



Supernova 测试仪 SSL 卸载用例说明

网测科技

2022/01/29



目录

引言	3
1.配置负载均衡,并启用 ssl 卸载功能	4
2.配置 Supernova 测试仪	6
3.运行用例	8
4.报文验证	8
5.HTTPS 并发用例特殊配置	10



引言

Supernova 测试仪支持 HTTPS 用例的 SSI 卸载功能,只需要在卸载 ssl 设备上配置好即可。除 https 并发用例外,测试仪上不需要做任何其它特殊配置, https 并发用例在"参数" 中有启用 ssl 卸载功能按钮,打开后可使并发连接数量的范围*2。

以负载均衡设备举例说明:



1.配置负载均衡,并启用 ssl 卸载功能

1) 使用浏览器打开 FortiGate 防火墙, 依次点击系统管理→接口, 选中 want1 编辑, ip 地 址/网络掩码与测试仪连接的客户端对应, 点击确定, 保存成功。

FortiGate 140D	3	② ③ F
系统管理		編組出
● ● 面版 ● <u>●</u> 网络 ● <u>第日</u> ● 路由 ● DNS	接口名称 別名 连援状态 类型	wan <mark>i@6:58:0E:35:CD:34)</mark> 与测试仪port1口连接的下一跳mac地址 <u>Benn</u> o 物理集口
- 数据包捕获 日 圖 配置 8 16 管理员设置	地址模式 IP地址/网络掩码	● 自定义 ○ DHCP ○ PPPoE ○专用于FortiAP/FortiSwitch [111.1.1.1/255.255.25.0 客户端子网ip
● ፪ 证书 ● 團 监视器	管理访问	☑ HTTPS ☑ PING ☑ HTTP ☑ FMG-访问☑ CAPWAP ☑ SSH ☑ SNMP ☑ TELNET
	DHCP服务器	□ 周用
	安全模式	None
	设备管理 检测并识别设备	
	监听 RADIUS 账单满息 附加的IP地址 注释	□
	管理状态	 ● ○ 已息用 ○ ○ 未息用 検定 取済
第略		
防火墙对象		
安全配置		
用户&设备		
日志与报告		

2) 选中 want2 口编辑, ip 地址/网络掩码与测试仪连接的服务端对应

FortiGate 140D	3-	
系统管理		编辑接口
● ● 回版 ● <u>第</u> 网络 ● 路由 ● DNS	接口名称 別名 连接状态 类型	wan208:58:0E:35:CD:35) 与测试仪连接的服务器端口port2子网ip [port2 巴图用 ● 物理第□
 数据包捕获 ● 圖 配置 ● 圖 管理员设置 	地址模式 IP地址/网络掩码	● 目定义 〇 DHCP 〇 PPPee ○ 专用于FortiAP/FortiSwitch 222.1.1.1/255.255.255.0 与测试仪连接的服务器port2子网掩码
● ፪ 证书	管理访问	☑ HTTPS ☑ PING ☑ HTTP ☑ FMG-访问 ☑ CAPWAP ☑ SSH ☑ SNMP ☑ TELNET
	DHCP服务器	□ 启用
	安全模式	None 🗸
	设备管理 检测并识别设备	
	监听 RADIUS 账单消息 附加的IP地址 注解	
	管理状态	◎ 〇 已回用 ○ ○ 未回用
		783 <u>C</u> HAUPS
第略		
防火墙对象		
安全配置		
用户处设备		
日志与报告		



Supernova 测试仪 SSL 卸载用例说明

3) 配置虚拟服务器信息,点击防火墙对象→负载均衡→虚拟服务器,点击新建,按测试需 求填写名称、类型、接口以及虚拟服务器 IP 和端口信息,点击"确定"回到首页新增一条。

FortiGate 140D	9		(2) 在线帮助	
系统管理 第略 防火增对象 中 🔤 地址	名称	HTTPS 新禮祭務 「P 」 wani ~		
 □ □ 前用表 □ □ 前用表 □ □ 清量控制 □ □ 清量控制 □ □ 清量控制 □ □ 清型均衡 	虚拟服务器IP 虚拟服务器端口 负载均衡方式 保持方式 HTTP多路复用	111.1.1.223 代理服务器ip地址 ◎ 薄IP hash マ 天 マ ◎ 多个HTTP博求回应共用一个TCP连接		
 ● <u>國務務務</u> ● 真实服务器 ● 建東检查 ④ 圖 监视器 	SSL卸载 证书 健康检查	● 供持套户稿IP 套户稿<>>FortiGate ▼ Fortinet_CA_SSLProxy ▼ 可用 成员		
	注释	■入注释 輸入注释 輸入	取消	

