程	首页 / し	7回放库管理					
系統配置							
开放平台	10.1s	È					
用户管理		名称	pcap文件	carray文件	协议	上传时间	操作
外部攻击库		1111	601f63832045e_pcap_1.pcap	601f63832045e_pcap_1.carray	tcp	2021-02-07 11:50:30	下载 翻除
L3回放库管理		https	606ff0929850c_pcap_1.pcap	606ff0929850c_pcap_1.carray	tcp	2021-04-09 14:13:45	下载 删除
病毒库管理		http	606ff57010b72_pcap_1.pcap	606ff57010b72_pcap_1.carray	tcp	2021-04-09 14:34:28	下载 删除
L7回放库管理		smtp	606ffbe5598ec_pcap_1.pcap	606ffbe5598ec_pcap_1.carray	tcp	2021-04-09 15:02:02	下载 翻除
系统信息		udp_dns	6073b3bea72db_pcap_1.pcap	6073b3bea72db_pcap_1.carray	udp	2021-04-12 10:43:17	下载 翻除
接入协议 🗸 👻		smtp	609e2f1e1224b_pcap_1.pcap	609e2f1e1224b_pcap_1.carray	tcp	2021-05-14 16:04:52	下载 翻除
网口设置		http	609e40ca14c46_pcap_1.pcap	609e40ca14c46_pcap_1.carray	tcp	2021-05-14 17:20:34	下载 翻除
变量设置		udp_dns	60a5c29786fd0_pcap_1.pcap	60a5c29786fd0_pcap_1.carray	udp	2021-05-20 10:00:04	下载 翻除
媒体对象		smtp	60d99e944cb0f_pcap_1.pcap	60d99e944cb0f_pcap_1.carray	tcp	2021-06-28 18:04:12	下载 翻除
客户端 ▼	<	1 > 到第 1 页 确定 共9条 10条	/页 ✔				

点击 上橋中本 按钮,进入上传 pcap 文件页面,对已经上传的 pcap 文件支持下载到本地或者删除操作。

		example-test 授权剩余时间:14;						
	首页 / L	.7回放库管理						
系统配置								
	the state	* Ettepcap						
用户管理		名称	pcap文件		carray文件	协议	上传时间	操作
		1111	601f63832045e c	DCAD 1.DCAD	601f63832045e pcap 1.carrav	tco	2021-02-07 11:50:30	下载 副除
L3回放库管理		https	606ff0929t	ар		×	2021-04-09 14:13:45	下载 翻除
病毒库管理		http	606ff57010	pcap文件 合选择文件			2021-04-09 14:34:28	下载 删除
L7回放库管理		smtp	606ffbe55	名称			2021-04-09 15:02:02	下载 删除
系统信息		udp_dns	6073b3bea				2021-04-12 10:43:17	下载 删除
		smtp	609e2f1e1	立即提交			2021-05-14 16:04:52	下载 删除
		http	609e40ca1				2021-05-14 17:20:34	下载 删除
		udp_dns	60a5c2978				2021-05-20 10:00:04	下载 删除
		smtp	60d99e944				2021-06-28 18:04:12	「「「「」」を見ていた。
	<	1 > 到第 1 页 确定 共9条 10条	/页 ~					
服存端 🔻						_		

3.2.7 系统信息

此页面可以查看系统的内存和存储空间的使用情况等信息,还有 测试硬盘写入速率,清理抓包文件等功能。

点击 按钮规述 按钮, 仪表会自动测试硬盘写入速率, 测试完成后会在页面展示。

点击 游理师包文件 按钮, 会清理 /var/www/KODExplorer/data/User/demo/home/dump/ 目录下所有抓包文件。

	三					dotouch@dotouch.co
工程	首页 / 系统信息					
系統配置						
开放平台	◇ 系统负载和内存					
用户管理	1分钟: 0.46			急内存: 15886M 副全, 4791M		
外部攻击库	15分钟: 0.46		5	使用率: 69.90%		
L3回放库管理	✓ 磁盘管理					
病毒库管理						
L7回放库管理	磁盘测速 清理抓包文件					
系统信息	文件系统	总大小	已使用	剩余	已使用占比%	挂截占
接入协议 🗸 👻	/dev/mapper/centos-root	26G	21G	5.3G	80%	1
网口设置	/dev/sda1	1014M	179M	836M	18%	/boot
	devtmpfs	4.8G	0	4.8G	0%	/dev
变量设置	tmpfs	1.6G	0	1.6G	0%	/run/user/0
媒体对象	tmpfs	7.8G	0	7.8G	0%	/sys/fs/cgroup
	tmpfs	7.8G	348K	7.8G	1%	/dev/shm
客户端 マ	tmpfs	7.8G	34M	7.8G	1%	/run

3.3 接入配置

3.3.1 PPPoE

PPPoE 页面用来添加 PPPoE 请求的客户端配置,配置后可以自动生成一个关联项。IP 协议版本支持 ipv4、 ipv6、ipv4&ipv6,用户文件用来配置生成用户端 mac 地址,vlan 等。

xpro_ns) ex	ample-test										touch@dotouch	i.com.cn 🔻 🗄
工程	首页 /	PPP0E												
系統配置 🔻														
接入协议		⊕ 添加												
PPPoE		名称	IP协议版本	客户端网卡	文件	心跳时间	延时下线时间	重试次数	用户上线速率	活跃用户数	用户活跃时长	最大连接数	稳定时间	操作
DHCP								无数据						
网口设置														
交量设置														
媒体对象														
客户端 ▼														
服务端 🔻														
关联														
测试订单														
报表 🔻														
终端														

点 击 🕀 添加 按钮,进入到配置界面

<mark>*</mark> 名称	pppoe	e-ipv4		
IP协议版本	ipv4			
客户端网卡	port0	v		
*用户文件	ic/hon	ne/resource/pppoe-ipv4_file	用户文件模糊	版下载 选择用户文件 生成用户文件
*心跳时间	0		秒	
*延时下线时间	0		秒	
*重试次数	3			
支持认证方式	PAP, C	HAP-MD5		
—— 用户上线衫	行为			
*用户在线8	时长	720000000		us
*最大拨号	号数	1000		
使用应用负	负载	OFF		不带承载时不能使用应用负载
上线证	東率	10		users/sec
活跃用F	⊃数	1000		
测试的	讨长	15		わ
拖尾田	时间	20		秒

名称: 填写客户端名称

客户端网卡:选择测试 PPPoE 协议的网卡

用户文件:为了避免每个 PPPoE 请求包的参数都相同,自定义 PPPoE 请求报文的变量。这里支持上传模板和自动 生成。

可定义的变量包括: mac、PPPOE 拨号的用户名和密码、外层 vlan 和内层 vlan

心跳时间: PPPoE 心跳间隔

延时下线时间: PPPoE 用户在线时间结束后, 延迟下线的时间

重试次数: PPPoE 拨号失败时重试的测试

支持认证方式:支持 pap 和 CHAP-MD5 两种方式

PPPoE 客户端新建完成后,关联项自动生成,无需手动添加

点 击 生成用户文件 可以生成用户文件

Ĵ.				
*文件名:	pppoe_file			
*MAC:	08:00:{\$mac_var}	i		
MAC变量:	{\$mac_var} 范围: 1	- 1 # 1	£ 1	
*用户:	dotouch{\$user_var}	(i)		
用户变量:	{\$user_var} 范围: 1	- 1 步 ;	£ 1	
*密码:	dotouch{\$pwd_var}	i		
密码变量:	{\$pwd_var} 范围: 1	- 1 步 1	€ 1	
VLAN1(外层):		G		
VLAN1变量:	{\$vlan1_var} 范围:	- #t	÷	
VLAN2(内层):		i		
VLAN2变量:	{\$vlan2_var} 范围:	- #t	÷.	
	立即提交			

配置后自动生成的关联项

xpro_ns	⊡ ⊜	example-test	受权剩余时间:	14天5小时47分	时间偏移:	0.000							dot	ouch@dotouch	.com.cn 🔻 🕴
工程	首页 / PPPoE														
系統配置 ▼															
接入协议 🔺	① 添加														
PPPoE	名称	IP协议版本	客户端网卡	文件	心趣时间	延时下线时间	重试	欠数	用户上线速率	活跃	用户数	用户活跃时长	最大连接数	稳定时间	操作
	pppoe	ipv4	null	/var/www/	0	0	3		100	1	000	720000000	4000000	100	編輯 删除
网口设置	4										_				•
	< 1	> 到第 1 页	确定 共1条	20 翁/贞 🗸											
	⊡ © e	xample-test 🛛 👸											dotoud	ch@dotouch.co	m.cn 🔻 🕴
工程	首页 / 关联														
系統配置 ▼															
接入协议 🗸 👻	添加测试订单														
國口沿雲	客户端关联	服务端关联													
交量设置	名称:	٩, ٢	ਵ												
媒体对象			+	"名称	关联类	₫	4子网类型	子网	协议类型	动作	网络	开启全局负载	*负载	•权重	
客户端 🗸		1	1	pppoe	接入网	[pppoe-ipv4]									^
10 g w _	0		/ 🗑 📚	SIP-UDP	用户面		IPv4	client	标准协议	SIP-UDP	sip		负载	100	
BR:255474 🗸 👻			1 🗊 📚	SIP-TCP	用户面		IPv4	client	标准协议	SIP-TCP	sip		负载	100	
关联	0		/ 🗑 📚	HANDLE	UDP 用户面		IPv4	client	标准协议	HANDLE-UDP	handle		负载	100	
测试订单			1 🖉 📚	pop3	用户面		IPv4	client	标准协议	pop3	pop3		负载	100	
10-			/ 🗑 📚	smtp	用户面		IPv4	client	标准协议	smtp	smtp		负载	100	
			/ 🛯 📚	ftp	用户面		IPv4	client	标准协议	ftp	ftp		负载	100	
29%-34%			/ 🔟 📚	RAW-TLS	_v6 用户面		IPv6	client_v6	标准协议	RAW-TLS	RAW-TLS		负载	100	

3.3.2 DHCP

DHCP 页面用来添加 DHCP 请求的客户端配置。IP 协议版本支持 ipv4、ipv6、ipv4&ipv6,用户文件用来配置生成用 户端 mac 地址, VLAN 等。

xpro_ns	프 🖶 DI	HCP 授权剩	涂时间:14天5小时	34分	时间偏移: 0.000						d	otouch@dotou	ich.com.cn 👻 🕴
工程	首页 / DHCP												
系统配置													
接入协议	⊕ 添加												
PPPoE	名称	IP协议版本	DHCPv6仿真模式	客户端网卡	文件	延时下线时间	重试次数	用户上线速率	活跃用户数	用户活跃时长	最大连接数	稳定时间	操作
DHCP	DHCP-lpv	lpv4&v6	DHCPv6&PD	port0	/var/www/KO	0	3	1	1000	720000000	4000000	100	編輯 副除
网口设置	DHCP-ipv	ipv4&v6	DHCPv6 PD	port0	/var/www/KO	0	3	1	1000	720000000	4000000	100	编辑 删除
变量设置	DHCP-ipv	ipv4&v6	DHCPv6	port0	/var/www/KO	0	3	1	1000	2000000	4000000	10	編輯 劃除
媒体对象	DHCP_ipv	ipv6	DHCPv6&PD	port0	/var/www/KO	0	3	10	1000	720000000	4000000	12	编辑 删除
客户端 ▼	DHCP-lpv	ipv6	DHCPv6 PD	port0	/var/www/KO	0	3	1	1000	720000000	40000000	12	编辑 删除
昭 久244 —	DHCP-ipv6	ipv6	DHCPv6	port0	/var/www/KO	0	3	1	1000	2000000	4000000	20	编辑制除
	DHCP-ipv4	ipv4		port0	/var/www/KO	0	3	1	1000	720000000	40000000	10	编辑 劃除
关联		2000 1 77	18cm # 7.62 20.68	an e									•
测试订单		3386 I 94	開進 六/京 20第	734 ¥									

点击 🕀 🚵 按钮,进入到配置界面

DHCP *名称 IP协议版本 ipv4 请选择 客户端网卡 Ŧ 选择用户文件 请输入文件路径 *用户文件 延时下线时间 0 秒 3 重试次数 用户上线行为 7200000000 *用户在线时长 us 40000000 *最大拨号数 使用应用负载 不带承载时不能使用应用负载 立即提交 重置

使用应用负载	OFF	不带承载时不能使用应用负载	Dotouch XPRO 云测网络仿真测试工具 v2.0R3
上线速率	100	users/sec	
活跃用户数	1000		
测试时长	100	秒	
拖尾时间	0	秒	

点击 生成用户文件 可以生成用户文件

MAC受量: {smac_var} 注目: · · 步长: · VLAN1: () () · 步长: · VLAN1变量: {\$vlan1_var} 范围: · 步长: · VLAN2: () · · 步长: · VLAN2: · · 步长: · · vLAN2变量: {\$vlan2_var} 范围: · 步长: option: 请选择 · 步长:	
MAC受量: {smac_var} :E国: 「 - 「	
MAC受量: {\$mac_var} ?:2回: 「 - 「	
MAC变量: {smac_var} 完固: 「 - 「	
MAC变量: {smac_var} 完固: 「 」 」 步长: 「 VLAN1: ① LAN1变量: {Svlan1_var} 范围: 」 步长: □	
MAC变量: {\$mac_var} 完固: 「 - 「	
MAC受重: {smac_var} 没国: 「 - 「	
MAC变量. {\$mac_var} 完电. · · · · · · · · · · · · · · · · · · ·	
MAC受重. {smac_var} ?Ell: ' - '	
* MAC: 08:00:{smac_var} (i)	
*文件名: dhcp_file	

网口设置 3.4

网口设置用来配置设备测试端口的 IP 信息 (不含管理口), 网卡列表显示的网卡信息由系统自动从设备上读取, 无需配置。

将鼠标移动到页面上的网卡 与标志处,可以查看网卡信息

xpro_ns		DHCP					
工程	首页/网	1+					
系統配置 ▼							
接入协议 👻	网卡列录						
网口设置		Ę	La construction de la constructi				
变量设置		port0	port1				
媒体对象							
客户端 ▼	+	8					99
服务端 ▼		网口名		IP	前缀长度	网关	攝作
关联		port0		acbd::1	120	acbd::2	编辑 删除
测试订单		port0		10.4.0.2	24	10.4.0.1	蝙嶽 删除
报表 ▼		port1		bbae::1	120	bbae::2	编辑图绘
终端		port1		11.4.0.2	24	11.4.0.1	編織 翻除

点击网卡标志, 一 可以编辑网卡的配置参数

xpro_ns	E	DHCP	授权剩余时间: 13天14小时间	6分	时间偏移:	0.000				dotouch@dotouch.com.cn 👻 🚦
工程	首页 /	网卡								
系統配置	•									
接入协议	- P##9				edit-port0			×		
网口设置		L L			* mtu	1500				
变量设置		port0	port1		混杂模式	OFF				
媒体对象					組播機式		关闭组播機式,IPv6将无法通信			
客户端	- +	Ŧ			17 L.					88
服务端	-	网口名		IP	31782	ON			网关	攝作
关联		port0		acbd::1	抓包数量	1000	\uparrow		acbd::2	編編 題除
测试订单		port0		10.4.0.2	vlan id	0	1-4094		10.4.0.1	· · · · · · · · · · · · · · · · · · ·
10.000		port1		bbae::1		<u>.</u>			obae::2	編載 影除
版表		port1		11.4.0.2	vlan优先级	U	0-7, ERIAO		11.4.0.1	9965 BBB
终端					ping诊断	OFF				
					ping目的地址					
						立則	<u>重要</u>			

MTU: 配置端口的 mtu 值, 默认为 1500

混杂模式:开启或者关闭网口的混杂模式

组播模式:开启或者关闭网口的组播功能,需要注意测试 ipv6 时必须开启此开关

抓包:开启端口抓包的功能,开启后测试运行时端口会自动抓包并保存抓包文件到资源管理器

抓包数量:开启抓包后,配置端口抓包的最大数量

vlan id: 配置端口带 vlan id

vlan 优先级:端口带 vlan 时,配置优先级

ping 诊断:开启或者关闭网口的 ping 诊断功能

ping 目的地址:开启抓包后,配置 ping 诊断的地址

网口设置页面可以配置网口的 IP 参数

xpro_ns		DHCP 授权剩余时间: 13天14小时				
工程	首页 / 网	ŀŧ				
系统配置		-				
接入协议 🔫	网卡列3					
网口设置						
变量设置		port0 port1				
媒体对象						
畜户端 ▼	+	8				99
服务端 🔻		网口名	IP	前缀长度	网关	操作
关联		port0	acbd::1	120	acbd::2	编辑 翻除
		port0	10.4.0.2	24	10.4.0.1	編編 删除
则试订单		port1	bbae::1	120	bbae::2	编辑 翻绘
报表 マ		port1	11.4.0.2	24	11.4.0.1	编辑 删除
مادية وا لم						

点击 土 按钮配置打开添加网口 IP 参数的配置页

xpro_ns					dotouch@dotouch.com.cn 👻 🚦
工程	首页 / 网 卡				
系統配置					
接入协议 🔫					
网口设置					
变量设置	port0 port1				
媒体对象		add-port	×		
客户端 ▼	+ 🗑	*网口名	通防坪 マ		88
服务端 🔫	- MD25	IP *IP		网关	操作
关联	port0	acbd::1 *前缀长度		acbd::2	
测试订单	port0	10.4.0.2		10.4.0.1	
报表 🔻		11 4 0 2		11.4.0.1	
终端	P erri		立即提交		

网口名:选择所用到的网口

IP 地址:配置该网口的接口 IP(<mark>可按照上图自定义,port0 的 IP 作为 port1 的网关,反过来 port0 的网关作为</mark> port1 的 ip)

前缀长度: 配置该网口 IP 地址的前缀

网关: 配置该网口的下一跳 IP 地址

MAC 地址为程序自动获取填入,无需手动配置

▲ 当前版本不支持通过界面修改管理口 IP,需自行在 linux 后台修改管理口 IP,完成管理口 IP 修改后,请勿使用 service network restart 命令重启网络服务,请使用 ifdown 和 ifup 命令重启管理网口。如果要打 ipv6 的流量,需要配上 ipv6 的地址,同时打入 ipv4 与 ipv6 的流量,需要在网卡同时配置上 ipv4 与 ipv6 的地址。

3.5变量设置

该功能模块用来定义变量,用来在仿真 HTTP、https、dns 时调用,按照变量规则生成海量的 HOST 与 URI,避免 仿真 HTTP 业务时所仿真的 HTTP 请求的 HOST 与 URI 均相同的情况。

xpro_ns	⊡ @ DHCP	授权剩余时间: 13天13小时57分	时间偏移: 0.000				dotouch@dotouch.com.cn ▼ :
工程	首页 / 変量设置						
系統配置 ▼							
接入协议 🗸 🔻	④ 添加						
网口设置							
变重设置	交量名	变量类型	区间范围下限	区间范围上限	步长	顺序	操作
媒体对象				无数编			
客户端 ▼							
服务端							
关联							
测试订单							
报表 ▼							
终端							

点击 🕀 🚈 按钮,进入添加变量页面

xpro_ns						
工程	首页 / 变量设置					
系統配置						
接入协议 🗸	 ① 添加 					
网口设置						
变重设置	交量名 3	安星类型 add-variable		~	顺序	操作
媒体对象		* <u>变量名</u>		- 1		
客户端 🔻		* 安曇英型	请选择	v		
服务端 🔻		*区间范围	min max	- 1		
关联		* 步长		- 1		
测试订单		10.00	· 御所招	-		
报表 🔻		100	HACT.	-		
终端			立即提交	- 1		
				- 1		
				- 1		
				_		

变量名:该变量的名称

变量类型:当前仅支持 init 型变量

区间范围: 变量值的区间范围, 如 200~65000

步长: 变量的变化规则, 如当步长为1时, 每调用一次变量则加1或减1

顺序:当前支持递增、递减与随机三种模式,其中当顺序为随机模式时,将不按设定步长变化(目前只支持递增 模式)

3.6媒体对象

媒体对象可以自定义一个虚拟的视频数据流。在 RTSP 协议测试中, 服务端可以选择引用这里添加的媒体对象, 测试时就可以按照定义的格式向终端发送 RTP 数据流。

	首页	/ 媒体对象						Í
系統配置 ▼								
接入协议 🗸 👻		→ 添加 →						
网口设置								
变量设置	序	号 名称	媒体采样率(Hz)	攝放較频	攝放码率(Kbps)	攝放时长(秒)	RTP載荷大小	攝作
10/10140	1	media	90000	25	N/A	N/A	8	編輯 图除
XKUTAJAK	2	media	90000	25	N/A	N/A	8	編織 删除
客户端 🔻								
服务端 🔻								
关联								
测试订单								
报表 🔻								
终端								

点击 🕀 🐄 按钮,填写视频流的各项参数

工程	首页	/ 媒	体对象							
系统配置										
接入协议		⊕ %	泰加							
网口设置								-		
变量设置	居	号	名称	媒体采样素	add-media			×	RTP载荷大小	操作
		1	media	90000	*名称			- 1	8	制除
深体对象		2	media	90000				- 1	8	高级 删除
客户端 🔻					*媒体采样率 (Hz)	90000	每秒对媒体对象的采样次数,单位 Hz	- 1		
売 お ままま しょう								- 1		
					* 播放帧频	25	每秒播放媒体对象数据帧的个数	- 1		
关联								- 1		
测试订单					(Kbps)	N/A	带它描放而深体又特的它特级重,单位 Kops	- 1		
17 = _								- 1		
100.00					★播放时长(秒)	N/A	媒体文件播放时间	- 1		
终端					*RTP载荷大小	8	服务债发送媒体视频的 payload 大小,单位字节(范围:8~1460)	- 1		
						立即提交				
								- 1		

名称: 自定义媒体流的名称

媒体采样率:视频媒体数据的采样率,表示每秒对媒体对象的采样次数,单位是 Hz **播放帧率**:视频数据的帧速率,表示每秒播放媒体对象数据帧的个数 **播放码率**:视频播放的码率,表示每秒播放流媒体文件的比特数量 **播放时长**:表示媒体播放文件的长度,单位是秒 RTP 载荷大小: 配置发送的 RTP 报文中所带载荷的大小

3.7客户端

3.7.1客户端子网配置

子网配置项用来配置 Client 端发起请求时的源 IP 地址范围,支持 IPv4 与 IPv6 ,选择 ipv4,添加 ipv4 地址,选择 ipv6,添加 ipv6 的地址。

xpro_ns		example	le-test												dotouch@	lotouch.com.cn 🔻	
工程	首页 / 春月	户端 / 子网															
<u>系統配置</u> ▼	IPv4	4 IP	v6														
接入协议 🔻	批量复制	9															
网口设置)	+ *	称	客户端网卡	接入类型	接入名称	IP源地址起始	IP源地址结束	IP目的地址起始	IP目的地址结束	DNS服务器IP	ARP学习	启用VLAN	Enable IPSec	Remote Access	Gatew
变量设置)	¢ 📋 🤉 cl	lient				1.1.1.2	1.1.1.20	20.20.1.1	20.20.1.2						
媒体对象																	
客户端 ▲																	
子网																	
网络																	
负载																	
动作																	
服务端 🔻																	
关联																	
测试订单																	

名称: 该 IP 子网的名称

接入类型: 该 IP 子网的接入类型, 例子中是仿真 http 协议, 可不选择

接入名称: 该 IP 子网的接入名称, 例子中是仿真 http 协议, 可不选择

客户端网卡:选择作为客户端的网卡

IP 源地址开始/IP 源地址结束: 用来配置该仿真时客户端子网的起始 IP 与结束 IP。

IP 目的地址开始/IP 目的地址结束:用来配置该仿真时服务端子网的起始 IP 与结束 IP

DNS 服务器 IP:当需要解析域名信息时,需指定 DNS 解析服务器的 IP 地址。

ARP **学习:**当被测设备工作在二层,如网桥模式、透明模式等,此时仪表客户端与服务端处于同一个网段,在该场景下需开启该功能,此时客户端会直接向服务端 IP 发起 arp 请求后将数据包直接发送给服务端,而不是将数据 包交由下一跳网关转发,开启该功能后,设备工作在 L2 模式。