4) 配置真实服务器,选择已配置的虚拟服务,填写 IP 地址、端口信息,点击"确认"新增一条真实服务器信息。

FortiGate 140D		2 在线帮助 向	♀ ↓ <	F
系統管理 第語 防火信引象 ● □ 地山 ● □ 地山 ● □ 地山 ● □ 池山 ● □ 池山 ● □ 読券 ● □ 読み ● □ 読知 ● □ 査知時 ● □ 査知路 ● □ 査知路 ● □ 重知服務	虚拟服务器 HTTPS_新建服务 □配置的过的虚 PP地址 222.1.1.200 第0 役里 1 最大连续数 0 HTTP主机 積式 活动 ▼	编组真实服务器 <mark>拟服务器名称</mark> b址		
安全配置 用户&设备 日志与报告				

5) 配置一条从客户端到服务器端的策略, 依次点击策略→策略→策略, 点击"新建", 目的 地址为已配置的虚拟服务器, 其他按测试需求进行配置。

FortiGate 140D	3-			② 在线帮助	() 向导	注销	F
系统管理			编辑输出策略				
策略	策略子类型	◎地址 ○ 用户认证 ○ 设备认证					
· [] 策略	流入接口	wan1 (port1) 与测试仪	客户端连接的防火	、墙端口			
·····································	源地址 流出接口	e all wan2 (port2) 与测试化图	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	「橋淀口			
	目的地址	● HTTPS_新建服务 虚拟服务					
- SSL/SSH检测	时间表	always	- HH				
🖬 🛄 监视器	服务	S ALL	0				
	动化恒	✓ ACCEPT	*				
	一 启用NAT						
	日志纪录选项						
	○ 无日志						
	● 记录安全事件日志						
	○ 记录全部会话日志						



2.配置 Supernova 测试仪

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

◎ 网测科技 netitest.com	日 田例 ジ	2 · · · · · · · · · · · · · · · · · · ·	医腔	报告	系统	移動	admin	V21.12.11 SL	ipernova-20C
网关设备测试 ② 53	HTTPS新数	ŧ							
 ● 代理设备测试 ● ● HTTP/HTTPS/HTTP2 	获取受测设备新 次完整的HTTPS	建HTTPS会话的最快速率 涂话。	B. 每个虚拟用户	建立一条TCP连接	ŧ,并进行SSL题	【手连接,完成	HTTPS事务(发送请求	和接收回应),最后关闭连接。	再新建TCP连接并包含一
HTTP	用例列表	选择用例选项							
>新建服务 → 并发服务	+ 端加		IP版	本 ● v4 ○	v6 〇 混合				2 刷新
> 请求服务 > 吞吐服务	□ 编号	L	受测设备工作模: 网络配:	 代理模式 置 默认模板 	· 0	1	4	端 克隆 详细信息	9月出 历史记录
HTTP2 RTSP/RTP/RTCP			講口绑	è 🗆					
 % Stream/UDP/TCP ■ 4-7层协议仿真 					确定	取消			

2) 点击确定,进入用例配置界面,配置子网信息。

	▼ /除川山屋1火土の1丁1		▼源加遷秋王机子
第1个虚拟主机子网	自移除主机子网 ◎禁用主机子问	第1个虚拟主机子网	自移除主机子网 ◎禁用主机子
虚拟主机子网主机位地址或范围	111.1.1.2 模拟客户端ip地址或范围	虚拟主机子网主机位地址或范围	■ 222.1.1.200 真实服务器ip地址。
	医料主机的主机地址泡園、毎个P地址模拟一个主机		虚拟主机的主机地址论图,每个IP地址模拟—个主机
CENCE OF 1 Manual	24 虚拟主机子网掩码长度, IPv4范围0-32, 也支持255.255.255.0的格 式, IPv6范围0.128-	100 L OUT WILL	■ 24 虚拟主机子网播码长度,IPv4范围0-32,也支持255.255.255.0的格 式。IPv6范围0-128-
虚拟主机子网网关	111.1.1.1 与客户端连接的防火墙子网ip地址	虚拟主机子网网	₹ 222.1.1.1 与服务器连接的防火墙子网ip地
	虚拟主机子网的下一跳网关,禁用边界网关时有效,启用时在边界网 关中配置		虚拟主机子网的下一跳网关,禁用边界网关时有效,启用时在边界网 关中配置
虚拟主机子网VLAN	1 🛛 🕜	虚拟主机子网VLA	N 1
	虚拟主机子网vLAN,禁用边界网关时有效,启用时在边界网关中配 置		虚拟主机子网VLAN,禁用边界网关时有效,启用时在边界网关中配 置
代理服务IP地址	111.1.1.223 虚拟服务器ip地址	虚拟主机模拟角的	▶ 只模拟服务端 ✓
	代理设备配置的虚拟服务器IP地址		虚拟主机测试过程中模拟的角色,可以选择只模拟客户端/只模拟服 务彉/同时模拟客户绩和服务靖
虚拟主机模拟角色	只模拟客户端 >		
	虚拟主机测试过程中概拟的角色,可以选择只概拟客户谱/只概拟服 务强/同时模拟客户端和服务端		
服务端所在端口	port2 🗸		

3) 配置下一跳 mac 地址。

安 白端		7	肥久 総		
porti			nort2		
蒙用 <u>蹒口</u>		MAC 68:91:d0:63:4c:bc	⊘ 萘用端口		MAC 68:91:d0:63:4c
网络配置 CPU核绑定 限速	抓包 网卡设置		网络配置 CPU核绑定	限速 抓包 网卡设置	
惠率与MAC			速率与MAC		
速率探测方式	自动协商 🗸		速率	探测方式 自动协商	~
	当使用某些模块和线缆无法自动探测到速率的	」 封,请使用手动指定		当使用某些模块和线缆无法m	自动探测到速率时,请使用手动指定
請口设置速率	1000	1	第日	设置速率 1000	
	请口要设置的速率,当速率探测方式为手动指	」 能定时设置,单位Mbps		第二要设置的速率,当速率	深则方式为手动指定时设置,单位Mbps
MAC伪装设置	A2:01	0 0	MAG	伪装设置 A2:02	0
	的转MAC的前两个字节(第一个字节的最低位	』 不能为1)		。 伪装MAC的前两个字节(第一	个字节的最低位不能为1)
講口指定MAC地址	68:91:d0:63:4c:bc	0	端口指定	MAC地址 68:91:d0:63:4c:bd	
	发送报文将使用指定的MAC地址,而不用网+	上 目的物理MAC地址		发送报文将使用指定的MAC	地址,而不用网卡的物理MAC地址
下一跳MAC地址获取方式	输入下——跳MAC地址 🗸 🗸		下一跳MAC地址	获取方式 输入下一跳MAC地址	~ 🗹
	与测试仪相连的下一跳满口的MAC地址的获取	」 取方式		与测试仪相连的下一跳满口的	的MAC地址的获取方式
下一跳网口的MAC地址	08:58:0E:35:CD:34 与测试仪安白	端连接的防火墙m	actitutul 下一跳网口的	MAC地址 08:5B:0E:35:CD:35 与	测试仪服务器端连接的ma



4) 点击客户端,配置代理或负载设备端口。

■ 网关设备测试 🕢	(54)	基本信息(HTTP	S新建)	
◎ 代理设备测试 ?		用例名称	HttpsCps_Proxy_admin_20220128-1	6:42: 测试时长 (时分秒) 0 : 1 : 0
HTTP/HTTPS/HTTP2			合法字符类型: A-Z / a-Z / 0-9 / : / - / _ (不支持中文符号) 测试在配置时长后自动结束,测试时长不能超过999小时
HTTP	0			
+ HTTPS		网络 人参	数 🔻 客户端 【 服务器	
>新建服务			渡端口范围	10000-65535
> 并发服务				范围: 1,000 - 65,535
> 请求服务			代理或色载设备谱口	
> 吞吐服务				范围: 0 - 65,535
HTTP2			客户端关闭模式	Reset
RTSP/RTP/RTCP				TCP关闭连接的方式,可以是fin三路挥手,也可以直接发reset报文关闭
% Stream/UDP/TCP		SSL洗项		
■ 4-7层协议仿真				
⊙ 工控协议仿真			静默天闭	
△ 数据流量模型			台泊的eel 形本	
目の田服祭測法の			JUFFEJSSLAK-	SSL版本,每个SSL版本对应的算法不一样
			证书认证方式	● 不认证 ○ 单向认证 ○ 双向认证
□ 終端客尸測试 €				SSL握手阶段,服务器发送证书,但客户请不对证书内容进行认证
♥ 系统安全测试 Ø			证书认证失败的处理	● 终止SSL握手,断开socket连接 ○ 报措并退出程序运行
ピ 网络流量分析 🕢				选择SSL证书认证失败时的操作
			SSL加密套件	选择所有 取消所有 🕗
				AES128-SHA