工程	首页 / 著	客户端 / 子	(Ø)														
系統配置	IF	Pv4	IPv6														
接入协议 🗸 🗸	批量复	記事															
网口设置			+	名称	客户端网卡	接入类型	接入名称	IP源地址起始	IP源地址结束	IP目的地址起始	IP目的地址结束	DNS服务器IP	ARP学习	启用VLAN	Enable IPSec	Remote Access	Gatew
变量设置			√ ×	client	~	`	-	1.1.1.2	1.1.1.20	20.20.1.1	20.20.1.2						IPv4
媒体对象	1	/LAN	IPSec	IPSecIKEv2 GREVPN	I 自定义U	DPVPN											
客户端 🔺	VLA		优先级														
子网		U 启用IP	22														
网络	IP:		掩码:	网关:													
负载																	
动作																	
服务端																	
关联																	

启用 VLAN: 当该子网需要启用 VLAN 时需勾选该功能(并配置下方 VLAN 相关信息)

VLAN ID: 该子网所在的 VLAN

优先级: 配置该 VLAN 的 Priority

启用 IP 配置: 配置该 Client 子网所在 VLAN 的 VLAN 子网 IP 地址

Enable IPSec: 当该子网需要启用 IPsec 是需勾选该功能 (勾选后需要在下方 IPsec 按照需求进行相应配置)

工程	首页 / 客户端 /	子网														
系統配置	IPv4	IPv6														
接入协议 🗸	批量复制															
网口设置		+	名称	客户端网卡	接入类型	接入名称	IP源地址起始	IP源地址结束	IP目的地址起始	IP目的地址结束	DNS服务器IP	ARP学习	启用VLAN	Enable IPSec	Remote Access	Gatew
安量设置		~ ×	client	~	~	-	1.1.1.2	1.1.1.20	20.20.1.1	20.20.1.2		0	0			IPv4
媒体对象	VLAN	IPSec	IPSecIKEv2 GREVPI	N 自定义UI	DPVPN											
客户端 🔺	IPSec Polic	ties	Massage Decemplere													
子网	General Percistant	Tunnel	Message Parameters													
网络	Phase 1		Phase 2	Max Re-tran	ismit(sec): 5	N/	AT-T									
负载	IKE Lifetime(sec): 28800	Transform: ESP	SaLI	28800	0.	nable NAT-Traversal									
动作	Source	Port: 1025		Lifetime(sec)			Keepalive interval:	300								
服务端 🔻							NAT Source Port	4500								
关联						N	AT Destination Port:	4500								
测试订单						Origin	al Destination Port:	500								
报表 ▼	PFS: Gro	up2(MODP-1024)	HASH: HMAC-SHA1	Encryption	3DES-CBC	~										

+点击 按钮可配置子网, 可添加多个子网, 并可编辑和删除已有子网 系統配置 IPv6 IPv4 批量复制 网口设置 □ + 名称 客户端网卡 接入类型 接入名称 IP 源地址起始 ARP学习 启用VLAN Enable IPSec Remote Access Gatew IP源地址结束 IP目的地址起始 IP目的地址结束 DNS服务器IP • • **~ x** ~ 变量设置 1.1.1.20 1 20.20.1.1 20.20.1.2 媒体对象 VLAN IPSec IPSecIKEv2 GREVPN 自定义UDPVPN 客户端 VLAN ID 优先级 子网 □ 启用IP配置 网络 掩码: 负载 服务错

3.7.2客户端网络配置

工程	首页 / 客户端 / 网络														
系統配置 🗸 🔻															
接入协议 🗸 👻	批景复制														
网口设置		+	名称	源端口开始	源端口结束	目的端口开始	*目的端口结束	1Pv4 mss	1Pv6 mss	*TCP retries	TCP窗口大小	开启TCP	IP时间戳	TCP时间戳	ack_delay
态量设置	0		udo	100	60000	00	00	1460	1440	3	32768	Kai			· · ·
	0	× •	ambr	100	4040	26	26	1400	4440	2	00700				
媒体对象		× •	smp	1000	1010	25	25	1400	1440	3	32708				
太白岸		× •	sip	1000	1010	5060	5060	1460	1440	3	32768				
E27 JUQ -		× 🔟	RTSP	2000	3000	554	554	1460	1440	3	32768				
子网		1	RAW-TLS	1000	1010	443	443	1460	1440	3	32768				
网络		1	pop3	1000	1010	110	110	1460	1440	3	32768				
		1	opcua	1000	1010	4840	4840	1460	1440	3	32768				
负载		1	modbus	1000	2010	502	502	1460	1440	3	32768				
动作		/ 🗑	https	1000	2000	443	443	1460	1440	3	32768				
服务端 🔻	0	1	handle	1000	1000	2641	2641	1460	1440	3	32768				
	0	1	ftp	1000	2000	21	21	1460	1440	3	32768				
关联		1	dns	1000	60000	53	53	1460	1440	3	32768				
测试订单		1	client	1000	60000	80	80	1460	1440	3	32768				· · ·
报表 🗸															

名称: 该条网络配置的名称

源端口开始:配置仿真时 Client 端发起请求的四层源端口最小值 **源端口结束**:配置仿真时 Client 端发起请求的四层源端口最大值,最大值为 65535 **目的端口开始**:配置仿真时 Client 端发起请求的四层目的端口最小值 **目的端口结束**:配置仿真时 Client 端发起请求的四层目的端口最大值,最大值为 65535 **IPv4 mss**: IPv4 最大报文段长度 IPv6 mss: IPv6 最大报文段长度

TCP retries: TCP 重传次数

1.1

首页 / 客户端 / 网络

工程

TCP 窗口大小: 可以配置 TCP 默认窗口大小

开启 TCP RST: 用来指定当在测试任务时间到期后,对仍然存活的 TCP 连接采取 TCP RST 的方式关闭连接,当不 勾选时默认以 Finish 方式关闭连接

IP 时间戳: 该功能是在 ip option 上打上时间戳来计算链路时延(双单臂需要客户端和服务端同时开启 ip 时间戳 才会统计时延)

点击	Т	按钮可添加多个网络配置,	并可编辑和已有网络配置

系統配置	_														
接入协议 🔻	批量复制														
网口设置		+	名称	源端口开始	源靖口结束	目的端口开始	*目的端口结束	1Pv4 mss	1Pv6 mss	"TCP retries	TCP窗口大小	开启TCP RST	IP时间戳	TCP时间戳	ack_delay
变量设置		√ x						1460	1440	3	32768				
媒体对象		/ 📋	udp	100	60000	90	90	1460	1440	3	32768				 *
	0	1	smtp	1000	1010	25	25	1460	1440	3	32768				
客尸蹒 ▲	0	1	sip	1000	1010	5060	5060	1460	1440	3	32768				
子网	0	1	RTSP	2000	3000	554	554	1460	1440	3	32768				
网络	0	1	RAW-TLS	1000	1010	443	443	1460	1440	3	32768				
负载	0	1	pop3	1000	1010	110	110	1460	1440	3	32768				
		1	opcua	1000	1010	4840	4840	1460	1440	3	32768				
动作	0	1	modbus	1000	2010	502	502	1460	1440	3	32768				
服务端 🔻		1	https	1000	2000	443	443	1460	1440	3	32768				
关联		1	handle	1000	1000	2641	2641	1460	1440	3	32768				
	0	1	ftp	1000	2000	21	21	1460	1440	3	32768				
测试订单	0	1	dns	1000	60000	53	53	1460	1440	3	32768				
报表 ▼	0	/ 🗑	client	1000	60000	80	80	1460	1440	3	32768				•

3.7.3客户端负载配置

负载配置用来配置仿真时的四层业务模型,有2种规格:并发连接数、新建连接数。





工程	首页 / 客户端 / 负载
系统配置	
接入协议 🗸 🔻	运程负载编辑 负载·2 ▼ +
网口设置	%和: 并发连接数(connections ▼ *总连接数: unlimited
变量设置	「慎武: 性能模式 ♥ ① 100 100 100 100 100 100 100 100 100 1
媒体对象	竹发连接数: 100 connections 80 *uptime: 1,000,000 us 自动计算 ①
客户端 🔺	*案统时间: 2021-08-18 10:34:08 60 60 60 60 60 60 60 60 60 60 60 60 60
子网	「信助时间: Y-m-d Hits.u ① ↓ Create Load Profile X
网络	*上升时间: 10 sec ① 40 - * ********************************
负载	*名称: 20*名称:
动作	
服务端 🔻	
关联	
测试订单	

名称: 配置该负载项的名称

规格: 该配置项配置新建连接数、并发连接数的优先级关系,如当选择新建连接数优先时,则在测试时优先满足 设定的新建连接数指标。

总连接数: 配置总连接数指标值

新建连接数: 配置新建连接数指标值

并发数: 配置并发数指标值

系统时间:显示当前系统时间

启动时间:配置订单开始运行时间(距离当前时间需要大于 4 分钟)。若运行订单时超过此时间,则此配置不生效。

等待时间: 配置测试等待时间

- 上升时间: 配置测试爬坡时间
- 稳定时间: 配置测试稳定时间
- 下降时间: 配置测试下坡时间
- 拖尾时间: 配置测试拖尾时间

3.7.4客户端动作配置

动作用来配置网络协议仿真时,所仿真协议的 Client 端一侧的配置。

T4Ŧ	直页 / 春尸踽 / 动作			
系統配置 ▼	_			
接入协议 👻	批量复制			
网口设置	0	+	"名称	"协议
->	•	1	SIP-UDP	SIP_UDP
受里以直	0	1	SIP-TCP	SIP_TCP
媒体对象	0	1	HANDLE-UDP	HANDLE_UDP
客户端 🔺		1	рор3	POP3
子网	0	/ 🗑	smtp	SMTP
网络		1	πρ	FTP
负载	0	1	ATTACK	ATTACK
动作	•	/ 🗑	RTSP	RTSP
	0	1	UDP_REPLAY	UDP_REPLAY
服务端 🔻	0	/ 🗑	TCP_REPLAY	TCP_REPLAY
关联		1	https	HTTPS
测试订单	0	1	HANDLE-TCP	HANDLE_TCP
报表 ▼		1	OPCUA	OPCUA
40 144		1	modbus	MODBUS
2030		1	tis-replay	TLS_REPLAY

点击 🕇 捞	钮,通	 	拉菜单可以选择所需	防真的协议。可添加多个动作,并	并可编辑和删除已有动作。
	首页 / 客户	満 / 动作			
系統配置	-				
接入协议	北量复制				
网口设置			+	"名称	物议
交量设置			✓ ×		~
螺体对象	0		1	SIP-UDP	RAW_TCP RAW_UDP
	0		/ 1	SIP-TCP	RAW_TLS HTTP HTTPS
客户::::::::::::::::::::::::::::::::::::	^		1	HANDLE-UDP	FTP TCP_REPLAY
子网	0		/ 🗑	pop3	TLS_REPLAY DNS_TCP
网络			/ 1	smtp	DNS_UDP RTSP
负载			1	πp	CUSP MODBUS
动作				ATTACK	NETCONF OPCUA HANDLE TOP
服务端	-			RTSP	HANDLE_UDP
** #*				UDP_REPLAY	UDP_REPLAY
X				TCP_REPLAY	TCP_REPLAY
测试订单				https	HTTPS
报表	-			HANDLE-TCP	HANDLE_TCP
终端				OPCUA	OPCUA
				modbus	MODBUS
				tis-replay	TLS_REPLAY

1.1

选择具体协议后,可编辑协议相关的参数,本版本支持如下类型的协议仿真及带4层状态的7层应用回放功能:

RAW TCP: 一种简单的基于 TCP 承载的非标准应用,可自定义 client/server 端发送内容的大小 RAW_UDP: 一种简单的基于 UDP 承载的非标准应用,可自定义 client/server 端发送内容的大小 RAW_TLS: 一种简单的基于 TLS 承载的非标准应用,可自定义 client/server 端发送内容的大小 HTTP: 仿真标准的 HTTP 业务, 支持 get/head/post method, 支持自定义 header 字段及内容字段, HTTPS: 仿真 HTTPS 业务,系统自动完成 SSL 协商、KEY 交换及加密通道的建立 FTP:模拟标准的 FTP 协议,支持同时模拟 Client 端与 Server 端,支持主/被动模式 TCP REPLAY: 回放基于 TCP 承载的标准应用(如 HTTP)及非标准应用(如微信/QQ) **UDP REPLAY**:回放基于 UDP 承载的标准应用及非标准应用 TLS REPLAY:回放基于 TLS 承载的标准应用及非标准应用 DNS TCP: 仿真基于 TCP 承载的域名解析服务 DNS UDP: 仿真基于 UDP 承载的域名解析服务 RTSP: 仿真视频质量测试 ATTACK: 仿真基于 CVE 漏洞的网络攻击 **CUSP**: 仿真 CUSP 协议 **MODBUS:** 仿真 MODBUS 协议 **NETCONF:** 仿真 netconf 协议 **OPCUA:** 仿真 opcua 通信接口协议 HANDLE_TCP: 仿真基于 TCP 承载 HANDLE 工控协议 HANDLE UDP: 仿真基于 UDP 承载 HANDLE 工控协议 L2TP: 仿真隧道协议 SMTP: 仿真电子邮件传输协议 **PO3P:** 仿真邮局 POP3 协议 SIP_TCP: 仿真基于 TCP 承载 SIP 协议 SIP_UDP: 仿真基于 UDP 承载 SIP 协议 MQTT_TCP: 仿真基于 TCP 承载 MQTT 协议 **COAP_UDP:** 仿真基于 UDP 承载 COAP 协议

a) 通用配置

工程	首引	5 / 客户端 / 动作					
系統配置 🔻							
按入协议 🚽		批量复制					
网口设置				+	"名称	18	<i>bi</i> X
· · · · · · · · · · · · · · · · · · ·				≺×	http	НТТР	~
媒体对象		Common HTTP P	'arameters 分片				
		*发送超时时间:	720000000	us 🕐			
<u>客尸</u> 端 ▲		"接收超时时间:	720000000	us 🛈			
子网		*Think Time:	0	us 🕐			
网络		"事物数量	1	次			
负载							
动作							
服务端 ▼							
关联							

名称: 配置该动作的名称

发送超时时间:单位 us,如在该时间范围内未将需要发送的内容发送出去,则认为发送失败

接收超时时间: 单位 us, 这个接收超时时间是指客户端如在该时间范围内未收到服务端返回的全部内容, 则认 为接收失败

Think Time: 当客户端请求事务数量超过 1 个时,业务延迟时间表示客户端发起的两个事务之间的时间间隔,如 HTTP 事务数量为 2,则表示客户端会发送两次 HTTP 请求,两次 HTTP 请求之间的时间间隔为此处设置的业务延迟时间。

事务数量: 配置客户端发起的事务数量,当事务数量为 2 时,表示在一个 TCP 连接中,客户端会发起 2 次相同 的业务请求,如仿真 HTTP, Method 为 GET,此时表示客户端会在一个 TCP 连接中发起 2 次 HTTP GET 请求。

工程	首页 / 春户端 / 动作				
系統配置 🔻					
接入协议 👻	批量复制				
Прилад	0	+	*名称	"协议	
MUKE		✓ ×	http	HTTP	v
变量设置					
媒体对象	Common HT	TP Parameters 分片			
	开启分片:				
客户端▲	*分片类型:	● 分片大小 ○ 分片数量			
子网	*分片大小:	0 bytes			
网络	*分片处理方式:	~			
1216	*分片发送顺序:	~			
负载	仅发送首包:				
动作					
服务端 🔻					

开启分片:当打开该功能开关时,客户端将依据设置的规则对 IP 报文进行分片

分片类型:当前支持分片大小与分片数量两种分片方式,当分片类型为"分片大小"时,客户端将按照设置的值 对 IP 报文进行分片操作,如设置的分片大小为 100 字节,实际报文大小为 1200 字节,则该 IP 报文将会被分为 12 个 IP 分片。当分片类型为"分片数量"时,客户端将按照设置的数量对原始 IP 报文进行分片,如设置的"分 片数量"为 5,实际 IP 报文大小为 1000 字节,则该 IP 报文会被分为 5 个等长的 IP 分片。

分片大小:当"分片类型"设置为分片大小时。该处配置有效,用来配置每个 IP 分片的长度

分片处理方式:当前仅支持自动分片,该处配置默认即可

分片发送顺序:当前支持正序发送分片与倒序发送分片两种方式,正序发送是指按照分片包的顺序先后发送,即 按照第一个分片、第二个分片、第 N 个分片的顺序发送,倒序发送则是先发送第 N 个分盘,再发送第 N-1 个分 片,直至最后发送第一个分片。

工框	首贞 / 客尸端 / 动作				
系統配置 🗸 👻					
按入协议 🚽	批量复制				
1867 (19) 84		+	名称	协议	
网口设置		(M			
变量设置		✓ X	http	HTTPS	~
10/10/144	Common HTTPS F	Parameters 分片 TLS			
3#UKAJ BK	开启SSL/TLS:				
客户端 ▲	*类型:	○ 国密 ● 标准			
子网	*版本:	SSLv3 V			
网络	加密赛件1:	ALL			
7378	加密赛件2:	~			
负载	加密賽件3:	· · ·			
动作	加密赛件4:	~			
	加密赛件5:	~			
服务端 🔻	"懂手超时时间;	30000 ms			
¥Ħ	客户通验证:				
~~*	客户请证书:	选择文件			
测试订单	客户请私钥:	选择文件			
招売 🗸	服务纳CA证书:	/var/www/KODExplorer/k 选择文件			
10.1	服务講证书验证模式	not_verify 🗸			
终端					

开启 SSL/TLS:开启 SSL/TLS 加密开关,支持 SSL/TLS 加密的协议才会展示 (默认勾选)

类型:选择加密类型

版本:选择加密协议版本

加密套件 1~5:选择加密套件,至少选择一个

握手超时时间:单位 ms,如在该时间范围内握手完成,则认为握手失败

客户端验证: 客户端身份验证开关

客户端证书:选择客户端证书

客户端私钥:选择客户端私钥

服务端 Ca 证书:选择服务端 CA 证书

服务端证书验证模式:目前支持三种模式,not_verify、allow_untrust、allow_trust 等

b) RAW TCP/UDP/TLS 配置方法

Common	RAW_T	CP Parameters	分片	TLS	
是否测量时延:		✓			
每秒采集包数:		10			
请求大小:		500	bytes		
*响应大小:		500	bytes		

是否测量时延:勾选表示进行时延测量功能

每秒采集包数:采样包数时延,会按照配置的数值进行每秒抽样包数进行时延计算,并在结果中进行统计

请求大小:设置客户端 RAW TCP/UDP/TLS 的请求报文大小(对于 TCP/UDP 而言为 TCP/UDP 的 payload 部分,对于 TLS 而言为 TLS 所承载的内容大小)。

响应大小:用来客户端对比校验服务端响应客户端请求的内容长度与应该接收的内容长度是否一致,客户端会根据此处配置的大小来校验服务端的响应是否正确。

客户端与服务端仅对双方发送内容的长度进行校验,不对内容是否一致进行校验。

各户端与服务端的请求大小与响应大小必须一致,即客户端的请求大小与服务端的请求大小一致,客户端的响应大小与服务端的响应大小一致。

c) HTTP/HTTPS 配置方法

HTTP/HTTPS 协议仿真时主要区别为当仿真 HTTPS 时,系统会自动完成 SSL 的协商及加密通道的建立过程,具体 配置方法完全一致。

Common	HTTP Parameters	分片	TLS	
General				
关联服务器:				
*Host:	www.tes	st.com 🕡		
*URI:	/index.h	tml		
*Method:	GET N	•		
如应码:	200			
header字段。				
fielder j se				
提交内容:				

关联服务器:绑定服务端 IP 和域名,确保每次访问的服务端 IP 和域名是对应的。

Method: 设置 HTTP 的方法类型,当前支持 GET/HEAD/POST

Host: 设置 HTTP host 头, 如 a.b.com

URI:设置统一资源标识符,即请求的资源路径

变量设置: 在构造 HOST 与 URI 时,为了避免仿真的海量 HTTP 业务请求的 host 与 uri 出现一样的情况,可在 HOST 与 URI 中引入变量,仪表将按照设定的变量与步长变化规则对 HOST 与 URI 自动变化,变量的设置在仪表的 "变量设置"菜单栏中配置,配置方法见本配置手册第 3.5 章节

提交内容大小: 当 method 为 POST 时,该配置项有效,用来当未配置"**提交内容**"配置项时, POST 动作所需提 交内容的大小,系统会依据该大小,自动构造内容

Header 字段: 用来定义 HTTP 的头部信息,可按照头部标准字段构造头部,或完全自定义头部字段

提交内容:当 Method 为 POST 时该配置项有效,用来配置 POST 动作向服务端提交的内容,当配置该项时, method 必须为 post,且当该项配置时,"**提交内容大小**"配置项不生效

自定义校验 Header:用来自定义客户端自校验 header,服务端会比对客户端请求的 header 校验值与服务端所配 置的 header 校验值,如两者不一致,则认为请求非法。

🦶 同一个 HOST 或 URI 中可同时引入多个变量。

d) FTP 配置方法

ftp 协议客户端配置框如下

Common	FTP Parameters	分片	TLS
*Method:	ftp_meth	od_get 🗸	
*模式:	ftp_mode	e_port ❤	
用户名:	anonymo	us	
密码:	123456		
*URI:	/test.html		
★数据传输端口]范围: 40001	- 65000	
*上传下载类型	文件大小	~	
文件大小:	1000	by	rtes
突发大小:	15000	by	rtes
突发间隔:	2	m	s

Method:设置客户端 FTP 行为,当前版本支持 GET 与 PUT

模式:设置客户端 FTP 的工作模式,当前支持主动模式(port)与被动模式(pasv)

ftp_mode_port: v4 主动模式

ftp_mode_pasv: v4 被动模式

ftp_mode_eprt: v6 主动模式

ftp_mode_epsv: v6 被动模式

ftp_mode_lprt: 服务器指定要连接的长地址和端口

ftp_mode_lpsv: 进入长被动模式

用户名: 设置客户端登陆 FTP 服务器的账号, 账号需要和服务端配置保持一致

密码: 设置客户端登陆 FTP 服务器的密码, 密码需要和服务端保持一致

URI: 在客户端行为为上传时,此 URI 可任意填写,服务端并无实际的路径,当客户端行为为下载时,此 URI 必须与服务端配置的目标文件 URI 一致 (目前只支持一级目录)

数据传输端口范围:用来配置 FTP 数据连接时所使用的端口的范围

上传下载类型: 支持文件大小和文件路径,选择为文件大小时,直接输入大小数值即可;选择为文件路径时,可 直接选择资源管理器中任意文件



用户可自行向文件库中上传文件,供配置时调用。

STEP:右键单击,选择"上传",可从本地向文件库中上传指定的文件


							×
洋	 ★ 收藏夹 ✓ 計 我的文档 ✓ desktop 	 < ▲ test FT 新建文件夹 ▼ ↑ 上传 	TP_File	★ ↑ ↓ Q		Q 	-
	document document music pictures test 公共目录 doc pictures share	pshell.v2.0.1.e xe	上传中:0/1 (159.5K/s) 本地上传 离线下载 选择文件 Dotouch_XproReplay_Conf 2.7M	清空所有 25.5%(159.5K/s)	★ 清空已完成 ※		
		1个项目	DROP FILES HE	RE			

e) TCP/UDP/TLS REPLAY 配置方法

Common	TCP_REPLAY Parameters	分片
*回放文件:	选择资源管理器	文件▼
*回放样包:		选择文件
开启HOST替换	: 0	
HOST替换:		

TCP/UDP/TLS 回放功能分别用来回放基于 TCP/UDP/TLS 的标准应用或非标准应用,仿真模块会自动构建 4 层的状态信息,实现带 4 层状态的回放,**当前支持单个数据包中仅有 1 条流的回放,不支持单个数据包中含有多条流。** 回放文件:目前支持选择 资源管理文件(carray 文件)和 L7 回放样包(pcap/cap 文件)。

回放样包:当回放文件是选择资源管理器文件时,回放时要求数据包格式为 C Arrays,因此对于常规的 PCAP/CAP 包,因此需借助 wireshark 将其转换成 C Arrays 格式,具体方法如下:

开启 HOST 替换: 是否替换回放文件中的 host

HOST 替换: 要替换的 HOST

PCAP/CAP 转 C Arrays 格式方法

STEP 1:用 wireshark 打开数据包,右键点击需要所需回放应用所在流的任意一个数据包,选择"追踪"

	top.stream eq 12								×	
No	Time	Source	Bestination	Protocol	Length Info					
Г	35 3.945966	192.168.3.77	183.230.37.209	TCP	66 64692	→ 80 [SYN] S	eq=0 Win=64240	0 Len=0 MSS=1460	WS=256 SACK_PERM=1	
	45 3.975794	183.230.37.209	192.168.3.77	TCP	Mark/Unmark Packet(s)	Ctrl+M	K] Seq=0 Ack	-1 Win-8192 Len-0	MSS=1412 WS=4 SACK_PERM	-1
	46 3.975898	192.168.3.77	183.230.37.209	TCP	Ignore/Unignore Packet(s)	Ctrl+D	q=1 Ack=1 Wir	n=131072 Len=0		
	47 3.976094	192.168.3.77	183.230.37.209	HTTP	设置/取消设置 时间参考	Ctrl+T				
	59 4.006089	183.230.37.209	192.168.3.77	HTTP	时间平移	Ctrl+Shift+T	dified			
	63 4.036170	192.168.3.77	183.230.37.209	HTTP	分组注释	Ctrl+Alt+C	HTTP/1.1			
	69 4.066286	183.230.37.209	192.168.3.77	HTTP	10 120 100		dified			
	73 4.067529	192.168.3.77	183.230.37.209	HTTP	编辑解析的名称		TTP/1.1			
	85 4.097123	183.230.37.209	192.168.3.77	HTTP	作为讨读器应用		dified			
	88 4.138234	192.168.3.77	183.230.37.209	TCP	Propaga as Filter		q=1631 Ack=38	B2 Win=130816 Len	1=0	
	109 4.276057	192.168.3.77	183.230.37.209	HTTP	prepare as filter	,	_AD_2C.js HT	TP/1.1		
	117 4.306272	183.230.37.209	192.168.3.77	HTTP			dified			
	118 4.307882	192.168.3.77	183.230.37.209	HTTP	刘诺看巴		_AD_3L.js HT	TP/1.1		
	128 4.338080	183.230.37.209	192.168.3.77	HTTP	SCTP	•	dified			
	133 4.344555	192.168.3.77	183.230.37.209	HTTP	追踪流	•	TCP 流	Ctrl+Alt+Shift+T		
	142 4.375360	183.230.37.209	192.168.3.77	HTTP	复制	•	UDP 流	Ctrl+Alt+Shift+U		
>	Frame 35: 66 bytes	on wire (528 bits),	66 bytes captured (528 bits)			TLS 流	Ctrl+Alt+Shift+S	0	
>	Ethernet II, Src:	CyberTAN 4f:8f:91 (b	0:fc:36:4f:8f:91), [st: Huawe:	协议首选项	•	HTTP 流	Ctrl+Alt+Shift+H		
>	Internet Protocol	Version 4, Src: 192.	168.3.77, Dst: 183.2	30.37.209	Decode As		HTTP/2 Strea	am		
~	Transmission Contr	ol Protocol, Src Por	t: 64692, Dst Port:	80, Seq: (在新窗口显示分组(W)		QUIC Stream	n		
	Source Port: 646	592							2	
	Destination Port	t: 80								
	[Stream index: 1	12]								
	[TCP Segment Ler	n: 0]								
	Sequence number:	: 0 (relative sequ	uence number)							
	Sequence number	(raw): 760344424								
	[Next sequence r	number: 1 (relativ	/e sequence number)]							
	Acknowledgment r	number: 0								
	Acknowlodgmont r	numbon (now), 0								
() 🍸 wireshark_WLAW_202	00810152852_a13768.pcapng						分组: 393 ・ 已显示: 2	9(7.4%)・已丢弃:0(0.0%) 翫	置: Defau

STEP 2:选择"显示和保存数据为"C Arrays",保存即可。

🛋 🗏 🖉 📴 🛣 🖄 🗳 🍳 🐡 🗢 🕾 🖗 📃 🔍 Q. Q. A. H

*WLAN	✔ Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · port0-http-get.pcap	-		- 0 ×
文件(F) 编辑(E) 视图(V) 跳转(G)				
🖌 🔳 🧷 🛞 📙 🛅 🗙 🛅 🍳	char peer0 0[] = { /* Packet 11 */		^	
	0x47, 0x45, 0x54, 0x20, 0x2f, 0x69, 0x6e, 0x64,			
N rop. stream eq. 12	0x65, 0x78, 0x35, 0x30, 0x2e, 0x68, 0x74, 0x6d,			
No. Time Source	0x6c, 0x20, 0x48, 0x54, 0x54, 0x50, 0x2f, 0x31,			
35 3.945966 192.1	0x2e, 0x31, 0x0d, 0x0a, 0x48, 0x6f, 0x73, 0x74,			6 SACK_PERM=1
45 3.975794 183.2	0x3a, 0x20, 0x77, 0x77, 0x77, 0x2e, 0x74, 0x65,			1412 WS=4 SACK_PERM=1
46 3.975898 192.1	0x/3, 0x/4, 0x2e, 0x63, 0x6t, 0x6d, 0x0d, 0x0d, 0x0a,			
47 3.976094 192.1	0x43, 0x54, 0x5e, 0x74, 0x55, 0x5e, 0x74, 0x2d,			
59 4.006089 183.2	0×24 , 0×74 , 0×26 , 0×26 , 0×26 , 0×26 , 0×27 , 0×26 , $0 \times $			
63 4.036170 192.1	0,00, 0,014, 0,21, 0,10, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,			
69 4.066286 183.2	char neer1 $01 = \frac{1}{2} + 2$ packet 12 */			
73 4.067529 192.1	0×48 , 0×54 , 0×54 , 0×56 , 0×16 , 0×26 , 0×21 , 0×26 , 0×31			
85 4.097123 183.2	(3,2), $(3,3)$, $(3,3)$, $(3,3)$, $(3,2)$, $(3,4)$, $($			
88 4.138234 192.1	0x0a, 0x53, 0x65, 0x72, 0x76, 0x65, 0x72, 0x3a,			
109 4.276057 192.1	0x20, 0x4d, 0x69, 0x63, 0x72, 0x6f, 0x73, 0x6f,			
117 4.306272 183.2	0x66, 0x74, 0x2d, 0x49, 0x49, 0x53, 0x2f, 0x36,			
118 4.307882 192.1	0x2e, 0x30, 0x0d, 0x0a, 0x43, 0x6f, 0x6e, 0x74,			
128 4.338080 183.2	0x65, 0x6e, 0x74, 0x2d, 0x54, 0x79, 0x70, 0x65,			
133 4.344555 192.1	0x3a, 0x20, 0x74, 0x65, 0x78, 0x74, 0x2f, 0x70,			
142 4.375360 183.3	0x6c, 0x61, 0x69, 0x6e, 0x0d, 0x0a, 0x4c, 0x61,			
	0x/3, 0x/4, 0x2d, 0x4d, 0x6+, 0x64, 0x69, 0x66,			
> Frame 35: 66 bytes on wir	0x09, 0x05, 0x04, 0x33, 0x20, 0x54, 0x08, 0x75, 0x20,			
> Ethernet II, Src: CyberTA	0×20 , 0×44 , 0×01 , 0×20 , 0×20 , 0×21 , 0×20 , $0 \times $			
> Internet Protocol Version	0×30 , 0×30 , 0×30 , 0×30 , 0×31 , 0×51 , 0×20 , 0×78			
 Transmission Control Prot 	9x70, 0x69, 0x72, 0x65, 0x73, 0x3a, 0x20, 0x54			
Source Port: 64692	0x68, 0x75, 0x2c, 0x20, 0x30, 0x31, 0x20, 0x4a,			
Destination Port: 80	0x61, 0x6e, 0x20, 0x31, 0x39, 0x37, 0x30, 0x20,			
[Stream index: 12]	0x30, 0x30, 0x3a, 0x30, 0x30, 0x3a, 0x31, 0x37,			
[TCP Segment Len: 0]	0x20, 0x47, 0x4d, 0x54, 0x0d, 0x0a, 0x43, 0x6f,			
Sequence number: 0 (0x6e, 0x74, 0x65, 0x6e, 0x74, 0x2d, 0x4c, 0x65,			
Sequence number (raw):	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		•	
[Next sequence number:			*	
Acknowledgment number:	型T_1X1Hg (ans pyrez) → 至小小IF床行数据/小 C Arrays →		π U Ψ	
Acknowlodgmont numbon (查找:		查找下一个(N)	
O 🖉 wireshark_WLAN_202008101528	源掉此流 打印 Save as 返回	Close	Help	s) · 已丢弃: 0 (0.0%) 配置: Defau

回放时选择保存后的数据包文件即可。

AA 当回放某个指定的应用时,此时客户端与服务端需配置同一个数据包文件。

f) DNS_TCP/DNS_UDP 配置方法

DNS_TCP/DNS_UDP 用来模拟客户端 DNS 请求行为,两者的区别为 4 层承载协议是 TCP 或 UDP。

Common	DNS_TCP Parameters	分片	TLS		
Domain类型:	批量生成 🗸				
批量生成Dom	ain: www.test{\$dns}	.com (i)			
*DNS类型:	A 🗸				

Domain: 用来配置 DNS 解析请求的目标域名,目前 domian 类型支持单个域名、批量生成和上传文件三种。批量 生成引用的时变量设置中配置的规则,上传文件时选择资源管理器中的 domian 文件(格式为 csv,文件列头为 domian,addr),客户端会对请求的域名对应 IP 进行校验,如有不一致,则会统计在 invalid-ip 中,如下图所示

		5 6 6	T Q M					
4	domin.list.csv	× +						
1	domain,add	r						
2	www.baidu.	com,10.1.214.	123					
3	google.com	,2.2.2.2						
4								
1	「苗洋橋」 水坊	各 裁		TPC				
P.		贝轼 大		551				
	测试用例ID	pid	id	网卡名	requests	responses	invalid-ip	host
	0	0	0	a	52040472	50746476	0	
	0	0	0	ропо	52949472	52/164/6	0	www.baidu.com
	0	0	1	port0	52949472	52719461	52719461	google.com
	0	2	5	port1	52040472	52949472	0	www.baidu.com
	0	2	5	porti	52545472	52348472	0	www.baidu.com
	0	2	6	port1	52949472	52949472	0	google.com

DNS 类型: 有 A 或者 AAAA 两种, A 表示 IPv4 模式的 DNS, AAAA 表示 IPv6 模式的 DNS。

g) RTSP 配置方法

RTSP 协议用来模拟客户端使用 RTSP 协议播放视频的行为,RTSP 协议默认使用 554 端口

快速访问	首页 / 客户端	/ 动作								
工程										
系統配置	批量复制									
接入协议 🗸 👻		+	1	名称				*协议	类型	
网口设置		√ ×					RTSP	~		
		1	h	tp				HTTP		
	Common	RTSP Parameters	分片	TLS						
媒体XI家	"URI:	/								
客户端	*保存MDI值	虚拟用户数: 256		(设置每秒新建保存)	/IDI值虚拟用户数)					
子网	"视频播放清	部析标准: 0	<= MD	I:DF <= 10	并且 0	<= MDI:MLR	<= 5	MDI ①		
网络	*视频播放一	一般标准: 11	<= MD	I:DF <= 50	并且 6	<= MDI:MLR	<= 20			
力并	"视频播放较	送标准: 51	<= MD	I:DF 或者 21	< MDI:MLR					
<u></u> 	播放关闭超	时时间: 10		s (播放关闭超时:着	\$户端收不到RTCP结	谏报文时, 在指;	包时间内未收到 R	RTP 报文,虚拟用户会停止媒体播放)		
动作	流的统计数	≣ : 0		(数量为0表示不统计	,范围[0-10000])					
服务端										
关联										
测试订单任务栏					版权所有:北	京触点互动信息	則技术有限公司]京ICP备19037780号		订单未运行

URI:设置统一资源标识符,即请求的资源路径

保存 MDI 值虚拟用户数: 报表中输出 MDI 值的虚拟用户数量, 这个值必须小于虚拟用户数的总量。

MDI 为 媒体流丢失率和延迟的组合评价指标

MDI(Media Delivery Index)媒体传输质量指标是由思科公司和 IneoQuest 共同提出的,对视频流在 IP 网络传输质量进行评估的测量指标。作为 IP 视频流传输质量测试的行业标准,MDI 测量指标广泛地应用于 IPTV 和 IP 有线数字电视网络质量评估和监测。

对 IP 视频流的传输质量用 RFC 4445 MDI 标识为: DF: MLR。

MDI 包括了两个参数:

• Delay Factor(延迟因素,简称 DF):该数值表明被测试视频流的延迟和抖动状况。DF 的单位是毫秒

(ms)。DF 将视频流抖动的变化换算为对视频传输和解码设备缓冲的需求。被测视频流抖动越大,DF 值越大。当网络设备和解码器的缓冲区容纳的视频内容时间不小于被测视频流 DF 读数时,将不会出现视频播放质量的下降。因为网络节点需要分配不小于 DF 值的缓冲用于平滑视频流抖动,所以 DF 的最大值为视频内容通过该网络节点的最小延迟。

 Media Loss Rate(媒体丢包速率,简称 MLR): MLR 的单位是每秒的媒体封包丢失数量。该数值表明 被测试视频流的传输丢包速率。由于视频信息的封包丢失将直接影响视频播放质量,理想的 IP 视频流传输 要求 MLR 数值为零。因为具体的视频播放设备对丢包可以通过视频解码中进行补偿或者丢包重传,在实际 测试中 MLR 的阈值可以相应调整。

流的统计数量: RTP 报表中输出统计数据, 配置统计流的数量就是输出统计流的数量。

h) attack 配置方法

快速访问					
丁程		1	ATTACK_UDP_分片数量_倒序	ATTACK	自定义攻击流
		1	ATTACK_UDP_分片数量_正序	ATTACK	自定义攻击流
接入协议 ▼		1	ATTACK_TCP_分片数量_正序	ATTACK	自定义攻击流
网口设置		1	ATTACK_TCP_分片数量_倒序	ATTACK	自走义攻击流
· · · · · · · · · · · · · · · · · · ·		1	ATTACK_TCP_分片大小_倒序	ATTACK	自定义攻击流
城休对象		1	ATTACK_TCP_分片大小_正序	ATTACK	自定义攻击流
客户端		~ ×	ATTACK_UDP	ATTACK	自定义攻击流
子网		1	ATTACK_TCP	ATTACK	自定义攻击流
网络	Common	ATTACK Parameters	分片 TLS		
负载	後型	自定义攻击流 🗸			
动作	"回放文件: "承载协议:		olorer/(选择文件		
大联					
			版权所有:北京触点互动信	息技术有限公司京ICP备19037780号	订单未运行

attack 模拟网络攻击行为,客户端模拟发送攻击报文,配置页面如下

类型:目前仅支持自定义攻击流

回放文件:回放文件选择系统自带的 CVE 漏洞攻击文件



承载协议:根据需要,可选 tcp 或者 udp 协议

i) CUSP 配置方法

模拟 CUSP 协议的 up 进行测试

	+	名称	协议	类型
PPPOE	√ ×		CUSP 🗸	
DHCP	× 🔟	L3-replay	L3_REPLAY	
媒体对象	1	attack1	ATTACK	自定义攻击流
客户端 🔺	1	udp	RAW_UDP	
子网	1	tcp	RAW_TCP	
网络	Common CUSP Parame	eters 分片 TLS		
负载	*CUSP心跳间隔时间: 30	S		
动作	*槽位数量:			
关联 测试订单任务栏 订单列表 日志 ▼	* 単个層位成型 # 一个層位成判論口数 量 * 虚拟口类型: * なXLAN ID范围: * VXLAN ID范围: * VXLAN 目的IP: * 彼号类型: 不扱	▼ - ((又支持GPE格式) 号 ▼		
报表 ▼		版权所有・北京触点の	5-36信自技术有限公司 克ICP各19037780号	

CUSP 心跳间隔时间: 协议心跳间隔的时间

槽位数: 仿真 UP 的槽位数量

子槽位数: 仿真 UP 的子槽位数量

每个槽位虚拟端口数: 仿真 UP 的单槽位虚拟口数量设置

虚拟口类型: 仿真接口的类型, 目前已支持 GE、10GE、40GE、100GE、Eth-Trunk、Tunnel、VE 这 7 种类型

Common	CUSP Parameters	分片	TLS
*CUSP心跳间隔时	时间: 30	s	
*槽位数量:			
*子槽位数量:			
*单个槽位虚拟端 量:	口数		
*虚拟口类型:	~		
*VXLAN ID范围:	GE	-	(仅支持GPE格式)
*VXLAN目的IP:	40GE		
*拨号类型:	Eth-Trunk Tunnel	•	

VXLAN ID 范围:测试数据 vxlan 的范围

VXLAN 目的 IP: 指定 vxlan 的目的 ip 地址

拨号类型:拨号类型可以选择不拨号,也可以选择拨号方式。目前已经支持 PPPoEv4、PPPoE v6、 PPPoEv4&v6 兼容模式以及 DHCPv4 模式

Common	CUSP Parameters	分片	TLS
*CUSP心跳间	隔时间: 30	s	
*槽位数量:	32		
*子槽位数量:	2		
* 单个槽位虚拟 量∶	端口数 4		
*虚拟口类型:	10GE 🗸]	
*VXLAN ID范酮	国: 200	- 65500	(仅支持GPE格式)
*VXLAN目的IF	192.168.2.10)	
*拨号类型:	DHCPv4	~	
*虚拟口拨号次	数: PPPOEv4		
*虚拟口拨号速	率: PPPOEv6	6	
*虚拟口拨号在	线时长: DHCPv4	s	
*每个虚拟口拨 数:	·号用户 400		
DHCP用户	参数		
*重试次数:	3		
*vlan1:			

j) attack play 配置方法 (该功能已经迁移到 L3_REPLAY 子系统中)

attackplay 使用外部攻击库导入攻击文件模拟网络攻击行为

工程	
713	★ "名称 "协议 类型
系统配置 ▼	✓ [™] L3-replay L3_REPLAY
网口设置	✓★ attack1 ATTACK_PLAY ■ 自定义攻击流
<u> 变量设置</u>	v û udp RAW_UDP
PPPOE	✓ [™] tcp RAW_TCP
DHCP	ATTACK_PLAY Parameters
媒体对象	*启用ip轮换: □
客户端 🔺	类型: 描述时长 ▼
子网	· 播 放速率(倍数): 10000
网络	措放(间隔(ms)):
负载	
动作	攻击文件列表(已选文件可拖拽调整文件顺序) 清空文件列表 选择文件
关联	

配置页包含如下参数:

启用 IP 轮换:每一次攻击文件发送时使用的 ip 地址在子网配置的网段中轮换

类型:播放类型,包括按时间和按次数播放两种,按时间播放时设置时间后,在设置的时间里所选的攻击 文件顺序轮播,时间结束时结束测试;按次数播放时,设置播放次数后,所选文件轮流播放该次数后结束 测试。

播放速率:测试时的发包速率对比源文件的播放速率,如2就是代表以2倍的速度发包

播放间隔:两次播放之间的间隔时间

一级目录/二级目录: 所选攻击文件文件的目录, 由导入的攻击库文件决定 **攻击文件列表**: 已选中播放的攻击文件列表, 可以配置1个也可以配置多个

k) MODBUS 配置方法

modbus 是应用于电子控制器上的一种通用语言,系统仿真 modbus client 与服务端进行通信。

Common	MODBUS Parameters	分片	
*工作模式	式: TCP模式 - client	~	
*启用广播模:	武: 🗌 启用广播楼	载ID号为0,未启用ID为1~24	7
*modbus	id: 1	至 1	
req/resp:			
*req/re	sp: 添加	清空列表	
控制端负载数	据	终端负载数据	
0100030013		0103CD6B05	删除
0100030014		0103CD6B05	删除
0100030015		0103CD6B05	删除
0100030016		0103CD6B05	删除
0100030017		0103CD6B05	删除
0100030018		0103CD6B05	删除

工作模式: modbus 支持串口模式和 tcp/ip 模式传输,此开关用于配置是否开启串行链路。开启串行链路则支持 ASCII 模式

modbusid: 配置 modbusclient 的设备 id

req/rsp:配置控制器和终端的负载数据,可以配置1条,也可以配置多条

l) NETCONF 配置方法

仿真 netconf 终端,与 netconf 服务端进行通讯

ETCONF Parameters 分片	SSH								
ESN ID:									
前缀. 1019001 后缀开始	1000	后缀结束	1499	生成效果: 101900101000~1019	00101499				
"自定义变量: 增加变量 (最大值-最小	值)%步长==0,最大	(值和最小值的差值)	必须为步长的整倍数。	变量名不能重复,随机关型无需步长					
28	最小價			最大值		英型	步长		攝作
t.	1			10		递増~	1		25 10
r	1			5		進减 🗸	2		18 10:
d	1			10		随机・			10 14
相定义uri: 添加 清空列表	5 统计名需要(能速唯一		峭应数援	启用统计	请求统计名		明应统计名	操作
:huawei:params:xml:ns:yang:huawei-device				xml version="1.0"<br encodion="1ITF-8"2		huawei-device-req-0		huawei-device-rsq-0	删除
ietf:params:xml:ns:yang:ietf-interfaces				xml version="1.0"<br encoding="11TF-8"?		ietf-interfaces-req-1		ietf-interfaces-rsq-1	删除
huawei:params:xml:ns:yang:huawei-license	,			xml version="1.0"<br encoding="1.ITF-8"?		huawei-license-req-2		huawei-license-rsq-2	册除余
huawei:params:xml:ns:yang:huawei-hrp				xml version="1.0"<br encodion="1TF-8"?		huawei-hrp-req-3		huawei-hrp-rsq-3	删除
i ielf:params.xml:ns:yang.ielf-system				xml version="1.0"<br encoding="1TE-8"?		ietf-system-req-4		ietf-system-rsq-4	删除

NETCONF Parameters	分片	SSH	
*username:	root		
*password:	huawei@123		
*hostkey:	/var/www/KODEx	plorer/(选择文件	
*客户端公钥:	/var/www/KODEx	plorer/c 选择文件	
authkey-type:	~		

ESN ID : 定义 ESN ID 范围, 分为前缀和后缀开始和后缀结束 自定义变量: 自定义变量的范围, 支持单个或以上 自定义 url: 自定义 url 请求格式, 支持单个或以上 SSH : 配置 ssh 相应的认证信息

m) OPCUA 配置方法



Key 值可以填写中文、英文、数字、符号等混合 Value 值只能填写数字

n) HANDLE (TCP/UDP) 配置方法

Common	HANDLE Parameters	分片	TLS	Handle认证	
命令: 添加	清空列表				
命令: Q	uery 🗸 名称:te	est	删除		
添加index	添加type 添加value				
index: 1		删除			type: HS_SITE V 删除
					type: HS_NA_DELEGATE V 删除
value: HS_A	DMIN V			删除	
	"Inc	dex": 1, meStamp": 56789434.			
	דד"	LType": 1,			
	тт"	"L": 34523454,			
	"Pe	ermission": 15,			
	"Ту	pe": "HS_ADMIN",			
	"Da	ata": {			
		AdminPermission": 15			
		'AdminRef': {			
		"RefHandleName": "	1234/2345",		
		"RefIndex": 1			
				k	

Common	HANDLE Parameters	分片	TLS	Handle认证	
客户端认证	E:				
— 认证 (Au	uthoritative) :				
*认证方式:	秘钥字符串 🗸)			
*秘钥字符串	123456				
*HASH算法	SHA1 🗸				
凭证 (Ce	ertify) :				
需要凭证:					
DSA密钥文	件: /var/www/KOD	Explorer/e 选择	译文件		
RSA密钥文	/var/www/KOD	Explorer/(选择	译文件		
HASH算法:	SHA1 🗸				
会话秘钥字符	符串: 123654				
摘要 (Di	gest) :				
需要摘要:					

命令:添加查询命令和对应的名称

Index: 对应查询命令的索引

type: 对应查询命令的类型, 可支持单个或以上

Value: 对应查询值,可支持单个或以上

Handle 认证:客户端与服务端认证信息配置,保持一致即可

DSA 密钥文件: /var/www/KODExplorer/data/Group/public/home/doc/handle_cert/dsakey.pem

RSA 密钥文件: /var/www/KODExplorer/data/Group/public/home/doc/handle_cert/rsapubkey.pem

o) L2TP 配置方法

L2TP 可与华为防火墙对接进行测试,仪表支持模拟 L2TP client 和 server

Common	L2TP Parameters	分片 TLS
*隧道名称前缀	dotouch	不超过50个字节
隧道密码认证		
*隧道密码:		
•确认隧道密码	k:	
保活时间:	60	s
"隧道数量:		1~64000 ①
*会话数量:		1~64000 ①
*重试次数:		0~255
PPP用户接入		
*用户名密码:	► + /	Ĩ
会话心跳时间	0	s

隧道名称前缀: 配置隧道名称前缀, 仪表作为客户端值对前缀校验

隧道密码认证:是否开启隧道密码认证
隧道密码: client 和 server 协商 L2TP 隧道的密码,2 侧需要保持一致
保活时间:隧道保活时间,超过该时间还未建立隧道,则关闭隧道,默认 60S
隧道数量:单个隧道名需要建立的隧道数量
会话数量:单个隧道需要建立的会话数量
重试次数:隧道建立失败重试的次数
PPP 用户接入:接入类型
用户名密码:用户认证需要的用户名和密码

会话心跳时间:会话是否存活检测发送心跳报文时间

p) SMTP 配置方法

Common SMTP	Parameters 分片 TLS
开启服务端认证:	
*SMTP服务器:	
*SMTP用户名:	
*SMTP密码:	
*SMTP申明:	ehlo 🗸
*邮件类型:	手动编辑 🗸
*发件人:	
"收件人:	多个收件人以英文逗号分隔
抄送:	多个收件人以英文逗号分隔
密送	多个收件人以英文逗号分辅
· #2	
土趣	
附件:	选择附件
文件	操作
*正文:	
H B T:	

开启服务端认证: 是否认证开关,需和服务端保持一致。开启后报文中会出现 SMTP 认证报文 SMTP 服务器:配置 SMTP 服务器信息

SMTP 用户名/密码: SMTP 邮件用户名和密码

SMTP 申明: 申明类型, 支持 ehlo 和 helo

邮件类型: 支持手动编辑和导入 eml

发件人:邮件发件人

收件人/抄送/密送:邮件收件人/抄送/密送,支持单个和以上(多个以英文逗号隔开)

主题:邮件主题:

附件:邮件需要发送的附件,支持 txt/word/execl

正文:邮件发送的正文,支持中英文/数字/字母/特殊符号/图片

q) MQTT_TCP 配置方法

	_TCP Parameters 分片	
人证方式	用户名/密码认证 🖌 🛈	
用户名:	admin	
密码:	123456 ①	
角色	发布者 🗸	
客户端: ①		
1令: 添加	清空列表	
func1: CONNEC		
	0 ×	
qos		
qos topic	test	
qos topic msg	test 1010	
qos topic msg func1: PINGRE	test 1010 EQ 册版余	
qos topic msg func1: PINGRE	test 1010 EQ 删除	
qos topic msg func1: [PINGRE func1: [PUBLISH	test 1010 EQ V 制除	
qos topic msg func1: [PINGRE func1: [PUBLISH qos	test 1010	
qos topic msg func1: [PINGRE] func1: [PUBLISH qos topic	test 1010 EQ ✓ 創除 H ✓ 創除 PUBLISH	
qos topic msg func1: [PINGRE func1: [PUBLISH qos topic msgid(0-65536)	Image: Imag	

认证方式:选择客户端认证方式(目前支持不认证、用户名密码认证、客户端 ID 认证三种认证方式) **角色:** 仿真 MQTT 协议中的角色(目前仅支持发布者)

命令:添加对应的指令信息,支持添加和删除,支持参数的命令可以配置参数。

r) POP3 配置方法

Common POP3 F	Parameters 分片	TLS			
*账号:	lcf@zqh.cn				
*密码:	123456				
命令:					
添加 流					
stat查询邮箱中的统计(✓ 删除			
uidl查询邮件的唯一标志	5符 、	 ✓ 	删除		
retr获取邮件的内容		 1 	删除		
dele邮件上设置删除标		 1 	删除		
rest清除所有邮件的删除	余标记	▶ 删除			
top获取邮件头和邮件体	中的前n行内容	 ✓ 1 	1	删除	
noop检测POP3客户端	与POP3服务器的连接情况、	✓ 删除			

账号密码: POP3 邮箱账号密码

命令:添加对应的指令信息,支持添加和删除

s) SIP(TCP/UDP)配置方法

快速访问						
00020015			1	SIP_TCP-功能_标准WAV文件	SIP_TCP	
工程						
交体配置 ▼		``	×	SIP_TCP-分片大小-正序	SIP_TCP V	
	Pages: 1 2	Next Last	1 of 2			
接入协议 👻	Common		aramatara 🛆	μ		
网口沿署	Common	01 _101 1	arameters))	A		
网口这旦	主叫UA N	umber前缀:	130			
变量设置	*主叫UAI	Number起始值:	10000000	0		
1411-2-142	*主叫UAI	Number步长:	10			
媒体对象	被叫UA N	umber前缀:	189			
客户端 🔺	*被叫UAI	Number起始值:	20000000	0		
78	*被叫UAI	Number步长:	10			
-1-MJ	*语音文件	-	自定义音频 🖌			
网络	*编码格式	h. 2-	G.711A 🗸			
负载	*采样率:		8000	HZ		
=== (/=	*比特率:		64	kbps		
利用	*RTP 流的	的发包间隔	40	ms ①		
关联						27mm+12-12
500-81-764/-762-144				版权所有: 北京触点互动	言思玟不有限公司京ICP备19037780号	1 甲木运行

主叫 UA Number 前缀:主叫 UA Number 的前缀,仅支持数字,英文字母,下划线 主叫 UA Number 起始值:主叫 UA Number 的起始值,仅支持数字 主叫 UA Number 步长:主叫 UA Number 的步长,在起始值基础上递增 被叫 UA Number 前缀:被叫 UA Number 的前缀,仅支持数字,英文字母,下划线 被叫 UA Number 起始值:被叫 UA Number 的起始值,仅支持数字 被叫 UA Number 步长:被叫 UA Number 的步长,在起始值基础上递增 语音文件:仿真的语音文件,支持选择标准的 wav 文件、自定义音频。 编码格式:自定义音频中的配置项,支持 G.711A,G.711U 采样率:自定义音频中的配置项,单位 Hz 比特率:自定义音频中的配置项,单位 Kbps RTP 流发包间隔:单位 ms, RTP 流发包间隔需要大于或等于 10ms

t)COAP_UDP 配置方法

,	-		
Common	COAP_UDP Parameters	分片	
客户端:			
"请求: 添加	清空列表		
删除			
method	GET 🗸		
type	CON(必须回	夏) 🗸	
options	coap://		
payload			
删除			
method	POST 🗸		
type	CON(必须回)	复) 🗸	
options	coap://		
payload			
删除			
method	PUT 🗸		
type	CON(必须回	复) 🗸	
options	coap://		
payload			
删除			
method	DELETE 🗸		
type	CON(必须回)	复) 🗸	
options	coap://		
payload			

请求:添加对应的请求,也可以删除,请求选项和载荷可配置。

u) GRE 配置方法

GRE 认证信息在子网中进行配置

subnets		~	✓ port2	✓ port3	✓ 1.1.1	1.3	1.1.1.3	
IPSec IF	PSecIKEv2	IPSec证书	GREVPN					
EVPN								
1.1.1.1								
1112								
5	<0-42949672	295>						
	IPSec IF EVPN 1.1.1.1 1.1.1.2 5	IPSec IPSecIKEv2 EVPN 1.1.1.1 1.1.1.2	ubnets ✓ IPSeciŒ书 IPSec IPSeciŒ书 I.1.1.1 1.1.1.2 ✓ 5 <-0.4294967295>	ubnets port2 port2 IPSec IPSecIKEv2 IPSec证书 GREVPN EVPN 1.1.1.1 1.1.1.2 	ubnets port2 port3 IPSec IPSecIKEv2 IPSecI正书 GREVPN UPN 1.1.1.1 1.1.1.2 	ubnets ✓ port2 ✓ port3 ✓ 1.1. IPSec IPSecIKEv2 IPSec证书 GREVPN EVPN 1.1.1.1 1.1.1.2 ✓ 5 <0-4294967295>	ubnets v v port2 port3 1.1.1.3 IPSec IPSecIKEv2 IPSec证书 GREVPN EVPN 1.1.1.1 1.1.1.1 1.1.1.1 1.1.1.2 5 <0-4294967295>	ubnets ✓ port2 port3 ✓ 1.1.1.3 1.1.1.3 IPSec IPSecIKEv2 IPSecIE# GREVPN EVPN 1.1.1.1 1.1.1.2 ✓ 5 <0.4294967295>

启用 GREVPN:是否启用 GREVPN **GRE 本端地址**:GRE 隧道的本端地址

GRE 对端地址: GRE 隧道的对端地址

GRE 隧道校验: 是否开启隧道校验

GRE 关键字校验: GRE 隧道采用的关键字校验信息

3.8服务端

3.8.1服务端子网配置

服务端子网配置项用来配置服务端回应 client 时的源 IP 地址范围,支持 IPv4 与 IPv6。

点击 🛨 按钮可添加多个服务端子网,并可编辑和删除已有服务端子网。

工程	首页 / 服隽靖 / 子网								
系統配置									
接入协议 👻	IPv4 IPv6								
网口设置	批量复制								
本量设置		+	名称	服务端网卡	IP目的地址起始	IP目的地址结束	ARP学习	启用VLAN	
	0	1	ipsec-fw-v4-server		10.10.10.253	10.10.10.253			÷
採体対象	VLAN GREVPN	自定义UDPVPN							
客户端 ▼	VLAN ID 优先级								
服务端 🔺	▲ IP: 現時 因為 (D): (D): (D): (D): (D): (D): (D): (D):								
子网									
网络									
Profiles									
关联									

名称: 该 IP 子网的名称

服务端网卡:选择作为服务端的网卡

IP 目的地址开始/IP 目的地址结束:用来配置该仿真时服务端子网的起始 IP 与结束 IP。

ARP **学习**:当被测设备工作在二层,如网桥模式、透明模式等,此时仪表服务端与客户端处于同一个网段时,在 该场景下需开启该功能,此时服务端会直接向客户端 IP 发起 arp 请求后将数据包直接发送给客户端,而不是将数 据包交由下一跳网关转发,开启该功能后,设备工作在 L2 模式。

启用 VLAN: 当该子网需要启用 VLAN 时需勾选该功能(并配置下方 VLAN 相关信息)

VLAN ID: 该子网所在的 VLAN

优先级: 配置该 VLAN 的 Priority

启用 IP 配置: 配置该 Server 子网所在 VLAN 的 VLAN 子网 IP 地址

3.8.2服务端网络配置

服务端网络配置配置服务端使用的端口范围和报文长度等参数。点击页面的 🕇 按钮合议新增网络配置,也可 以编辑和删除已有网络配置项。

工作主	首页 / 服务端 / 网络											
系統配置	-											
接入协议	★ 批量复制											
网口:小學		+	名称	源端口开始	源端口结束	IPv4 mss	IPv6 mss	TCP retries	TCP窗口大小	IP时间戳	TCP时间数	ack_delay
MUQE		1	udp	90	90	1460	1440	3	32768			
变量设置		1	smtp	25	25	1460	1440	3	32768			
媒体对象		1	sip	5060	5060	1460	1440	3	32768			
	0	1	server	80	80	1460	1440	3	32768			
客尸端		1	RTSP	554	554	1460	1440	3	32768			
服务端	▲ □	1	RAW-TLS	443	443	1460	1440	3	32768			
子网	0	1	pop3	110	110	1460	1440	3	32768			
177140		1	opcua	4840	4840	1460	1440	3	32768			
网络		1	modbus	502	502	1460	1440	3	32768			
Profiles		1	https	443	443	1460	1440	3	32768			
关联	0	1	handle	2641	2641	1460	1440	3	32768			
201-11744		1	ftp	21	21	1460	1440	3	32768			
期就订单		1	dns	53	53	1460	1440	3	32768			
报表	-											

名称: 该条网络配置的名称

源端口开始:配置仿真时 Server 端的四层源端口最小值

源端口结束:配置仿真时 Server 端的四层源端口最大值,最大值为 65535

IPv4 mss: IPv4 最大报文段长度

IPv6 mss: IPv6 最大报文段长度

TCP retries: TCP 重传次数

TCP 窗口大小: 配置滑动窗口大小

IP 时间戳: 该功能是在 ip option 上打上时间戳来计算链路时延(双单臂需要客户端和服务端同时开启 ip 时间戳 才会统计时延)

3.8.3服务端 Profiles 配置

Profiles 用来配置网络协议仿真时,所仿真协议的 Server 端一侧的基本配置,部分仿真动作如网络攻击仿真不需要 server,所以无需配置服务端。页面可添加多个动作,并可编辑和删除已有 Profiles。

快速访问	首页 / 服务端 /	Profiles		
工程				
系统配置	批量复制			
接入协议 🗸		+	名称	协议
网口设置		1	https	HTTPS
变量设置		/ 🗑	test	RAW_TCP
媒体对象		/ 1	http	HTTP
客户端 ▼				
服务端				
子网				
网络				
Profiles				
关联				
测试订单任务栏 			版权所有:北京触点互动信息技术有限公司京ICP备19037780	号 订单未运行

点击 🕇 按钮添加新的 profile 后,可以选择所需仿真的协议。



a) 通用配置

首页 / 服务端	/ Profiles					
批量复制						
			+	名称		协议
			√×		HTTP	~
			1	http		нттр
Common	HTTP Par	rameters 分片				
发送超时时间	0:	720000000	us			
接收超时时间	1):	720000000	us			
业务时延:		0	us			
事物数量:		1	次			

Profiles 名称: 配置该 Profile 的名称

发送超时时间:单位 us,如在该时间范围内未将需要发送的内容发送出去,则认为发送失败 接收超时时间:单位 us,如服务端在该时间范围内未收到客户端请求的全部内容,则认为接收失败 Think Time:表示服务端在收到客户端请求事务时,延迟所设置的时间再发送事务响应,如客户端发起 HTTP GET 请求,此时服务端会延迟此处所配置的时间后才发送 Reponse 响应。 **事务数量:**配置服务端响应的事务数量,当事务数量为 2 时,表示在一个 TCP 连接中,客户端会发起 2 次相同的 业务请求,服务端也会响应两次。

首页 / **服务端** / Profiles

批量复制				
	+	名称	协议	
	√ ×	http	НТТР	~
Common HTTP	Parameters 分片			
开启分片:	0			
分片类型:	◎ 分片大小 ○ 分片数量			
分片大小	0 bytes			
分片处理方式:	~			
分片发送顺序:	~			
仅发送首包:				

开启分片:当打开该功能开关时,服务端将依据设置的规则对 IP 报文进行分片

分片类型:当前支持分片大小与分片数量两种分片方式,当分片类型为"分片大小"时,服务端将按照设置的值 对 IP 报文进行分片操作,如设置的分片大小为 100 字节,实际报文大小为 1200 字节,则该 IP 报文将会被分为 12 个 IP 分片。当分片类型为"分片数量"时,服务端将按照设置的数量对原始 IP 报文进行分片,如设置的"分 片数量"为 5,实际 IP 报文大小为 1000 字节,则该 IP 报文会被分为 5 个等长的 IP 分片。

分片大小: 当"分片类型"设置为分片大小时。该处配置有效,用来配置每个 IP 分片的长度

分片处理方式:当前仅支持自动分片,该处配置默认即可

分片发送顺序:当前支持正序发送分片与倒序发送分片两种方式,正序发送是指按照分片包的顺序先后发送,即 按照第一个分片、第二个分片、第 N 个分片的顺序发送,倒序发送则是先发送第 N 个分盘,再发送第 N-1 个分 片,直至最后发送第一个分片。

b) RAW TCP/UDP/TLS 配置方法

Common	RAW_TCP I	Parameters	分片	
是否测量时延:				
每秒采集包数:		0		
请求大小:				bytes
响应大小:				bytes

请求大小(客户端请求内容长度校验):用来服务端对比校验客户端发送的内容长度与应该接收的内容长度是否 一致,服务端会根据此处配置的大小来校验客户端的请求是否正确。

响应大小 (客户端请求响应内容长度): 设置服务端响应客户端请求的响应内容长度大小,客户端收到后会与其 配置的"**响应大小**"进行比对,如两者一致,则认为事务结束。

服务端与客户端仅对双方发送内容的长度进行校验,不对内容是否一致进行校验。

— 服务端与客户端的请求大小与响应大小必须一致,即服务端的请求大小与客户端的请求大小一致,服务端 的响应大小与客户端的响应大小一致。

c) HTTP/HTTPS 配置方法

HTTP/HTTPS 协议仿真时主要区别为当仿真 HTTPS 时,系统会自动完成 SSL 的协商及加密通道的建立过程,具体 配置方法完全一致。

当服务端返回内容类型为"页面大小"时,服务端会随机伪造"响应大小"配置项中设定长度的内容

Common	HTTP Parameters	分片	TLS		
响应码:	200 🗸				
header字段:	Server: Micro Content-Type Last-Modified Expires: Thu,	soft-IIS/6.0 e: text/plain I: Thu Jan 1 00:00: 01 Jan 1970 00:0	17 1970 D:17 GMT		
自定义校验 Header:					
返回内容:	页面大小	~			
页面大小:	200	bytes			

当服务端返回内容类型为"文件"时,服务端会加载"文件"配置项中选择的文件作为内容返回给客户端

Common HITP Param	eters 分斤					
响应码: [200 🗸					
header字段:	Server: Microsoft-IIS/6 Content-Type: text/pla Last-Modified: Thu Ja Expires: Thu, 01 Jan	8.0 in n 1 00:00:17 1970 1970 00:00:17 GMT				
自定义校验Header:						
返回内容: [文件 🖌 🖌					
URI:			(i) 文件:	ž	b择文件创建指定大小文件 +]
/ 🛛 🐳	tis-	replay			TLS_REPLAY	
/ 🗑 📚	DN	选择附件				- 🗆 X
/ 🗑 📚	DN	🚖 收藏夹	< 🛆 doc	ument test	★ ↑	Q
✓ ×	h	✓ ▲ 我的文档	新建文件夹 👻 🚹 上	:传 -	ie o ee	III . • •
/1:	RA	> document				
/ 🗑 📚	RA	> dump		7 7	7 7	
/ 🖬 📚	RA	∨ [0] 公共目录	1 10	500 1000	BitTorrent.carr dhcp.carray ay	dns.txt
Common HTTP Param 前应码: 200 header字段: Se Ca	eters 分片 ママ erver: Microsoft-IIS/6.0 ontent-Type: text/plain sst-Modified: Thu Jan 1.00	custom-cve doc resource share system	dns2.bt ftp	http.carray http_cctv_mi	us http_cctv_new http_huashuT s V	http_leTV
自定义校验Header: 返回内容: 文代 URL:	xpires: Thu, 01 Jan 1970 0 #		http_netease_ http_sina_diam hd bo	imap.carray IM_weixin.ca ay	arr ipv6_dns.txt menu.sql	mysql.carray
			36个项目			弗拉 取消

当服务端返回内容类型为"混合页面大小"是,服务端会将配置中混合大小按照轮询顺序依次返回给客户端

	h.
自定义校验Header:	
提交内容大小:	bytes
*返回内容:	混合页面大小 🗸
"混合页面大小:	200
	300

当服务端返回类容类型为"指定目录"时,服务端会加载指定目录下的文件名作为 uri 返回给客户端,此时客户端配置的 uri 也必须是该目录下的 uri 名称

Common	HTTP Parameters	分片		
响应码:	200 🗸]		
header字段:	Serve Conte Last-N Expire	r: Microsoft-IIS/6.0 nt-Type: text/plain /lodified: Thu Jan 1 es: Thu, 01 Jan 197	00:00:17 1970 70 00:00:17 GMT	
自定义校验He	ader:			
返回内容:	指定目前	₹		
目录:	/test/tes	t		

响应码:设置服务端响应客户端请求时的响应码,当前支持 200 和 404

Header 字段: 服务端 Response 报文的 header 字段,可自定义标准及非标准字段。

文件:配置服务端响应客户端请求该 URI 时使用指定文件返回给客户端,当配置该项时,"响应大小"字段不生效。

自定义校验 Header:用来验证客户端所配置 header 字段与服务端 header 字段是否一致,如不一致,则认为请求 非法。

🔪 当"指定目录"的目录大小大于 1G 时,请使用 HTTP Dir 子系统进行测试。

d) FTP 配置方法

Common	FTP Parameters	分片	
*开启认证:			
用户名:	anon	ymous	
密码:			
数据传输端口	范围: 4000	1 - 65000	(
上传下载类型		~	
突发大小:	5000	0	bytes
突发间隔:	2		ms

开启认证:是否启用登陆认证,开启认证后,客户端用户名和密码必须和服务端保持一致。 用户名:设置客户端登陆 FTP 服务器的账号,账号需要和服务端配置保持一致 密码:设置客户端登陆 FTP 服务器的密码,密码需要和服务端保持一致 数据传输端口范围:用来配置 FTP 数据连接时所使用的端口的范围 上传下载类型:

支持文件大小和文件路径,选择为文件大小时,直接输入大小数值即可。 选择为文件路径时,需配置 URI,然后选择资源管理器中任意文件。

e) TCP/UDP/TLS REPLAY 配置方法

Common	TCP_REPLAY Parameters	分片	
*回放文件:	选择资源管理器	文件 🗸	
*回放样包:		选择文件	
开启HOST替拍	ಱ: □		
HOST替换:			

TCP/UDP/TLS 回放功能分别用来回放基于 TCP/UDP/TLS 的标准应用或非标准应用,仿真模块会自动构建 4 层的状态信息,实现带 4 层状态的回放,当前支持单个数据包中仅有 1 条流的回放,不支持单个数据包中含有多条流。 回放文件:目前支持选择 资源管理文件(carray 文件)和 L7 回放样包(pcap/cap 文件)。

回放样包:当回放文件是选择资源管理器文件时,回放时要求数据包格式为 C Arrays,因此对于常规的 PCAP/CAP 包,因此需借助 wireshark 将其转换成 C Arrays 格式。

开启 HOST 替换: 是否替换回放文件中的 host

HOST 替换: 要替换的 HOST

▶ 当回放某个指定的应用时,此时客户端与服务端需配置同一个数据包文件。

当前版本仅支持单个数据包文件中只包含1条流。

f) DNS_TCP/DNS_UDP 配置方法

Common DNS_TCF	Parameters 分片
*Host文件:	上传文件 ✔
*上传Host文件:	选择文件 ④
*TTL生存时间(s):	0
Common DNS	TCP Parameters 分片
*Host文件:	手动创建 ✔
*手动创建host文件:	 ✓ + /
*TTL生存时间(s):	0
Common DNS *Host文件: *手动创建host文件: *TTL生存时间(s):	TCP Parameters 分片 手动创建 ✓ ✓ + ✓ 面 0

DNS_TCP/DNS_UDP 用来配置域名与 IP 的对应关系

Host 文件: 用来添加记录有域名与 IP 对应关系的 Host 文件,当接收到客户端发起的域名解析请求时,服务端将 查询 host 文件,根据 host 文件中记录的域名与 IP 对应关系,响应客户端的域名解析请求。支持上传文件和 手动创建

手动创建 host 文件: 当 Host 文件选择 手动创建 时,展示 **手动创建 host 文件,**点击 + 号可以手动创建 host 文件,并支持修改和删除。

上传 Host 文件:当 Host 文件选择 上传文件时,展示上传 Host 文件,点击选择文件即可从资源管理器中选择一 上传的 host 文件,Host 文件类型及域名填写方式参照 Linux 下的 hosts 文件,可直接下载 linux 系统/etc 目录下的 hosts 文件进行编辑添加 DNS 记录后上传至仪表。上传方式如下:



g) RTSP 配置方法

RTSP 服务端配置中, 仅需要配置服务端播放的流媒体文件。

Common	RTSP Parameters	分片	TLS				
流媒体:	●文件 ○媒(体对象					
URI:	1						
文件:		选择文	件 (目前只支持H264格式,	, 媒体采样率为90000,	帧数为25的视频)		

流媒体支持两种模式

文件: 自主上传的流媒体文件, 目前仅支持 H264 格式的文件。

媒体对象:即媒体对象中配置的虚拟视频媒体文件,下拉选择即可。

h) MODBUS 配置方法

MODBUS 服务端配置中,需要配置工作模式和协议传输模式

Common MODBUS Parar	meters 分片	
*工作模式: TCP模式 - s	erver 🗸	
*启用广播模式: 🗌 🔋 启	開广播模式ID号为0,未启用ID为1-	247
*modbusid: 1	至 1	
req/resp:		
*reg/resp: 添加	清空列表	
*req/resp: 添加	清空列表	
*req/resp: <mark>添加</mark> 控制端负载数据	清空列表 终端负载数据	
Yreq/resp: 添加 控制端负载数据 0100030013	清空列表 终端负载数据 0103CD6B05	删除
req/resp: 添加 控制端负载数据 0100030013 0100030014	清空列表 终端负载数据 0103CD6B05 0103CD6B05	删除
*req/resp: 添加 控制端负载数据 0100030013 0100030014 0100030015	清空列表 终端负载数据 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05	删除 删除
Yreq/resp: 添加 控制端负载数据 0100030013 0100030014 0100030015 0100030016 0100030016	清空列表	删除 删除 删除
req/resp: 添加 控制端负载数据 0100030013 0100030014 0100030015 0100030015 0100030016 0100030017 0100030017	済空列表 终端负载数据 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05	删除 删除 删除 删除
Yreq/resp: 添加 控制端负载数据 0100030013 0100030014 0100030015 0100030016 0100030017 0100030017 0100030018	済空列表 総議会戦数据 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05 0103CD6B05	
Yreq/resp: 添加 控制端负载数据 0100030013 0100030014 0100030015 0100030016 0100030017 0100030017 0100030018 0100030019 0100030019	済空列ま 総議负載数据 0103CD6805	· · · · · · · · · · · · · · · · · · ·

工作模式:modbus 支持串口模式和 tcp/ip 模式传输,此开关用于配置是否开启串行链路。开启串行链路则支持 ASCII 模式

modbusid: 配置 modbus client 的设备 id

req/rsp: 配置控制器和终端的负载数据,可以配置1条,也可以配置多条

i) OPCUA 配置方法

Common	OPCUA Parameters	分片	
key/value:	:		
*key/valu	e: 添加	清空列表	
key		value	
key_test		12345678	

Key 值可以填写中文、英文、数字、符号等混合 Value 值只能填写数字 注意:需与客户端填写保持一致

j) L2TP 配置方法

	+	名称	协议
	✓ ×		L2TP v
Common L2TP	Parameters 分片		
本端隧道名称前缀:	dotouch		
隧道密码认证:			
隧道密码:			
确认隧道密码:			
认证城:	不认证・+ / 窗		
L2TP认证模式:	CHAP&PAP 🗸		
用户地址分配:	ip_pool ▼ + ✓ 富		
保活时间:	60 s		

edit								×
— 用	*名称 ip_po 户地址池分配(最多200	ol 服务器地力 务端承载技	上为服 协议目					
No.	*本端IP(i)	*服务器地址	*地址池起始地址	*地址池结束地址	*首选DNS	*备选DNS	+	
1	172.16.100.5	10.1.1.1	10.1.1.100	10.1.1.110	10.1.1.1	8.8.8.8	添加 删除	
 本务	端地址填写服 端子网地址段 内ip		地址协议	1 池为与承载 目的地址同 段地址				

本端隧道名称:配置本端隧道名称,默认与客户端一致即可 隧道密码认证:是否开启隧道密码认证 隧道密码: client和 server协商 L2TP 隧道的密码,2 侧需要保持一致 认证域:添加用户认证用户名和密码 L2TP 认证模式:支持 CHAP/PAP/CHAP&PAP 三种模式 PPP 用户接入:接入类型 **用户地址分配:** 配置 server 分配给用户的 ip 信息,可以新增,修改,删除 **保活时间:** 隧道保活时间,超过该时间还未建立隧道,则关闭隧道,默认 60S

k) HANDLE (TCP/UDP) 配置方法

Common HANDLE	Parameters 分片 TLS Handle认证		
*命令: 添加	清空列表		
命令: Query	✓ 名称: test 删除		
添加index 添加type	添加value		
index: 1	删除	type: HS_SITE	
		type: HS_NA_DELEGATE V 翻除	
value: HS_ADMIN	▼ { "Index": 1	1	
	"TimeStamp": 56789434,		
	"TTLType": 1,		
	"TTL": 34523454,		
	"Permission": 15,		
	"Data": {		
	"AdminPermission": 15,		
	"AdminRef": {		
	"RefHandleName": "1234/2345", "Reflordev": 1		
Common HANDI	F Parameters 슈브 TIS Handleit)과		
服务端认证:			
 认证 (Authoritativ	e) :		
*需要认证:			
*秘钥字符串:	123456		
*DSA密钥文件:	选择文件		
*HASH算法:	SHA1 V		
凭证 (Certify) :			
凭证方式:	HS_SIGNED V		
DSA密钥文件:	/var/www/KODExplorer/ 选择文件		
RSA密钥文件:	/var/www/KODExplorer/d 选择文件		
HASH算法:	SHA1 🗸		
会话秘钥字符串:	123654		
摘要 (Digest) :			
塔西古 上 ,	MDE		
1835673306	The second secon		

命令:添加查询命令和对应的名称

Index: 对应查询命令的索引

type: 对应查询命令的类型, 可支持单个或以上

Value: 对应查询值,可支持单个或以上

Handle 认证:客户端与服务端认证信息配置,保持一致即可

DSA 密钥文件: /var/www/KODExplorer/data/Group/public/home/doc/handle_cert/dsakey.pem

RSA 密钥文件: /var/www/KODExplorer/data/Group/public/home/doc/handle_cert/rsapubkey.pem

l) SMTP 配置方法

Common	SMTP Parameters	分片	TLS
开启服务端认	iΞ: 🗆		
*SMTP用户名	i:		
*SMTP密码:			

开启服务端认证: 是否认证开关,需和客户端保持一致。开启后报文中会出现 SMTP 认证报文 SMTP 用户名/密码: 与客户端配置保持一致

m) POP3 配置方法

*账号: *密码:	Common	POP3 Parameters	分片	TLS
*密码:	*账号:			
	*密码:			

账号/密码: 与客户端配置保持一致

n) SIP(TCP/UDP)配置方法

快速访问	首页 / 服务端 /	Profiles								
工程	_									
系統配置	批量复制			_						
接入协议 🗸 🗸				+	名称				协议	
网门设置			~	×				SIP_TCP		~
本最沿置			1	۳. T	http-server				HTTP	
	Common	SIP_TCP F	Parameters	分片						
媒体对家	被叫UA Num	ber前缀:	189							
客户端 🔻	*被叫UA Nu	mber起始值:	20000000	(1)						
服务端	*被叫UA Nu	mber步长:	10							
子网	*语音文件:		自定义音频 G.711A 🗸	v						
网络	*采样率:		8000	HZ						
Profiles	*比特率:		64	kbps						
	* RTP 流的发	包间隔	40	ms 🛈						
关联										
测试订单任务栏										
					版权后	后有: 北京触点互动信息技术有限/	公司 克ICP备19037780)号	订单未	运行

被叫 UA Number 前缀:被叫 UA Number 的前缀,仅支持数字,英文字母,下划线 被叫 UA Number 起始值:被叫 UA Number 的起始值,仅支持数字 被叫 UA Number 步长:被叫 UA Number 的步长,在起始值基础上递增 语音文件:仿真的语音文件,支持选择标准的 wav 文件、自定义音频。 编码格式:自定义音频中的配置项,支持 G.711A,G.711U 采样率:自定义音频中的配置项,单位 Hz 比特率:自定义音频中的配置项,单位 Kbps RTP 流发包间隔:单位 ms,RTP 流发包间隔需要大于或等于 10ms 📙 服务端与客户端的 被叫 UA, 语音文件 相关配置需保持一致。

o) MQTT_TCP 配置方法

Common MQTT_TC	P Parameters 分片
*认证方式	用户名/密码认证 🗸 ①
*用户名:	admin 🛈
*密码:	123456
*角色	发布者 🗸
服务端:	
*爺令: 添加 func: CONNACK msgid(0~65536)	清空列表 ✓ <u>測除</u> 1
func: PINGRESP	別除
msgid(0~65536) func: PUBACK	1
msgid(0~65536)	1

认证方式:选择客户端认证方式(目前支持不认证、用户名密码认证、客户端 ID 认证三种认证方式) **角色:** 仿真 MQTT 协议中的角色(目前仅支持发布者)

命令:添加对应的指令信息,支持添加和删除。

p) COAP_UDP 配置方法

Common	COAP_UDP Parameters 分片
服务端:	
*自动回复	
*响应: 添加	清空列表
删除	
method	GET V
type	SUCCESS-VALID V
options	coap://
payload	
删除	
method	POST V
type	SUCCESS-CREATED V
options	coap://
payload	

自动回复:开启自动回复,开启后根据客户端请求命令自动响应。 **响应:**添加对应的请求,也可以删除,请求选项和载荷可配置。

3.9关联

3.9.1服务端和客户端关联

关联配置项用来绑定最终客户端的各项配置, 包括客户端关联页和服务端关联页,分别绑定前面配置的客户端 和服务端各项参数。

工程	首页 / 关联												
系統配置 ▼	添加测试订单												
接入协议 🔻													
网口设置	客户端关联 服务端关联												
变量设置	名称:	े .											
媒体对象		+	"名称	关联类型	*子网类型	*子网	"协议类型	动作	'网络	开启全局负载	负载	*权重	
客户端 🔻		1	pppoe	接入网[pppoe-ipv4]									*
服名端 👻		1 🗰 📚	SIP-UDP	用户面	IPv4	client	标准协议	SIP-UDP	sip		负载	100	
		/ 🗑 📚	SIP-TCP	用户面	IPv4	client	标准协议	SIP-TCP	sip		负载	100	
关联		/ 🗑 📚	HANDLE-UDP	用户面	IPv4	client	标准协议	HANDLE-UDP	handle		负载	100	
测试订单		1	pop3	用户面	IPv4	client	标准协议	pop3	pop3		负载	100	
		1 🗊 📚	smtp	用户面	IPv4	client	标准协议	smtp	smtp		负载	100	
- 报表 ▼		1 🖉 📚	ftp	用户面	IPv4	client	标准协议	ftp	ftp		负载	100	
终端		1 🗑 📚	RAW-TLS_v6	用户面	IPv6	client_v6	标准协议	RAW-TLS	RAW-TLS		负载	100	
	0	1 🗊 📚	RAW-UDP_v6	用户面	IPv6	client_v6	标准协议	RAW-UDP	client		负载	100	
	0	1 🖉 📚	RAW-TCP_v6	用户面	IPv6	client_v6	标准协议	RAW-TCP	client		负载	100	
	0	1 🗊 📚	rtsp	用户面	IPv4	client	标准协议	RTSP	RTSP		负载	100	
	0	1 🗑 📚	udp_replay	用户面	IPv4	client	标准协议	UDP_REPLAY	udp		负载	100	
	0	1 🗑 🖉	tcp_replay	用户面	IPv4	client	标准协议	TCP_REPLAY	udp		负载	100	
		1 🗑 📚	https	用户面	IPv4	client	标准协议	https	https		负载	100	
		1 🗑 📚	HANDLE-TCP	用户面	IPv4	client	标准协议	HANDLE-TCP	handle		负载	100	*
	Pages: 1 2 Next Last 1 of	2											

点击 🕂 按钮添加关联,可以添加多条关联,并可编辑和删除已有关联

工程	首页 / 关联											
系統配置 ▼	经由利用:FiT#											
接入协议 👻												
网口设置												
变量设置	名称	<u>्</u> ४										
媒体对象	0	-	名称	关联类型	子网类型	子网	协议类型	动作	·网络	开启全局负载	负载	"权重
寄戸端 ▼		√ ×]	~	~	~	~	~	0	~	
	0	1	pppoe	接入网[pppoe-ipv4]								A
• INCCOM	0	1 🗑 📚	SIP-UDP	用户面	IPv4	client	标准协议	SIP-UDP	sip		负载	100
关联	0	1 🗑 📚	SIP-TCP	用户面	IPv4	client	标准协议	SIP-TCP	sip		负载	100
測试订单	0	1 🗑 📚	HANDLE-UDP	用户面	IPv4	client	标准协议	HANDLE-UDP	handle		负载	100
	0	1 🗑 📚	pop3	用户面	IPv4	client	标准协议	pop3	pop3		负载	100
- 报表 ▼	0	/ 🗑 📚	smtp	用户面	IPv4	client	标准协议	smtp	smtp		负载	100
终端	0	/ 🗑 📚	ftp	用户面	IPv4	client	标准协议	ftp	ftp		负载	100
	0	/ 🗑 📚	RAW-TLS_v6	用户面	IPv6	client_v6	标准协议	RAW-TLS	RAW-TLS		负载	100

名称:配置客户端关联名称
关联类型:配置客户端关联类型
子网类型:配置客户端子网类型
子网:配置客户端子网,选择在"子网"中已配置子网
协议类型:配置客户端使用协议类型
动作:选择在"动作配置"中已配置动作
网络:配置客户端的网络
开启全局负载:配置是否开启全局负载

负载:选择在"**负载**"中一配置负载

权重:配置该动作的权重,在进行一次测试时,可同时仿真多种业务流量,如同时仿真 HTTP、FTP、DNS 等,此时可通过设置权重值来配置不同业务仿真流量所占比例,当前支持按照新建的权重设置。

3.9.2添加测试订单

新建测试订单时,需要首先勾选客户端关联和服务端关联项,然后点击 按知题试订单 按钮,就会弹出一个生成测试订单的弹窗。

	首贞 / 关联					
系統配置	57-6-190-P1T 24					
接入协议 🔻	780110316(1) 4±	添加测试订单	:	×		
网口设置	客户端关联(1) 服务端关联(1)	任务名称 测试订单-819				
变量设置	名称 📃 🤇 🏹	开启协议篡改 OFF	协议复改规则编辑 规则等助手册			
媒体对象	D	导入篡改文件	选择文件 ①	Profile	网络	
客户端 🔻	D			SIP-UDP	sip	*
8D 47 Mil				SIP-TCP	sip	
BR953m 🔻				HANDLE-UDP	handle	
关联		立即运行		pop3	pop3	
测验表开始	O	SEARCE 13		smtp	smtp	
1016010 -				ftp	ftp	
报表 マ	O			RAW-TLS	RAW-TLS	
终端	O			RAW-UDP	server	
	O			RAW-TCP	server	
	O			RTSP	RTSP	
	O			UDP_repaly	udp	
				TCP_repaly	udp	
				https	https	
	0			HANDLE-TCP	handle	
	0			OPCUA	opcua	Ţ

所属任务栏:任务栏名称可以自定义填写

开启协议篡改:点击开启协议篡改可以自定义修改协议,详细规则见 3.9.3 节。

立即运行:提交订单,并立即运行

3.9.3协议篡改规则配置

网络协议模糊测试是在 XPRO 云测网络仿真测试工具已有协议栈基础之上的叠加功能,可以给管理员提供灵活的数据包修改功能进行协议的模糊化测试,测试被测设备的协议健壮性。

目前支持的改包协议包括:

- ●2 层协议: 以太网
- ●3 层协议: IPV4 / IPV6
- ●4 层协议: TCP / UDP
- ●7 层协议:通过脚本自定义规则进行匹配和修改。

配置栏在生成测试订单的页面,如下图所示:

开启协议篡改后,点击协议篡改规则编辑进入规则编辑页面

工程	首页 / 关联							
系统配置								
	添加测试订单		添加测试订单					×
网口设置	客户端关联(1)	服务端关联(1)	任务名称	测试订单-819				
变量设置	名称:	<u>م</u> ک	开启协议篡改		协议复改规则编辑	规则帮助手册		_
媒体对象			B) 管计文件					
	0		4/2021+		辺洋文件 ①			
各广;蹒 ▼								
			, v	即运行				
测试订单	0							
招表								
								_
添加测试订单					×			
15 4 4 9 4	测定21 单 040							
江另有小	2015(1) 1 -019		_					
エロホルの留いた	ON ON	协议算收扣则编辑	비미미 호망 만 구 유유					
) I A WIX X X X		1/3 CALLAR HALPOUND HTTP REA	X6X3+9 40-3-00					
导入篡改文件		Edit Protocol	Tamper					×
导入复改文件		Edit Protocol	Tamper IPV6					×
导入复改文件		Edit Protocol	Tamper IPV6	業用		修改包数目	時印刷医若用	×
导入篡改文件		Edit Protocol IPV4 字段名称 version 面	Xelectronetary Tamper IPV6 定值 ✔ 3	关型		修改包数量 10	除机间隔范围	*
57月87以至4 导入要改文件 立即5	五行 五行	Edit Protocol IPV4 学级名称 version 庫 ihl 不	Note the set of the	<u>类型</u>		修改包数量 10 	随机间隔范围 	×
7月前初代要求 导入篡改文件 <u>文即</u> 政	五行	Edit Protocol IPV4 76826 version () ihl () dscp () ()	- CARTHALE +112 Tamper IPV6 空値 ▼) 3 等次 ▼	<u>类型</u>		修改包数量 10 ()	酸机间隔花園 	×
7月670公里在 导入墓故文件 <u>文即</u> 近	五 石 万	Edit Protocol IPV4 FRAM version III inl TA dscp TA ecn TA	- ○ Cold Weak (+ 1)(2) Tamper - IPV6 空値 ▼) 3 学弦 ▼ 学弦 ▼	<u>英型</u>		修改包設量 10 (二) (二) (二) (二)	随机间隔范围 	×
57月1700年8 导入夏波文件 立起明	ž行	Edit Protocol IPV4 \$7984# wersion III ihl 不 dscp 不 ecn 不 total_ien 不	Tamper IPV6 E値 ▼) 3 接衣 ▼ 接衣 ▼ 接衣 ▼ 使液 ▼	类型 		修改包数量 10 (二) (二) (二) (二) (二) (二) (二)	除机间隔范围 	×
》1月1976年8 号入赛放文件 <u>文田</u> 段	运行	Edit Protocol IPV4 FRAM ini Ā dscp Ā ecn Ā total_ien Ā id Ā	マルビマサルス + 1(2) Tamper 道・) 3 夢波 マ	英型 		修改包設量 10 10 10 10 10 10 10 10 10 10	Rét/Jag隔范田 	×
	žíj	Edit Protocol IPV4 PRS4M version ini 不 dscp 不 ecn 不 total_ien 不 id 不 trag_rsv 不	Cold the de frig) Tamper IPV6 IPV6 Fract マ 3 Fra	类型			酸机间隔范围	×
》月前初以至此 导入要成文件 文团》	£f7	Edit Protocol IPV4 PRS4h version III ini IX dscp IX ccn IX total_ian IX frag_rsv IX frag_rsv IX frag_rsv IX	Cold the de frig) Tamper IPV6 IPV6 IPV5 IO I IP I	<u>类型</u>		修改包数量		×
)) 局の (文件	运行	Edit Protocol IPV4 FR848 version III ini III dscp III con III total_len III itag_rsv III frag_dt III frag_dt III IIII	Cold the de (1)(2) Tamper IPV6 IPV6 IPV5	<u>类型</u>			bt小问隔花眼	
)) 局の 以 生民 局入意改文件 <u>文</u> 目明	蓋行	Edit Protocol IPV4 PRS4 version III ini 不 dscp 不 ecn 不 total_len 不 id 不 trag_rsv 不 trag_uf 不 trag_uf 不 trag_oft 不	マルロビサルム チャリ2 Tamper IPV6 空値 マ) 3 修改 マ)	类型				×
)) 局入類改文件 <u> 文田</u> 1 1 1 1 1 1 1 1 1 1 1 1 1	ž行	Edit Protocol IPV4 FR84th version ihl 茶 dscp 茶 ecn 茶 total_len 茶 id 茶 frag_rsv 茶 frag_rdf 茶 frag_mf 茶 frag_off 茶 tu 花	マルロ(中和点(中))2 Tamper 「IPV6 「空値で) 3 「夢衣マ) 「夢衣マ) 「夢衣マ) 「夢衣マ) 「夢衣マ) 「「「「」」」 「「」」 「「」 「」 「」	英型 			RefLege ·	×
) 局入 要入 要 次 体 文 即	۲	Edit Protocol IPV4 \$7924b version III inl A dscp A ecn A id A frag_rsv A frag_dt A frag_mt A frag_off A ttu A proto A sip A	小品で#Act #102 Tamper IPV6 空値 v) 3 療衣 v) 療衣 v) 夢衣 v)	类型			Béhijikati	
	ي ي ي ي ي ي	Edit Protocol IPV4 学段名称 version inl 方成名称 dscp ccn dscp tda_con tda_con id frag_rsv trag_rnf rag_off sip id	マルロ(中央レチョ)2 Tamper IPV6 管弦 マ 小 小 小 学弦 マ 学 な マ	<u>类型</u>			股机间隔范围	
	五行 五行 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	Edit Protocol IPV4 PR84% version ini Score id frag_fsv frag_fsv frag_fsv frag_fsv frag_fsv frag_ft frag_ff frag	マルロ(中本ムチョ)2 Tamper IPV6 管査 マ 3 夢衣 マ	<u>类型</u>			MAIAIRAZIN	

Ipv4 和 ipv6 的协议篡改目前都已经支持。支持修改的协议字段在列表中可以选择修改方式,包括 3 种方式

IPV4 IPV6

字段名 称	类型	修改包数量	随机间隔范围	*
version	送増 ✓ 不修改 0,100] - [0,100] 固定值 随机值			*
ihl	通道 小豚皮 ♥			
dscp	「不修改 ✔			
ecn	「不修改 ✔			

固定值:将协议中的该参数修改为一个自定义的固定值

随机值:配置一个范围后,参数在该范围内随机改变,每个报文的参数值随机改变 递增:在设置的范围内,该参数按照配置的步长参数,每个报文的参数值依次递增 例如 ipv4 的 ver 参数,对应的是数据报文中的这个部分。

Wireshark · Packet 1 · udp_64_1_1.pcap	-	0 3
> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)		
> Ethernet II, Src: Private_00:00:02 (11:00:00:00:00:02), Dst: Private_00:00:01 (11:	00:00:00:00:01)	
✓ Internet Protocol Version 4, Src: 100.0.0.1, Dst: 100.0.0.2		
(0100) = (Version: 4)		
\dots 0101 = Header Length: 20 bytes (5)		
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
Total Length: 50		
Identification: 0x0000 (0)		
> Flags: 0x4000, Don't fragment		
Time to live: 64		
Protocol: UDP (17)		
Header checksum: 0x3abb [validation disabled]		
[Header checksum status: Unverified]		
Source: 100.0.0.1		
Destination: 100.0.0.2		
> User Datagram Protocol, Src Port: 12345, Dst Port: 1024		
> Data (22 bytes)		
0000 11 00 00 00 00 01 11 00 00 00 00 02 08 00 45 00		
0010 00 32 00 00 40 00 40 11 3a bb 64 00 00 01 64 00 ·2··@·@· :·d···d·		
0020 00 02 30 39 04 00 00 1e ff d3 55 44 50 55 44 5009 UDPUDP		
0030 32 37 30 30 30 30 30 30 44 30 30 30 30 30 44 32 27000000 D00000D2		

lpv4 的 ihl 对应的是数据报文的这个部分:

Wireshark · Packet 1 · udp_64_1_1.pcap -	٥	×
> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)		
> Ethernet II, Src: Private_00:00:02 (11:00:00:00:00:02), Dst: Private_00:00:01 (11:00:00:00:00:01)		
 Internet Protocol Version 4, Src: 100.0.0.1, Dst: 100.0.0.2 		
0100 = Version: 4		
0101=CHeader Length: 10 bytes (5)		
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
Total Length: 50		
Identification: 0x0000 (0)		
> Flags: 0x4000, Don't fragment		
Time to live: 64		
Protocol: UDP (17)		
Header checksum: 0x3abb [validation disabled]		
[Header checksum status: Unverified]		
Source: 100.0.0.1		
Destination: 100.0.2		_
Solition (2) butter)		
> Data (22 Dytes)		
0000 11 00 00 00 01 11 00 00 00 02 08 00 45 00		
0010 00 32 00 00 40 00 40 11 3a bb 64 00 00 01 64 00 -2@.@. :.dd.		
0020 00 02 30 39 04 00 00 1e tt d 3 55 44 50 55 44 50 ···09····· UDPUDP		

lpv4.dscp 对应的是数据报文的这个部分:

Wireshark · Packet 1 · udp_64_1_1.pcap ٥ × > Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) ~ > Ethernet II, Src: Private_00:00:02 (11:00:00:00:00:02), Dst: Private_00:00:01 (11:00:00:00:00:01) ✓ Internet Protocol Version 4, Src: 100.0.0.1, Dst: 100.0.0.2 0100 = Version: 4 ... 0101 = Header Length: 20 bytes (5) Differentiated Services Field 0x00 (DSCP: CS0, ECN: Not-ECT) 0000 00.. = Differentiated Services Codepoint: Default (0)00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 50 Identification: 0x0000 (0) ✓ Flags: 0x4000, Don't fragment 0... = Reserved bit: Not set .1.. = Don't fragment: Set ..0. = More fragments: Not set ...0 0000 0000 0000 = Fragment offset: 0 Time to live: 64 Protocol: UDP (17) Header checksum: 0x3abb [validation disabled] 0000 11 00 00 00 00 01 11 00 00 00 00 02 08 00 45 00 • • • E •

Ipv4.tota_lenl 对应的是数据包的如下报文:

Wireshark · Packet 1 · udp_64_1_1.pcap	-	٥	×
> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)			^
> Ethernet II, Src: Private_00:00:02 (11:00:00:00:00:02), Dst: Private_00:00:01 (11:00:00:00:00:01)			
✓ Internet Protocol Version 4, Src: 100.0.0.1, Dst: 100.0.0.2			
0100 = Version: 4			
0101 = Header Length: 20 bytes (5)			
✓ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)			
0000 00 = Differentiated Services Codepoint: Default (0)			
Total Length: 50			
Identification: 0x0000 (0)			
✓ Flags: 0x4000, Don't fragment			
0 = Reserved bit: Not set			
.1 = Don't fragment: Set			
.0 = More fragments: Not set			
0 0000 0000 0000 = Fragment offset: 0			
Time to live: 64			
Protocol - UDP (17)			
Header checksum 0x3abh [validation disabled]			
			~
0000 11 00 00 00 01 11 00 00 00 00 02 08 00 45 00 ······E·			
0010 00 32 00 00 40 00 40 11 3a bb 64 00 00 01 64 00 2··@·@· :·d···d·			
0020 00 02 30 39 04 00 00 1e ff d3 55 44 50 55 44 5009UDPUDP			
32 37 30 30 30 30 30 30 30 44 30 30 30 44 32 2700000 D0000D2			

以此类推,管理员可以通过 wireshark 工具分析数据包结构来对应系统里的触发条件的变量。 按照变量定义顺序查找 wireshark 样包就可以一一对应上具体字段。目前系统已经预置好了 如下包头的定义:

- 以太网
- 带 VLAN 以太网
- IPV4
- IPV6
- TCP
- UDP

3.10 测试订单

测试订单用来对当前运行及历史的测试订单进行管理。

工程	首页 / 測试订单								
系统配置 ▼									
接入协议 🔻									
网口设置	订单编号	工程名 任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	操作
变量设置	xpro_ns20210715164144_425	RAW_TCP RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:42:00	2021-07-15 16:41:44	日志 洋橋 关联 删除 重新运行
媒体对象	xpro_ns20210715163837_424	RAW_TCP RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:38:54	2021-07-15 16:38:37	日志 洋情 关联 删除 重新运行
客户端 🔻	xpro_ns20210715163525_423	RAW_TCP RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:35:42	2021-07-15 16:35:25	日志 详情 关联 删除 里新运行
关联	xpro_ns20210715163134_422	RAW_TCP RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:31:54	2021-07-15 16:31:34	日志 洋情 关联 删除 里新运行
SBD-FSTM	xpro_ns20210715153129_421	RAW_TCP RAW_TCP_&	工单运行结束	UI创建	成功		2021-07-15 15:31:45	2021-07-15 15:31:29	日志洋情、关联、删除、重新运行
<i>资</i> 国内 年	xpro_ns20210715152617_420	RAW_TCP RAW_TCP_\$	工单运行结束	UI创建	成功		2021-07-15 15:26:36	2021-07-15 15:26:17	日志 洋情 关联 删除 重新运行
报表 ▼	xpro_ns20210715151154_419	RAW_TCP RAW_TCP_V6	工单运行结束	UI创建	成功		2021-07-15 15:12:12	2021-07-15 15:11:54	日志 洋情 关联 删除 重新运行
终端	xpro_ns20210715150933_418	RAW_TCP RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 15:09:51	2021-07-15 15:09:33	日志 详情 关联 劃除 里新运行
	xpro_ns20210715150631_417	RAW_TCP RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 15:06:48	2021-07-15 15:06:31	日志 详情 关联 劃除 里新运行
	xpro_ns20210715150419_416	RAW_TCP RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 15:04:36	2021-07-15 15:04:19	日志 详情 关联 删除 重新运行
	xpro_ns20210715150132_415	RAW_TCP RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 15:01:48	2021-07-15 15:01:32	日志 详情 关联 删除 重新运行
	xpro_ns20210715145938_414	RAW_TCP RAW_TCP_§	工单运行结束	UI创建	成功		2021-07-15 14:59:57	2021-07-15 14:59:38	日志 详情 关联 删除 重新运行
	xpro_ns20210715145527_413	RAW_TCP RAW_TCP	工单运行结束	UI创建	成功		2021-07-15 14:55:46	2021-07-15 14:55:27	日志 详情 关联 删除 里新运行
	xpro_ns20210702091921_253	RAW_TCP RAW_TCP	工单运行结束	UI创建	成功		2021-07-02 09:19:37	2021-07-02 09:19:21	日志 详情 关联 劃除 重新运行
	xpro_ns20210701170402_247	RAW_TCP RAW_TCP	工单运行结束	UI创建	成功		2021-07-01 17:04:19	2021-07-01 17:04:02	日志洋情、关联、删除、重新运行

在测试订单页面,点击 日志 按钮可以查看订单日志。

运行日志 X	
err.log ns-run.stat ipsec.log	
EAL: Detected 8 loore(s) EAL: Detected 1 NUMA nodes EAL: Multi-process socket /var/un/dpdk/rte/mp_socket EAL: Multi-process socket /var/un/dpdk/rte/mp_socket EAL: Probing VFIO support. EAL: Probing VFIO support. EAL: Probing VFIO support. EAL: Prob wive 8008: 100.0 en NUMA socket -1 EAL: Invalid NUMA socket, default to 0 EAL: prob wiver 8008: 100.0 ent_mxnet3 EAL: PCI device 0000:0:0.0 on NUMA socket -1 EAL: PCI device 0000:0:0.0 on NUMA socket -1 EAL: PCI device 0000:0:0.0 on NUMA socket -1 EAL: PCI device 0000:13:0.0 on NUMA socket -1 USERT: INFO: can not open file /dci/pro-ns/fpga ini.fpga disabled testpmd: create a new mubur pol -smult_prod_ socket_0:=:n=15300, size=2176, socket=0 testpmd: create a new mubur pol -smult_prod_ socket_0:=:n=15300, size=2176, socket=0 testpmd: create a new mubur pol -smult_prod_ socket_0:=:n=15300, size=2176, socket=0 testpmd: created a new mubur quot sevel-de: inig_mp_mc USERT: imap port 1 at cores[3 4 5] USERT: imap port 1 at cores[3 4 5] USERT: imap port 1 at cores[3 4 5] USERT: treating mempool global_f_d_mbuf-0 on core 0(size: 8192, obj_size: 2304, priv: 4 cache: 512) USERT: creating mempool global_f_d_mbuf-0 on core 3(size: 10240, obj_size: 46, priv: 4 cache: 512) USERT: creating mempool global_f_d_mbuf-0 on core 3(size: 10240, obj_size: 46, priv: 4 cache: 512) USERT: Creating mempool global_f_d_mbuf-0 on core 3(size: 10240, obj_size: 128, priv: 4 cache: 512) USERT: Creating mempool global_f_d_mbuf_clone3 on core 3(size: 10240, obj_size: 128, priv: 4 cache: 512) USERT: found 2 Ethernet ports USERT: Starting feetwe packet loop on lcore 1, core index 1 USERT: Starting feetwe packet loop on lcore 3, core index 3 USERT: Starting feetwe packet loop on lcore 3, core index 3 USERT: Starting feetwe packet loop on lcore 3, core index 3 USERT: Starting feetwe packet loop on lcore 5, core index 3 USERT: Starting feetwe packet loop on lcore 5, core index 3 USERT: Starting feetwe packet loop on lcore 5, core index 3 USERT: Port 1 Link Up, speed 10	
	1

在测试订单页面,点击按钮可以 详想进入订单详情页面,查看订单的运行状态和订单相关信息。

其中"订单详情"标签,可查看集中呈现的订单详细配置关联信息

工程	首页 / 测试订单管理 / 订单详情
系统配置 ▼	
接入协议	订单详情 监控 负载 关联统计
网口设置	版本 : 1 ▶ 工程信息
变量设置	▶ 客户端关联详情
媒体对象	▶ RAW_ICP_分片教量_正序_V6
客户端 ▼	阿口名: port0 服务端网卡: port1
关联	子网类型: IPv6
	权重:6
测试订单	息用全局负载: 否
报表 ▼	名称: RAW_TCP_分片数量_正序_V6 *****
	※型: 作車
终端	
	▶ Q载
	▶ 运行配置
	》 网を

点击"**监控**"标签,可查看订单运行的实时统计信息,包括客户端/服务端的会话数,tx /rx pps, tx/rx bps, tx/rx pkts 等信息

				Dotou	uch XPRO 云测网络仿真测	则试工具 v2.0R3
	首页 / 測试订单管理 / 监控					
2 1 494						
14310 -	订单详情 监控	负载 关联统计				
设置	12345 6 7					
设置						
	订单执行					
对象	Clobal		Test Olympic (Olimpi)		Test Observ(Ossuer)	
	Giobai		lest stages(client)		Test Stages(Server)	
· #		2024 00 40 00 40 00				
	start_ume	2021-08-19 09:46:08	APP		APP	
	run time	16s	connection/s	0	connection/s	0
	remain time	0s	concurrent	0	concurrent	0
订单	max_core_usage	0%	sessions	300	sessions	300
	port0-dump	write fail 0 other fail 0	requests	300	requests	300
	port1-dump	write fail 0 other fail 0	responses	300	responses	300
			invalid-msg	0	invalid-msg	0
			invite-msg	0	invite-msg	0
			no-len	0	no-len	0
			trans-enc	0	trans-enc	0
			closed no req	0	closed-no-req	0
			closed-ito-tesp	0	closed-no-resp	0
			resp/s	0	resp/s	0
			ssl failed	0	ssl failed	0
			ssl verify err	0	ssl verify err	0
			connect_fail	0	open_fail	0
			min-lat	0	min-lat	0
			max-lat	0	max-lat	0
			avg-lat	0	avg-lat	0
			smin-lat	0	smin-lat	0
			smax-lat	0	smax-lat	0
			smin-avg	0	smin-avg	0
			min_delay	0	min_delay	0
			max_delay	0	max_delay	0
			avg_ooidy	U	avy_uolay	0



点击"负载"标签,可查看图形化呈现的新建会话、并发会话、流速及包速信息

Dotouch XPRO 云测网络仿真测试工具 v2.0R3



在测试订单页面,点击 关联 按钮可以查看订单关联。

则试订单									
8									
单编号		1						创建时间	操作
o_ns20210715164144_425	天联信息						×	2021-07-15 16:41:44	日志洋情关联剧院重新运行
o_ns20210715163837_424	客户端关联						- 1	2021-07-15 16:38:37	日志详情 关联 删除 重新运行
_ns20210715163525_423	关联ID	关联名称	子网名称	网络	动作	负载	- U	2021-07-15 16:35:25	日志洋協美联 删除 重新运行
ns20210715163134_422	1783	RAW TCP 分片数	ipv6	raw top	RAW TCP 分片数	raw top	18	2021-07-15 16:31:34	日志洋情、关联、副除、重新运行
ns20210715153129_421						_ '	- 11	2021-07-15 15:31:29	日志洋情、关联、删除、重新运行
ns20210715152617_420							- 11	2021-07-15 15:26:17	日志洋情、关联、删除、重新运行
ns20210715151154_419							- 11	2021-07-15 15:11:54	日志洋情、关联、删除、重新运行
ns20210715150933_418							- 11	2021-07-15 15:09:33	日志洋情、关联、删除、重新运行
ns20210715150631_417								2021-07-15 15:06:31	日志详情 关联 删除 重新运行
ns20210715150419_416								2021-07-15 15:04:19	日志詳情、关联、删除、重新运行
ns20210715150132_415							- 18	2021-07-15 15:01:32	日志洋情、关联、删除、重新运行
ns20210715145938_414								2021-07-15 14:59:38	日志详情 关联 删除 里新运行
_ns20210715145527_413	RAW_TCP	RAW_TCP	工单运行结束	UI创建	成功	2021-07	-15 14:55:46	2021-07-15 14:55:27	日志 洋情 关联 删除 重新运行

在测试订单页面,点击 删除 按钮可以删除订单。

首页 / 測试订单									
Ø									
订单编号	工程名	任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	操作
xpro_ns20210818180240_819	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-08-18 18:02:59	2021-08-18 18:02:40	日志洋情、关联、删除、里新运行
xpro_ns20210715164144_425	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:42:00	2021-07-15 16:41:44	日志详情、关联、删除、重新运行
xpro_ns20210715163837_424	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:38:54	2021-07-15 16:38:37	日志详情、关联、删除、重新运行
xpro_ns20210715163525_423	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:35:42	2021-07-15 16:35:25	日志详情、关联、删除、重新运行
xpro_ns20210715163134_422	RAW_TCP	RAW_TCP_分	工单运行结合。		×		2021-07-15 16:31:54	2021-07-15 16:31:34	日志详情、关联、删除、重新运行
xpro_ns20210715153129_421	RAW_TCP	RAW_TCP_参	工单运行行确认	要删除吗?			2021-07-15 15:31:45	2021-07-15 15:31:29	日志详情、关联、删除、重新运行
xpro_ns20210715152617_420	RAW_TCP	RAW_TCP_参	工单运行的	20	- Rotar		2021-07-15 15:26:36	2021-07-15 15:26:17	日志详情、关联、删除、重新运行
xpro_ns20210715151154_419	RAW_TCP	RAW_TCP_V6	工单运行的		AL AXIB		2021-07-15 15:12:12	2021-07-15 15:11:54	日志洋情、关联、删除、重新运行
xpro_ns20210715150933_418	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 15:09:51	2021-07-15 15:09:33	日志洋情、关联、删除、重新运行

在测试订单页面,点击按 重新运行 钮可以重新运行订单。重新运行订单时,会询问是否保留原订单数据,

首页	1 / 测试订单										
	05										
	24										
	订单编号	工程名	任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	操作	
	xpro_ns20210818180240_819	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-08-18 18:02:59	2021-08-18 18:02:40	日志洋情关联 删除 重新运行	^
	xpro_ns20210715164144_425	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:42:00	2021-07-15 16:41:44	日志 详情 关联 删除 重新运行	
	xpro_ns20210715163837_424	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:38:54	2021-07-15 16:38:37	日志 洋侍 关联 删除 重新运行	
	xpro_ns20210715163525_423	RAW_TCP	RAW_TCP_分	工单运行结束	UI创建	成功		2021-07-15 16:35:42	2021-07-15 16:35:25	日志 详情 关联 删除 重新运行	
	xpro_ns20210715163134_422	RAW_TCP	RAW_TCP_分	工单运行结合。		×		2021-07-15 16:31:54	2021-07-15 16:31:34	日志 详情 关联 删除 重新运行	
	xpro_ns20210715153129_421	RAW_TCP	RAW_TCP_参	工单运行经是否	保留原用例结果	数据?		2021-07-15 15:31:45	2021-07-15 15:31:29	日志 详情 关联 删除 里新运行	
	xpro_ns20210715152617_420	RAW_TCP	RAW_TCP_&	工单运行结				2021-07-15 15:26:36	2021-07-15 15:26:17	日志 详情 关联 删除 重新运行	
	xpro_ns20210715151154_419	RAW_TCP	RAW_TCP_V6	工单运行的				2021-07-15 15:12:12	2021-07-15 15:11:54	日志 详 情 关 联	

可以根据实际需求选择是否保留,选择完成后,会跳转到订单运行详情页

工程	首页 / 测试订单管理 / 监控		
系統配置			
接入协议 🗸	订单详情 监控 负载 关联统计		
网口设置	1286567		
变量设置	准實开始		
媒体对象	Global	Test Stages(Client)	Test Stages(Server)
客户端 ▼			
关联			
测试订单			
报表 ▼			
终端			

 山上 当提交了多个任务时,会按照排队顺序依次执行排队订单。

3.11 报表

报表模块用来查看各测试订单的汇总统计报表,当前支持11种类型的报表

3.11.1 网口报表

网口报表功能用来从网口维度统计测试信息,包括网口的接收字节数,网口的接收报文数,网口的发送字节数, 网口的发送报文数,网口的工作速率等,可拖拉滚动条查看从网口维度统计的全部信息。

TRUE V	首页 / 报表											
接入协议 🔻												
网口设置	订单编号		Q									
变量设置												
媒体对象												
客户端 ▼					A/7804107	7.00	1.00.11.mlm.+++-	177.14-177-b-	ID NU-berry	10.114.17 L		
关联	ID.	月中端号	网卡名	网卡ID	初始的同	工種ID	接収子口	接收推入	友达子节	双达拔义	两卡速度	
380-43744	1549	xpro_ns202108190	port0	0	2021-08-19 09:46:34	237	204676	1818	212582	2110	1000	Î
約54.11 中	1550	xpro_ns202108190	port1	1	2021-08-19 09:46:34	237	263222	2110	161044	1818	1000	
报表	1547	xpro_ns202108181	port0	0	2021-08-18 18:03:24	237	204676	1818	212582	2110	1000	
网口报表	1548	xpro_ns202108181	port1	1	2021-08-18 18:03:24	237	263222	2110	161044	1818	1000	
测试用例报表	839	xpro_ns202107151	port0	0	2021-07-15 16:42:31	237	204676	1818	212582	2110	1000	
URL统计	840	xpro_ns202107151	port1	1	2021-07-15 16:42:31	237	263222	2110	161044	1818	1000	
应用统计	837	xpro_ns202107151	port0	0	2021-07-15 16:39:19	237	204676	1818	212582	2110	1000	
RTCP报表	838	xpro_ns202107151	port1	1	2021-07-15 16:39:19	237	263222	2110	161044	1818	1000	
RTP报表	835	xpro_ns202107151	port0	0	2021-07-15 16:36:07	237	230476	2118	286982	3310	1000	
RTP详细报表	836	xpro_ns202107151	port1	1	2021-07-15 16:36:07	237	366422	3310	179644	2118	1000	
RTSP报表	833	xpro_ns202107151	port0	0	2021-07-15 16:32:19	237	230476	2118	286982	3310	1000	
CUSP报表	834	xpro_ns202107151	port1	1	2021-07-15 16:32:19	237	366422	3310	179644	2118	1000	+
CUSP用户接入报表			# 20 @ 20 @ @								+	
用户 _{控 入 招志}			共 36 元 20 策/贝 ♥									

3.11.2 测试用例报表

测试用例报表功能用来从测试用例维度统计测试信息,包括该测试用例的执行状态、运行时长、打开会话\关闭 会话数,测试用例中各网口的接收字节数,接收报文数,发送字节数,发送报文数,可拖拉滚动条查看全部信

急。											
工程	首页 / 报表										
系統配置											
接入协议 🗸 👻	订单编号		Q								
网口设置											
变量设置											
煤体对象											
ALCONT AC	ID	订单编号	网卡名	网卡ID	测试用例ID	创建时间	工程ID	动作名称	网络	子网	动作/profile
客户端 🔻	1650	xpro_ns202108190	port0	0	1783	2021-08-19 09:46:34	237	RAW_TCP_分片数	raw_tcp	ipv6	RAW_TCP_u5206u
关联	1651	xpro_ns202108190	port1	1	1783	2021-08-19 09:46:34	237	RAW_TCP_分片数	raw_tcp	ipv6	RAW_TCP_u5206u
測试订单	1648	xpro_ns202108181	port0	0	1783	2021-08-18 18:03:24	237	RAW_TCP_分片数	raw_tcp	іриб	RAW_TCP_u5206u
报表	1649	xpro_ns202108181	port1	1	1783	2021-08-18 18:03:24	237	RAW_TCP_分片数	raw_tcp	ipv6	RAW_TCP_u5206u
网门报表	967	xpro_ns202107151	port0	0	1783	2021-07-15 16:42:31	237	RAW_TCP_分片数	raw_tcp	ipv6	RAW_TCP_u5206u
御計用例据書	968	xpro_ns202107151	port1	1	1783	2021-07-15 16:42:31	237	RAW_TCP_分片数	raw_tcp	ірv6	RAW_TCP_u5206u
	965	xpro_ns202107151	port0	0	1782	2021-07-15 16:39:19	237	RAW_TCP_分片数	raw_tcp	ipv6	RAW_TCP_u5206u
- CITESOLI	966	xpro_ns202107151	port1	1	1782	2021-07-15 16:39:19	237	RAW_TCP_分片数	raw_tcp	ipv6	RAW_TCP_u5206u
应用统计	963	xpro_ns202107151	port0	0	1781	2021-07-15 16:36:07	237	RAW_TCP_分片大	raw_tcp	ірv6	RAW_TCP_u5206u
RTCP报表	964	xpro_ns202107151	port1	1	1781	2021-07-15 16:36:07	237	RAW_TCP_分片大	raw_tcp	ipv6	RAW_TCP_u5206u
RTP报表	961	xpro_ns202107151	port0	0	1780	2021-07-15 16:32:19	237	RAW_TCP_分片大	raw_tcp	іруб	RAW_TCP_u5206u
RTP详细报表	962	xpro_ns202107151	port1	1	1780	2021-07-15 16:32:19	237	RAW_TCP_分片大	raw_tcp	ipv6	RAW_TCP_u5206u
RTSP报表	4	1									
CUSP报表	< 1 2 > 图	第二1页 确定	共 38 条 20 条/页 ✔								

3.11.3 URL 统计报表

URL 统计报表功能统计 订单创建时间,view.idx、网络、子网、动作/profile、请求、响应、view.host、view.path 等信息,可拖拉滚动条查看全部信息。

报表 ▲												
网口报表												
测试用例报表												
URL统计	ID	订单编号	测试用例ID	÷₩	动作/profile	请求	响应	view.host	view.p			
应用统计	10	xpro_ns202104261	640	ipv4	http	10	10	0	/index			
RTCP报表	< 1 > 到第 1 页 确定 共1余 20条/页 ✓											
RTP报表												
RTP详细报表												
RTSP报表												
CUSP报表												
CUSP用户接入报表												

3.11.4 应用统计报表

应用统计报表统计应用协议及收发包字节数, 会话数等。
Dotouch XPRO 云测网络仿真测试工具 v2.0R3

e+ma#P#	88 🚔								
	ID	订邮编号	测试用例ID		工程ID	网络	子网	动作/profile	接收字节
C.96LT	419737	xpro_ns202104261	640	29:10	183	http	ipv4	http	738
HISTELT	419738	xpro_ns202104261	640	29:10	183	http	ipv4	http	738
「CP报表	419739	xpro_ns202104261	640	29:10	183	http	îpv4	http	738
P报表	419740	xpro_ns202104261	640	29:10	183	http	ipv4	http	738
P详细报表	419741	xpro_ns202104261	640	29:10	183	http	ipv4	http	738
SP报表	419742	xpro_ns202104261	640	29:10	183	http	ipv4	http	0
JSP报表	419743	xpro_ns202104261	640	29:10	183	http	ipv4	http	0
JSP用户接入报表	419744	xpro_ns202104261	640	29:10	183	http	ipv4	http	0
户接入报表	419745	xpro_ns202104261	640	29:10	183	http	ipv4	http	0

3.11.5 RTCP 报表

RTCP 报表统计 RTSP 相关执行状态、运行时间、接收字节、接收报文、发送字节、发送报文信息

报表 🔺									
网口报表									
测试用例报表	订单编号	工程ID	网卡ID	测试用例ID	创建时间	网卡名	类型	预期执行时间	执行划
URL统计	xpro_ns202104161	62	1	0	2021-04-16 15:38:16	port1	TCP SRV	1	PASS
应用统计	xpro_ns202104161	62	0	0	2021-04-16 15:38:16	port0	TCP CL	40	PASS
RTCP报表	xpro_ns202104161	62	1	0	2021-04-16 15:34:13	port1	TCP SRV	1	PASS
RTP报表	xpro_ns202104161	62	0	0	2021-04-16 15:34:13	port0	TCP CL	40	PASS
RTP详细报表	xpro_ns202104161	62	1	0	2021-04-16 15:30:34	port1	TCP SRV	1	PASS
RTSP报表	xpro_ns202104161	62	0	0	2021-04-16 15:30:34	port0	TCP CL	40	PASS
CUSP报表	xpro_ns202104161	62	1	0	2021-04-16 15:27:43	port1	TCP SRV	1	PASS
CUSP用户接入报表	xpro_ns202104161	62	0	0	2021-04-16 15:27:43	port0	TCP CL	40	PASS
用户接入报表	xpro_ns202104161	62	1	0	2021-04-16 15:23:06	port1	TCP SRV	1	PASS
终端			版	权所有: 北京触点互动(言息技术有限公司 京ICP	备19037780号		订单未运行	

3.11.6 RTP 报表

RTP 统计报表功能是用来统计 RTSP 协议中 RTP 流信息,统计信息有类型、运行时间、接收字节、接收报文、发送字节、发送报文、视频播放质量

	R 2										
媒体对象	订单编号	工程ID	网卡ID	测试用例ID	创建时间	网卡名	类型	预期执行时间	执行状态	运行时间	接收字节
寄戸端 ▼	xpro_ns202106291	261	0	0	2021-06-29 11:02:05	port0	TCP CL	32	PASSED	45.98	6906600
服务端 🔫	xpro_ns202106291	261	0	0	2021-06-29 11:02:03	port0	TCP CL	32	RUNNING	45.00	6906600
关联	xpro_ns202106291	261	0	0	2021-06-29 11:02:03	port0	TCP CL	32	RUNNING	44.00	6906600
测试订单	xpro_ns202106291	261	0	0	2021-06-29 11:02:01	port0	TCP CL	32	RUNNING	43.00	6906600
报去	xpro_ns202106291	261	0	0	2021-06-29 11:02:01	port0	TCP CL	32	RUNNING	42.00	6906600
	xpro_ns202106291	261	0	0	2021-06-29 11:01:59	port0	TCP CL	32	RUNNING	41.00	6906600
	xpro_ns202106291	261	0	0	2021-06-29 11:01:59	port0	TCP CL	32	RUNNING	40.00	6906600
	xpro_ns202106291	261	0	0	2021-06-29 11:01:57	port0	TCP CL	32	RUNNING	39.00	6906600
URLINGT	xpro_ns202106291	261	0	0	2021-06-29 11:01:57	port0	TCP CL	32	RUNNING	38.00	6906600
应用统计	xpro_ns202106291	261	0	0	2021-06-29 11:01:56	port0	TCP CL	32	RUNNING	37.00	6906600
RTCP报表	xpro_ns202106291	261	0	0	2021-06-29 11:01:55	port0	TCP CL	32	RUNNING	36.00	6906600
RTP报表	xpro_ns202106291	261	0	0	2021-06-29 11:01:53	port0	TCP CL	32	RUNNING	35.00	6906600
DTD洋细胞毒	4	-									

3.11.7 RTP 详细报表

RTP 详细报表是用来统计 RTSP 协议中传输 RTP 流相关信息

MIGH
变量设置
媒体对象
API COLUMN
客户端 マ
服务端 👻
关联
~**
赋订单
报表 🔺
网口报表
80-8 B/5H?=
测试用例报本
URL统计
应用统计
RTCP报表
RTP报表
RIPHANDE
RTSP报表

3.11.8 RTSP 报表

RTSP 报表统计 RTSP 协议中网卡接收数据,包含类型、预期执行时间、执行状态、运行时间、接收字节、发送字 节、请求数、响应数等信息

工程	首页 / 报表										
系統配置 🔻	-										
接入协议 🔫	订单编号		Q								
网口设置											
变量设置											
媒体对象		TRID	RED	36才用AUD	AIRPRIC	网上文	(46 7 F)	初期はつわり回	执行状态	法行时间	接供支持
客户端 ▼	xpro_ps202106291	261	1	0	2021-06-29 11:02:16	port1	TCP SRV	1	PASSED	60.98	33600
服务端 👻	xpro_ns202106291	261	0	0	2021-06-29 11:02:16	port0	TCP CL	32	PASSED	45.98	55500
¥₩											
编制的工作											
12=											
网口版本											
2010/10/10/10/20											
应用统计											
RTCP报表											
RTP报表											
RTP详细报表	4										•
RTSP报表	< 1 > 到篇	1 页 确定 共2分	簽 20 条/页 ✔								
CUEDIR#											

3.11.9 CUSP 报表

Cusp 报表统计 CUSP 协议订单中网卡收发字节数,请求和响应的数量及状态等信息。

接入协议 👻	首页 / 报表	
网口设置		
安堂设置	(7单编号 Q	
媒体对象		
客户端 👻		
服务端 👻	1997 (📤	
关联		无政策
新试订单		
报表		
网口报表		
割试用例报表		
URLMit		
应用统计		
RTCP报表		
RTP报表		
RTP详细报表		
RTSP服表		
CUSP服表		
CUSP用户输入报表		

3.11.10 CUSP 用户接入报表

CUSP 用户接入报表统计 UP 控制口 IP、用户接入口 ID、用户接入协议类型,用户上下线数量,及用户在线数量 等信息

·9 11:8 %									
网口报表	00 a								
测试用例报表									
upi (AX)-	订单编号	J□ID	用户上线次数	用户建立连接次数	用户下线次数	用户在线数	成功获取ipv4数	成功获取ipv6数	接收IAPD数
UKLØGIT	xpro_ns202104261	0000	1000	100	100	100	1000	10000	10000
应用统计	xpro_ps202104261	1000	1000	100	100	100	1000	10000	10000
RTCP报表					100				
PTP据丰	xpro_ns202104261	0000	1000	100	100	100	1000	10000	10000
KTT JK4K	xpro_ns202104261	0000	1000	100	100	100	1000	10000	10000
RTP详细报表									
RTSP报表									
CUSP报表									
	•								Þ
CUSP用户接入报表	< 1 > 到第	1页 确定 非	共4条 20条/页 ✔						
用户接入报表									
终端				版权所有: 北京触点互	动信息技术有限公司 京	CP备19037780号		订单未运行	

3.11.11 用户接入报表

用户接入报表统计 PPPoE 和 DHCP 协议中 用户接入协议类型、用户上线次数、用户建立连接次数、用户下线次数、用户在线数 及 PPPoE 和 DHCP 会话数量 和状态统计。

报表 ▲								
网口报表								
测试用例报表								
URL统计	订申辅号	测试用例ID	创建时间	网卡名	用户接入协议类型	用尸上线次数	用尸建立连接次数	用戶下线次数
di militi i	xpro_ns202103241	1	2021-03-24 17:16:47	port0	PPPOEv4	110	110	0
应用死口	xpro_ns2021032411	1	2021-03-24 11:20:06	port0	PPPOEv4	110	110	0
RTCP报表	xpro_ns202103241	1	2021-03-24 10:59:03	port0	PPPOEv4	0	0	0
RTP报表	xpro_ns202103241	0	2021-03-24 10:46:27	port0	PPPOEv4	110	110	0
RTP详细报表	xpro_ns202103241	0	2021-03-24 10:42:36	port0	PPPOEv4	110	110	0
RTSP报表								
CUSP报表								
	•							Þ
CUSP用户接入报表	< 1 > 到第 1	页 确定 共5条 20条/页	~					
用户接入报表								
终端			版权所有:北	京触点互动信息技术有限	公司京ICP备19037780号	<u>-</u>	订单未	运行

3.12 终端

终端功能是模拟 ssh 登陆仪表服务器后台执行一些查询或者启动关闭服务的操作,便于在电脑未安装 ssh 工具的 情况下对仪表进行维护和检查

服务器		×
+		TT 📤 🛱
名称	IP	操作
ceshi	192.168.2.148	/ 注 接
< 1 > 到第 1 页 确定	共1条 20条/页 🗸	

点击编辑按钮, 输入对应服务器 ssh 连接的相关信息, 点击连接即可远程连接到服务器后台

编辑服务器		×
*名称	ceshi	
*IP	192.168.2.148	
*用户	root	
*密码	dotouch@2020	
* 端口	22	
	立即提交	

右边列表列举了一些常用命令,点击命令后面的执行按钮,即可执行当前操作,操作支持添加、编辑、删除和执 行操作,维护人员可根据自己使用情况进行添加维护

终端 - 192.168.2.148

复制当的连接		
Connecting to 192.168.2.148:22 Connection established.	常用命令	+
Last login: Thu Feb 25 11:28:02 2021 from 192.168.2.22 [root@localhost ~]# /home/ns/xpro-ns -v	名称	操作
xpro-ns v2.9.1 018:16:35, Feb 22 2021, revision:NA,svn:039.qpd::DPUK 19.008.01NS0FLAG:=m64 -ptnread -1/root/qpdk-19.00/110/110 rte_eal/linux/eal/include -march=mative -DRTE_MACHINE_CPUFLAG_SSE -DRTE_MACHINE_CPUFLAG_SSE2 -DRTE_MACHINE_CPUFLAG Macriture CPUFLag_SSE3 -DRTE MACHINE CPUFLAG_SSE4 1 -DRTE MACHINE CPUFLAG_SSE4 2 -DRTE MACHINE CPUFLAG SSE5 -DRTE	重启服务器	🖌 💼 执行
G PCLMULQUQ -DRTE MACHINE CPUFLAG AVX -DRTE MACHINE CPUFLAG RORAND -DRTE MACHINE CPUFLAG FSGSBASE -DRTE MACHINE CPUFLAG F16C - DRTE MACHINE CPUTLAG AVX2 -mno-aes -I/home/xpro-ns.2.9.1/build/include -I/root/dpdk-19.08/x86 64-native-linuxapp-gcc-release/i	查看ns版本	🖊 🍵 执行
nclude /root/dpdk-19.08/x86_64-native-linuxapp-gcc-release/include/rte_config.h _D_NU_SOURCE _I/home/xpro-ns.2.9.1/i nc _I/home/xpro-ns.2.9.1/inc/appl -I/home/xpro-ns.2.9.1/inc/kni_if _I/home/xpro-ns.2.9.1/inc/ring_if _I/home/xpro-ns.2.9.1/inc	重启中间件	2 🗊 执行
/sock -I/home/xpro-ns.2.9.1/inc/appl/sigudp -I/home/xpro-ns.2.9.1/api/generated/c -I/home/xpro-ns.2.9.1/api/generated/xlate -I/home/xpro-ns.2.9.1/3rdparty -I/home/xpro-ns.2.9.1/ext/include -I/home/xpro-ns.2.9.1/ext/ukey/include -I/home/xpro-ns.2.9.1/ext/include -I/home/xpro-ns.	查看网络端口	🖌 💼 执行
<pre>F/stc/cyclonetcp = 1/home/xpro-ns.2.9.1/stc/stc/cyclonetcp/common = 1/home/xpro-ns.2.9.1/ext/stc/cyclonetcp/lpv6_port = 1/home/xpro- ro-ns.2.9.1/ext/stc/ngap = 1/home/xpro-ns.2.9.1/stc/usrsctp = 1/home/xpro-s.2.9.1/stc/usrsctp/netinet = 1/home/xpro-ns.2.9.1/stc/ (usrsct/netinet6.W=W=1)1.Wetrict_prototwores_Wetsign_prototwore_Wetsign_collections_Well_studied6[inition_wetsign_prototwore]</pre>	大页配置查看	/ 宣 执行
ith -Wcast-align -Wnested-externs -Wcast-qual -Wformat-nonliteral -Wformat-security -Wundef -Wwrite-strings -Wdeprecated -Wno- address-of-packed-member -Wmaybe-uninitialized -Werror -DTPG HAVE STATS -DTPG MD DEBUG LOGS -DTPG SW CHECKSUMMING -DWITH UKEY	查看授权	/ 窗 执行
-DNDEBUG -03 -ggdb3 -D_GNU_SOURCE -DXPRO_OPEN_GTPU_TUN -DXPRO_MCI_SIGNAL_QOSRULE (root@localhost ~)# []	ns check	
	查看网卡绑定 本是供温	
	型 相 描 误	
		T MG



4.1 工程

配置参考 3.1

I3_throughput	三 ● MC接入 授权剩余时间:12天13小时11分 时间偏移:0.000
工程	首页/工程
MCI 👻	工程编辑
L3 throughput	1程 MCI接入 ▼ + / 音
运行	描述
测试订单	用户 dotouch@dotouch.com.cn
报表 ▼	
终端	导入工程
	选择文件 重置
	导出工程 (请勿修改导出文件名,否则会导致导入工程失败)
	 • 导出工程

4.2 网口设置

配置参考 3.4 。

I3_throughput	☲ ⊜ MCI接入	授权剩余时间: 12天13小时15分	时间偏移: 0.000			dotouch@dotouch.com.cn ▼	:
	首页 / 网卡						
	网上列車						
网口设置							
L3 throughput		<u>ل</u>					
	port0	port1					
测试订单							
报表 ▼	+ 🖻					177	[
终端	网口名	IP		前缀长度	网关	操作	
				无数据			

4.3 L3 Throughput

L3 吞吐测试设置页面。点击 () 添加 按钮,进入配置页面,可以增加多个配置项,但是只能有一个配置项 处于启用状态。

13_throughput	3	Ξ	● мсi接;	► 授权乗	余时间: 12天	13小时11分	时间偏	≸: 0.000						dotouch@do	otouch.com.cn 👻 🚦
	首页	/ L3	thourghout												
网口设置		⊕ ≱	iba												
L3 throughput															
		9-号	启用	启用擴入	名称	协议						网卡配查			操作
WERTM							网口名	speed	帧长度	起始IP	结束IP	网关	前缀长度	IP步长	
		1	-		norf0<->n	ten	port0	10000000	1514	1.1.1.1	1.1.1.250	3.3.3.1	24	1	10xx23
服表 ▼			-	100	parto p	top	port1	10000000	1514	3.3.3.1	3.3.3.1	1.1.1.1	24	1	1000 C
终祸		2	~		portfor se	ude	port0	11000000	1514	1.1.1.2	1.1.1.200	1.1.2.3	24	1	
		2		28	portop	uup	port1	11000000	1514	1.1.2.3	1.1.2.3	1.1.1.2	24	1	94/101 B19/2
	4	<	> 別第	1 页 建	暄 共2条 20	●页 ✔									•

首页 / L3 throughput / 编辑					
L3 throughput set					
启用接入模式 OFF					
*协议 请选择					~
port_1 p	port_2				
• 网卡	请选择 ▼				
*speed		kbps			
*顿长度		Byte			
IP					
*IP段					
*前缀长度					
* 网关					
- 2 K					
sport					
* 珀東演山					
25 K					
			立即提交重管	L	订单未运行

启用: 是否启用该配置项开关。

启用接入模式:是否启用接入。

协议:选择三层承载协议,支持 TCP 和 UDP。

网卡:选择测试时使用的网卡。

Speed: 设置发包速率

帧长度: 设置数据帧的长度

IP 段:测试时使用的 IP 地址段

前缀长度: 配置该网口 IP 地址的前缀

网关: 配置该网口的下一跳 IP 地址

<u> hort1</u> 设置的网关需要在 port2 设置的 IP 段里。port2 设置的网关需要在 port1 设置的 IP 段里。

步长: IP 端递增步长

起始端口:配置测试时使用端口起始值 结束端口:配置测试时使用端口结束值 步长:端口递增步长

🦺 Port2 设置页面和 port1 一样。网卡需要选择不同的网卡。

4.4 运行

点击

运行页面可以开始运行订单和停止订单运行。

●开始运行 按钮,可以启动订单执行。

I3_throughput		MCI接入 授权剩余			
工程	首页 / 运行				
MCI ~	运行参数				
L3 throughput	运行时长	120	秒		
运行	系统时间	2021-08-19 10:51:36			
测试订单	启动时间	Y-m-d H:i:s.u	() 请选择	~	
报表 ▼		●开始运行			
终端					

运行时长:订单运行时长,单位秒

系统时间:显示当前系统时间

启动时间: 配置订单开始运行时间(距离当前时间需要大于4分钟)。

4.5 订单列表

订单列表页面,可以查看订单当前运行阶段,当前运行状态,运行开始时间,运行时长等。

工程	首	页 / 测试订单									
мсі 👻											
网口设置		Ø									
L3 throughput		订单编号	工程名	任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	操作
运行		13_throughput20210819112541_826	MCI接入		工单运行结束	UI创建	成功		2021-08-19 11:25:59	2021-08-19 11:25:41	日志详情 翻除 重新运行
测试订单											
报表 👻											
终端											

点击 🛤 按钮, 可以查看订单执行日志

	首页 / 測试订单					
网口设置	Ø					
	订单编号	IN: HEAD	~	的间	创建时间	操作
	I3_throughput20210819112541_826	MCG:		9 11:25:59	2021-08-19 11:25:41	日志洋協制除重新运行
测试订单		err.log ns-run.stat ipsec.log	- 1			
		EAL: Detected 8 (cone(s) EAL: Detected 1 NUMA nodes EAL: Multi-process socket /var/unidpdk/ite/mp_socket EAL: Multi-process socket /var/unidpdk/ite/mp_socket	- 1			
经满		EAL Pricing VirDi sundri EAL Pricing VirDi sundri EAL Pricing VirDi sundri EAL Price Virole 2000 CP 000 CP NUMA socket -1 EAL Inviati NUMA socket, default to 0 EAL prote driver 1000 CP 000 On NUMA socket -1 EAL Prote driver 1000 CP 000 On NUMA socket -1 EAL prote driver 1000 CP 000 On NUMA socket -1 EAL prote driver 1000 CP 000 On NUMA socket -1 EAL prote driver 1000 CP 000 on NUMA socket -1 USER1 INFO Can not open file Motoryon-shops all (Egg di sabled testamic arease an even thorp on Influe Motoryon-shops all (Egg di sabled testamic arease an even thorp on Influe Motoryon-shops all (Egg di sabled testamic preferred mempol op a selected mg_mg_mc USER1 inflo Cantor Social -1 USER1 inflo Cantor Remoted Social -1 USER1 inflo Canto				

按钮,可以查看订单运行监控,流速,包速等负载图表。 详情 点击 工程 首页 / 測试订单管理 / 监控 监控 负载 L3 throughput **1234567** *订单运行结束* Global Test Stages start_time curr_time stop_time max_core_usage port0-dump port1-dump 2021-08-19 11:26:16 2021-08-19 11:28:18 2021-08-19 11:28:18 0% write fail 0 other fail 0 write fail 0 other fail 0 port0 port0<->port1 2282ns 20138ns 15669634ns 0 2 120 0 0 0 0 port_pair lantency_min lantency_max trans_fail arp_rxptss pr_typtss pr-typts bc-bps bc-bps bc-bps bc-bps bc-byts pc-kpts pc-kp MCI 0 97,868 150,122,070 98,349 150,864,466

首页 / 测试订单管理 / 负载 负载 监控 包速 流速 流速 bps 白白土 25,000,000 20,000,000 15,000,000 10.000.000 5,000,000 0 11:26:00 11:26:30 11:27:00 11:27:30 11:28:00 11:28:17 8/ B

首页 / 測试订单管理 / 负载



4.6 报表

报表模块用来查看各测试订单的汇总统计报表,L3 Throughout 子系统当前支持 2 种类型的报表

网口报表:参考 3.11.1

工程	首页 / 报表 / 网口报表	ŧ									
MCI -											
网口设置	订单编号		Q								
L3 throughput											
运行											
测试订单	ID	订单编号	网卡名	网卡ID	创建时间	工程ID	接收字节	接收报文	发送字节	发送报文	网卡速度
报表 ▲	1561	I3_throughput20210	port0	0	2021-08-19 11:28:17	217	150122070	97868	148504090	98349	1000
网口报表	1562	I3_throughput20210	port1	1	2021-08-19 11:28:17	217	150864466	98349	147777780	97868	1000
测试用例报表											
终端											
测试用例报	表:参考:	3.11.2									

首页 / 报表 / 用例报表 Q 订单编号 网口设置 m 🛓 执行状态 网卡名 网卡ID ID 订单编号 测试用例ID 创建时间 工程ID 动作名称 类型 运行时间 1661 I3_throughput20210. port0 0 2021-08-19 11:28:17 217 RX_TX_PORT PASSED 122.67 网口报表 1662 I3_throughput20210. port1 2021-08-19 11:28:17 217 RX_TX_PORT PASSED 122.08 测试用例报表

4.7 终端

参考 3.12



第5章 L2 replay 配置指南

5.1 工程

配置参考 3.1

l2_replay	
工程	首页 / 工程
网口设置	
报文捕获	
报文资源管理	工程 XTestApi - + / 面
回放	描述
运行	用户 dotouch@dotouch.com.cn
测试订单	
报表 ▼	
任务列表	
终 <u>端</u>	

5.2 网口设置

配置参考 3.4 , L2 replay 子系统中网口设置页面不需要配置 IP 信息。

	표 📾 XTestApi	授权剩余时间: 12天9小时40分	
工程	首页 / 网卡		
网口设置			
报文捕获	网卡列表	_	
报文资源管理	슬		
回放	port0	port1	
运行			
测试订单			
报表 ▼			
任务列表			
终端			



工程	首页 / 抓包配置							
网口设置								
报文捕获								
报文资源管理								
回放	port0	port1	edit-portu			×		
运行	开始抓包。停止抓包。		开启抓包					
测试订单			抓包大小	20480	М			
报表 🔻	网口	抓包时长(ns)	抓包时长	50	sec (i)		异常包数	丢包款
任务列表 🔻			切片(分段)大小	20480	м			
终端			抓包文件前缀	136_6				
			抓包文件目录	/home/pcap				
			smac时间戳	OFF				
				立即	提交重置			

开启抓包:是否在该网口开启抓包功能

抓包大小: 配置需要捕获报文大小 (单位 M)

抓包时长: 配置需要抓取报文时长 (单位 S), 和抓包大小同时配置, 达到二者其一则停止捕获。

切片/分段大小:配置每个抓包文件保存的大小。默认单位 M

抓包文件前缀: 定义保存的抓包文件前缀名称 (每次进行报文捕获时需要修改前缀名称)

抓包文件目录:配置抓包文件存储的服务器后台目录(如果需要捕获大量报文,建议目录配置在较大的磁盘中)

Smac 时间戳: 配置是否开启高精度时间戳

开始抓包:在该网口上启用抓包订单(详细信息可在测试订单中查看)

5.4 报文资源管理

对网口捕获和手动导入的报文进行分析,以列表和图标的形式展示分析结果

工程	首页	/ 报文资源管理	Đ											
网口设置 报文捕获	包	文件导入 (挂載)	遊盘导入)											
报文资源管理		绝对路径	包文件目录绝对路径	导入										
回放														
	po	ap文件列表												
測试订单		样包名称	样包路径	报文序号	起始时间(ns)	持续时长(ns)	包总数	包大小(bytes)	有无索引	类型	音注	分析	操作	
报表 🔻		prefix_0.p	/home/dump/prefix_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	副除 脅注	分析结果
任务列表 🔻		136_6_0.p	/home/pcap/136_6_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	劃除 雷注	分析结果
终端		136_4_0.p	/home/pcap/136_4_0.pcapng	0	2021-08-03 14:24:11.339239	200039372835	11087678	2147483647	有	网口抓包		分析	劃除 备注	分析结果
		136_1_0.p	/home/pcap/136_1_0.pcapng	0	2021-08-03 13:59:22.619902	200019633281	2220195	1842756824	有	网口抓包		分析	删除	分析结果
		1_4_0.pca	/home/1_4_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	制除 备注	分析结果
		2_3_0.pca	/home/2_3_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	制除 备注	分析结果
		1_3_0.pca	/home/1_3_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	删除	分析结果
		2_2_0.pca	/home/2_2_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	制除 备注	分析结果
		1_2_0.pca	/home/1_2_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	制除 备注	分析结果
		2_1_0.pca	/home/2_1_0.pcapng	0	2021-07-23 13:37:07.79667737	99997632561	0	112	有	网口抓包		分析	劃除 餐注	分析结果

绝对路径:填写服务器后台目录(点击导入按钮,会将该目录下以 pcap 和 pcapng 结尾的报文导入到系统,手动导入的包文件需要点击操作栏下的分析按钮进行分析)

删除:手动删除当前报文分析结果

备注:可以对报文进行备注。

分析结果: 查看当前抓包文件的 speed 曲线统计

5.5 回放

报文快速回放功能,可设置回放倍速和回放次数。回放任务在保存配置后在测试订单任务栏中点击 进行新增回放任务

	首页 / L2 replay	
网口设置	1.2 Replay	海市場印度
报文捕获	all riopray	
报文资源管理	*回放速率倍数	1 范涵: 0.000001~1000000, 不会修改mac时题
回放	*网卡	port0 v
测试订单	- 回放穴数	
报表 🔻	*启动等待时间	0
任务列表 🔻	根据SMAC修	● OFF ① 按照讨议件国际不支持
终端	正时載	
	写入SMAC	① 按照讨次相国的不变持
	回放文件	 通择资源管理器文件 输入文件夹或审文件路径 通择样包 按索引文件回放
		选起资源营营建立文件 (同选多个文件)
		回放文件列表(已造文件可拖披清整文件顺序) 清空文件列表
	*1	/homeipcap/15_4_0.pcapng
		立即提交

回放速率倍速:测试时的发包速率对比源文件的播放速率,如2就是代表以2倍的速度发包

网卡:选择需要进行回放的网卡

回放次数: 配置需要对原包进行多少次的回放

启动等待时间:配置多长时间后进行回放报文,默认单位:秒

根据 SMAC 修正时戳:开启此项,回放时读取 SMAC,根据 SMAC 的值校正 PCAP 报文得到的时间戳,不开启此 开关,直接将 PCAP 报文得到的时间戳作为回放相关的时间戳使用。

写入 SMAC: SMAC 开关,开启时,回放时将时间戳信息写入 SMAC,关闭时,不修改 SMAC

回放文件: 支持"选择资源管理器"、"输入文件夹或者文件路径"、"选择样包","按索引回放"进行回放。

清空文件列表:将当前选择的回放文件清空,进行重新选择

立即提交:将上述配置进行提交保存

👠 只有"选择样包"选项会有速率堆积图

5.6 运行

启动回放订单运行。

系统时间:显示当前系统时间

启动 时间:配置订单开始运行时间(距离当前时间需要大于4分钟)。

工程	首页 / 运行	
网口设置		
报文捕获		
报文资源管理	系统时间 2021-08-19 14:39:45	
回放	启动时间 Y-m-d H:its.u	~
运行	●开始运行	
测试订单		
报表 ▼		
任务列表		
终端		

Dotouch XPRO 云测网络仿真测试工具 v2.0R3

5.7 测试订单

对当前以及历史订单信息进行统计和展示,可进行日志查看、详情查看 和 删除订单信息,重新运行等操作

工程	首	页 / 測试订单管理 / 測试订单									
网口设置											
报文捕获		Ø									
报文资源管理		订单编号	工程名	任务名称	当前运行阶段	来源	当前运行状态	失败消息	运行开始时间	创建时间	攝作
回放		l2_replay20210811143316_802	XTestApi		工单运行结束	UI创建	成功		2021-08-11 14:33:29	2021-08-11 14:33:16	日志 洋情 删除 重新运行
		20210806181626_781	XTestApi		工单运行结束	接口下单	用户主动发起		2021-08-06 18:16:39	2021-08-06 18:16:26	日志 详情 删除
測试订单		20210806181321_780	XTestApi		工单运行结束	接口下单	成功		2021-08-06 18:13:33	2021-08-06 18:13:21	日志 洋債 删除
报表 ▼		20210806161713_779	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-08-06 16:17:26	2021-08-06 16:17:13	日志 洋橋 删除
174701# _		20210804162544_713	XTestApi	网口抓包	工单运行结束	UI创建	用户主动发起		2021-08-04 16:25:55	2021-08-04 16:25:44	日志 洋橋 删除
任务列表 ▼		20210803142354_700	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-08-03 14:24:10	2021-08-03 14:23:54	日志 洋情 删除
终端		20210803141625_699	XTestApi	网口抓包	工单运行结束	UI创建	用户主动发起		2021-08-03 14:16:40	2021-08-03 14:16:25	日志 洋情 影除
		20210803140629_698	XTestApi	网口抓包	工单运行结束	UI创建	失败	USER1: ERROR:write file /home/pcap/1	2021-08-03 14:06:43	2021-08-03 14:06:29	日志 洋情 删除
		20210803135908_697	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-08-03 13:59:21	2021-08-03 13:59:08	日志 洋橋 删除
		20210723140819_646	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-07-23 14:08:43	2021-07-23 14:08:19	日志 洋橋 删除
		20210723135103_645	XTestApi	网口抓包	工单运行结束	UI创建	成功		2021-07-23 13:51:27	2021-07-23 13:51:03	日志 洋情 懸除

只有通过 UI 创建的 回放订单支持 重新运行。

5.8 报表

5.8.1网口报表

网口报表功能用来从网口维度统计测试信息,包括网口的接收字节数,网口的接收报文数,网口的发送字节数, 网口的发送报文数,网口的工作速率等,可拖拉滚动条查看从网口维度统计的全部信息。

工程	首页 / 报表 / 网口报表										
网口设置	_										
报文捕获	订单编号 12_	replay20210811143316_802									
报文资源管理											
回放	89 4										
运行	ID	订单编号	网卡名	网卡ID	创建时间	工程ID	接收字节	接收报文	发送字节	发送报文	网卡速度
测试订单	1521	l2_replay20210811143316_802	port0	0	2021-08-11 14:35:32	126	0	0	8781394418	11087678	1000
报表 🔺	1522	l2_replay20210811143316_802	port1	1	2021-08-11 14:35:32	126	0	0	0	0	1000
网口报表											
測试用例报表											
任务列表 🗸 🔻											
终端											

5.8.2测试用例报表

测试用例报表功能用来从测试用例维度统计测试信息,包括该测试用例的执行状态、运行时长、打开会话\关闭 会话数,测试用例中各网口的接收字节数,接收报文数,发送字节数,发送报文数,可拖拉滚动条查看全部信

息。												
工程	首页	/ 报表 / 用例报表										
网口设置												
报文捕获		订单编号		Q,								
报文资源管理												
回放		n 4										
运行		D	订单编号	网卡名	网卡ID	创建时间	工程ID	炎型	执行状态	运行时间	接收报文	接收字节
测试订单	1	1439	20210803142354_7	port0	0	2021-08-03 14:27:40	126	RX_TX_PORT	PASSED	201.90	11087678	9003147978
报表 🔺	1	1438	20210803141625_6	port0	0	2021-08-03 14:19:17	126	RX_TX_PORT	RUNNING	156.00	11047207	8964596888
网口报表	1	1437	20210803140629_6	port0	0	2021-08-03 14:09:20	126	RX_TX_PORT	RUNNING	158.00	10610655	8605812100
测试用例报表	1	1436	20210803135908_6	port0	0	2021-08-03 14:02:56	126	RX_TX_PORT	PASSED	201.90	2220195	1802793216
任务列表 🗸 🗸	1	1340	20210723140819_6	port0	0	2021-07-23 14:09:50	126	RX_TX_PORT	PASSED	51.90	0	0
终端	1	1341	20210723140819_6	port1	1	2021-07-23 14:09:50	126	RX_TX_PORT	PASSED	51.90	0	0
>< 300	1	1338	20210723135103_6	port0	0	2021-07-23 13:52:29	126	RX_TX_PORT	PASSED	51.90	0	0
	1	1339	20210723135103_6	port1	1	2021-07-23 13:52:29	126	RX_TX_PORT	PASSED	51.90	0	0
	1	1336	20210723134041_6	port0	0	2021-07-23 13:42:08	126	RX_TX_PORT	PASSED	51.90	0	0
	1	1337	20210723134041_6	port1	1	2021-07-23 13:42:08	126	RX_TX_PORT	PASSED	51.90	0	0

5.9 终端

工程	首页 / 报表 / 用例报	表							
网口设置									
报文捕获	订单编号			服务器		×			
报文资源管理				+		TH 4 6			
回放				名称	IP	操作			
运行	ID	订单编号	网	覃阳峰	192.168.2.142	/ 11 注接			
测试订单	1439	20210803142354_7	pc	< 1 > 到第 1 页 确定	共1条 20条/页 ✔				
报表 🔺	1438	20210803141625_6	pc						
网口报表	1437	20210803140629_6	pc						
测试用例报表	1436	20210803135908_6	pc						
任务列表 🗸 🔻	1340	20210723140819_6	pc						
终端	1341	20210723140819_6	pc						
	1338	20210723135103_6	pc						
	1339	20210723135103_6	po						
	1336	20210723134041_6	pc						
	1337	20210723134041_6	pc						
	1334	20210723133649_6	pc						
	1335	20210723133649_6	pc						

第6章 Attack 配置指南

L3 replay 子系统在使用上与 xpro_ns 子系统基本一致,在测试模式上采用双臂模式,只是在动作协议支持上增加 了 l3 replay、ddos 和 attack play 类型,背景流与 xpro_ns 一致。此部分只介绍与 xpro_ns 子系统增加的 3 中协议 部分。

6.1 工程

配置参考 3.1

6.2 系统配置

配置参考 3.2

6.3 接入配置

配置参考 3.3

6.4 网口配置

配置参考 3.4

6.5 变量设置

配置参考 3.5

6.6 媒体对象

配置参考 3.6

6.7 客户端

6.7.1客户端子网配置

配置参考 3.7.1

6.7.2客户端网络配置

配置参考 3.7.2

6.7.3客户端负载配置

配置参考 3.7.3

6.7.4客户端动作配置

a) ATTACK_PLAY 配置方法

attack_play 将系统集成进来的攻击库文件按照一定的配置规则进行仿真攻击,可用来检测被测设备的安全性。

				Dotoucn XPRO 云测网络仿具测试工具 V2.0R				
	×	attack play		ATTACK_PL	AY	~	系统攻击流	
ATTACK_PLAY Parameters	分片							
*启用ip轮换:								
*类型:	插放次数 ∨							
等待时间(s):	0							
*播放次数:	1							
*播放速率(倍数):	10000							
播放间隔(ms):	5000							
启用5元组日志记录:	 ✓ 							
启用重传:								
一级目录:	威胁对抗能力验证、	 						
二级目录:	工业互联网 🗸							
*攻击文件列表(已选文件中	可拖拽调整文件顺序)	清空文件列表	译文件					
1	远程代码执行/漏洞利用	月/2004-1315	甸					
2	远程代码执行/漏洞利用	月/10-061	Ē					
3	域提权/漏洞利用/14-0	68	Ē					
4	远程代码执行/漏洞利用	月/09-050	Ē					

启用 ip 轮换: 是否开启 ip 轮换, 不开启则所有的的攻击报文只默认使用子网配置中的第一个源/目的 ip 进行仿 直。

类型:播放类型,包括按时间和按次数播放两种,配置按时间播放时设置时间后,在设置的时间里所选的攻击文 件顺序轮播,时间结束时结束测试;配置按次数播放时,设置播放次数后,所选文件轮流播放该次数后结束测 试.

等待时间: 配置启动等待时间

播放次数: 配置需要播放多少次报文

播放速率:测试时的发包速率对比源文件的播放速率,如2就是代表以2倍的速度发包。

播放间隔:两次播放之间的间隔时间

启用五元组日志记录: 配置是否开启五元组日志记录

启用重传: 配置是否开启 tcp 重传

一级目录: 攻击库文件以及目录

二级目录: 攻击库文件二级目录

攻击文件列表:显示当前选择后的攻击库文件

b) L3 replay 配置方法

L3 replay 回放功能用来回放基于用户自主上传的 pcap 包,将报文按照条件清洗后,仿真模块会自动构建 4 层的状态信息,修改源和目的 ip 地址进行回放。

Dotouch XPRO 云测网络仿真测试工具 v2.0R3

	√ ×	I3_replay	L3_REPLAY	~	
	1	attack_play	A	ITTACK_PLAY	系统攻击流
3_REPLAY Parameters	分片				
"启用ip轮换:					
类型:	播放次数 ~	ſ			
等待时间(s):	10				
"播放次数:	1				
"播放速率(倍数):	10000				
播放间隔(ms):	500				
启用5元组日志记录:					
启用重传:					
"回放文件列表(已选文件	牛可拖拽调整文件)	顺序) 清空文件列表 选择文件			
1	6045e8da188f	5-11277-4-clean.pcap	ī		

启用 ip 轮换:每一次文件发送时使用的 ip 地址在子网配置的网段中轮换

类型:播放类型,包括按时间和按次数播放两种,配置按时间播放时设置时间后,在设置的时间里所选的 攻击文件顺序轮播,时间结束时结束测试;配置按次数播放时,设置播放次数后,所选文件轮流播放该次 数后结束测试。

等待时间:配置启动等待时间,开始进行测试

播放速率:测试时的发包速率对比源文件的播放速率,如2就是代表以2倍的速度发包

播放间隔:两次播放之间的间隔时间

启用五元组日志记录: 配置是否开启五元组日志记录

启用重传: 配置是否开启 tcp 重传

回放文件列表:在系统配置-L3 回放库管理页面导入的自定义 pcap 文件,可以选择一个,也可以选择多个

c) Ddos 配置方法

	~	×	ddos-icmp-ping-flood	DDOS V	
	1	[*] 🔟	http	HTTP	
	1	* W	I3_replay	L3_REPLAY	
	-	* 1	attack_play	ATTACK_PLAY	系统攻击流
DDOS Para	meters				
*运行时间(s):	12			
*启动等待时	时间(s):	10			
*每秒包数:		1			
*回放样包		/var/www/KODExplo	rer/data/User/demo/home/pcap-builder/icmp-I 选择样包		

运行时间: 配置 ddos 攻击运行时间

启动等待时间:配置启动等待时间,开始进行测试

每秒包数: 配置 ddos 每秒攻击的包数

回放样包:选择需要进行攻击的 ddos 样包(可以根据包构建器进行灵活配置对应的 ddos 攻击包构建,例如: ddos-icmp-ping-flood、ddos-tcp-syn-flood、ddos-udp-flood、ddos-udp-port-scan、arp-flood、ddosevasive-udp)

d) Virus_attack 配置方法

	+		名称		协议				
	~ ×		virus_attack		VIRUS_ATTACK	~			
	1		http		HTTP				
Common	Common VIRUS_ATTACK Para 需要先在服务端profiles配置好承载协议,如: http								
*选择承载协议	选择承载协议: Intp v 0								
*病毒文件:	清空文件列表 选择文件								
URI:	/1	文件:	test.txt						
	-								
URI:	/2	文件:	running.json	I					

选择承载协议:病毒库承载的应用协议,目前只支持承载 http 协议
清空文件列表:清空当前选择的文件列表
选择文件:选择病毒库文件
URI:URI必须和客户端 URI,服务端 URI 保持一致
文件:病毒库文件(双臂只支持一个病毒库文件,双单臂可以配置多个病毒库文件)

6.8 关联

配置参考 3.9

6.9 测试订单

配置参考 3.10

6.10 报表

配置参考 3.11 报表

6.11 包构建器

按照规则进行数据包的构造,构造的包用于 ddos 攻击中样包,可按照模板中的包进行编辑保存样包。

数据包构建器 超增模版			l j	
名称: kmp 保存文件名称	PCAP!	列表:		
> Pcap Header (文件头24B)	ID) 名称	创建时间	操作
> Packet Header (数据包头16B)	48	B icmp	2021-03-04 18:4	编辑 下载
> Ethernet (以太网14B)	45	5 tcp-example	2021-03-02 14:5	編輯 下载
> IP (互联网协议20B)	44	4 evasive-udp	2021-02-24 13:3	編輯 下载
	43	3 arp-flood	2021-02-24 13:3	編輯 下载
	42	2 udp-port-scan	2021-02-24 13:3	编辑 下载
> File 2018	41	1 udp-flood	2021-02-24 13:3	編組 下载
	40	0 tcp-syn-flood	2021-02-24 13:3	編輯 下载
	<	1 > 到第 1 页	确定 共7条 20条/页	₫ ✔

6.12 终端

配置参考 3.12

工程	首页 / 工程	
系統配置	-	
接入协议 🔻	▼ I程 virus_attack v 服务器	×
网口设置	模式 双单母	8 4 8
变量设置	業型 互联网 名称 IP 生	最作
媒体对象	専団峰 192.168.2.142 🖊	産業
客户端 ▼	★ (1) > 到第 (1) 页 (論定) 共1条 20条页 ◆	
服务端	■ 用户 datauch@datauch.com.cn	
关联		
测试订单	导入工程	
报表 🔻	▼	
包构建器		
终端	导出工程 (诸勿修政导出文件名,否则会导致导入工程失效)	
	④每出工程	

第7章 RFC2544 配置指南

RFC2544 子系统与 xpro_ns 子系统配置基本一致,用于配置常规协议背景流,与 2544 配合使用,单独的 2544 配 置在关联---RFC2544 中进行配置,且测试 2544 功能必须使用专用的 fpga 加速网卡。

7.1 工程

配置参考 3.1

7.2 系统配置

配置参考 3.2



配置参考 3.3

7.4 网口配置

配置参考 3.4

7.5 变量设置

配置参考 3.5

7.6 媒体对象

配置参考 3.6

7.7 客户端

7.7.1客户端子网配置

配置参考 3.7.1

7.7.2客户端网络配置

配置参考 3.7.2

7.7.3客户端负载配置

配置参考 3.7.3

7.7.4客户端动作配置

配置参考 3.7.4

7.8 关联

关联配置项用来绑定最终客户端的各项配置, 包括客户端关联页和 RFC2544 关联页, 分别绑定前面配置的客户端各项参数。

客户端关联	RFC2544			
批量复制				
暂只支持单关联				
	+	"名称	"测试模式	流量拓扑
	✓ ×	rfc-2544-吞吐-ipv4-l2	L2交换模式 ¥	双向
Pages: First Pr	rev 1 2 2 of 2			
基本配置	网口配置 吞吐量配置			
*运行时长(s):	20			
"拖尾时长(s):	1			
*使能地址学习	9: 学习一次 × 武项			
吞吐量测试	. 🗹			
背靠背测试	: 0			
时延测试				
丢包率测试				

基本配置:

运行时长:运行时长,订单总共的运行时长=测试次数*时长*帧长度的个数+运行时长

拖尾时长: 订单结束之前的拖尾时长

使能地址学习: 配置 mac 地址学习时只学习一次还是每次测试都学习

选择测试项:	支持吞叶量、	背靠背、	时延和丟包率

基本配置 网口配置	吞吐量配置
报文类型: ip 接口地址数量: 10 「例卡选择	
源接口网卡:	
目的接口网卡:	
和置链路层	
MAC地址:	00:00:42:01:01:1A
接口内跳变步长:	00:00:00:00:01
端口间跳变步长:	00:00:10:00:00
*配置网络层 *1Pv4地址	
IPV4地址:	1.1.1.5
接口内跳变步长:	0.0.0.1
端口间跳变步长:	1.0.0
IPv4网关:	1.1.1.1
网口配置:	
报文类型 :支	持 ipv4 和 ipv6
校内山山山半月	

接口地址数量:接口地址数量(目前版本最大支持 80个地址跳变,超过 80的部分无效)

网卡选择:选择需要进行 2544 测试的源和目的接口网卡

配置链路层: 配置链路层 mac 地址规则

配置网络层: 配置 ipv4 或者 ipv6 网络层地址规则

基本配置 网口配置	吞吐量配置
*测试时长	
测试次数:	1
测试时长:	
时长:	
*帧长度(字节)	
自定义:	64,128,256,512,1024,1280,1]多个以英文逗号分隔①
*负载	
速率下限(%):	10
速率上限(%):	100
初始速率(%):	10
测试精度(%):	10
测试精度(%):	10

吞吐量配置:

测试次数: 配置需要进行测试的次数

测试时长:选择按照时长或者突发个数进行测试

时长:需要测试的时间

帧长度: 配置测试的帧长度, 支持单个或者多个

速率下限:二分法探测的速率下限

速率上限:二分法探测的速率上限

初始速率:二分法探测的初始速率

测试精度:二分法探测结束的速率标识

7.9 测试订单

Dotouch XPRO 云测网络仿真测试工具 v2.0R3

配置参考 3.10



配置参考 3.11 报表