5) 配置报文捕获查看用例运行报文交互过程。

网络设置						配置端口组
8户端		🧭 💭	服务端			
port1			port2			
美用端口		MAC 68:91:d0:63:4c:bc	◎ 禁用講口			MAC 68:91:d0:63:4
网络配置 CPU核绑定 限速	抓包 网卡设置		网络配置 CPU核能		柳色の未没量	
包			抓包			
协议类型	全部 🖌			协议类型	全部	
	请选择协议的类型,无表示不启用抓包				请选择协议的类型,无表示不启用抓包	
IP地址				IP地址		1
	源IP地址或者目的IP地址,例如17.1.1.2				源IP地址或者目的IP地址,例如17.1.1.2	
第日				洲口		
	源講口或者目的講口,例如80				源講口或者目的端口,例如80	
Pcap文件大小				Pcap文件大小		1
	pcap文件大小, 0 - 2000MB (默认)				pcap文件大小, 0 - 2000MB (默认)	Ê D
捕获包数	10000			捕获包数	10000	
	范围:0-6000000(默认)				范围:0-600000((()()))	L'A

6) 用例编辑完成后,可以点击启动直接运行用例,也可以点击保存,保存用例配置。

🚫 M测科	支 m		一 资源	副 对象	这 些控	後告	系统	東 帮助 adm	in	V21.1	2.11 Su	perno	va-200
📕 网关设备测试 😧	63	HTTP	S新建										
♥ 代理设备测试 ♀		井取岳御	心多新神山エエロマイ	〉活的最快速家	每个虑的国	白碑立冬TCD社	培 - 并进行eei 据毛油		冬/岩法津谷和诗小	(同成) 長の	- 关闭法接 - 1	Fair Topit	读并何令
HTTP/HTTPS/HTTP2		次完整的	HTTPS会话。		49 1 /2219/1		18, / 21133612-742	1327 7500/1111 0 9 4	70 (XXX2 HH-1 YH-13KH				DR/IGA
▶ HTTP	0												
► HTTPS		用例列	康										
>新建服务													_
> 并发服务		+ 増加	1 前册所	- 🛃 导)	λ								2刷新
> 请求服务				landa Trian	-	an ata			14.05		-		
> 吞吐服务		U	编号 运行	任务列表	用户	名子			编辑	兒隆	详细信息	合田	历史记录
► HTTP2			1 5		admin	HttpsCps_Pro	oxy_admin_20220128	-16:13:45	1	2		2	0



3.运行用例

 点击运行按钮运行测试用例,展示监控数据页面,用例运行结束,可以点击下载报文查 看用例运行中报文交互

例类型: HTTPS新建 测试用	户: admin 用例名称: HttpsCps	_Proxy_admin_20220128-16:42:11				0	9 停止
€鍵结果		状态用例限速 HTTP请求统计 Si	SL证书认证失败详细		网络层(PPS)	-	-
92.168.13.233 - 总和	彩旗				 10和 10和 10和 10和 	S 18 / 11	
TTP_新建速率	1,248	应用层			100 100 10 000 0+41	64.04	-
2.168.13.233 - Port1	砂值	●和 V port1 V port2 V			192.108.13.233 - PORT	eru	20.5
TTP_新建速率	1,248		砂值	总数	10.3.1993	4,992	110.04
2.168.13.233 - Port2	砂值	HTTP_新建速率	1,248	22,400	100.100.10.000. 0.40	0,240	01
TTP_新建速率	0	HTTP_新建失败 ¹	0	0	192.100.13.233 - POIL2	49100	204
		HTTP_请求速率	1,248	22,430	TR.A.SRW	0,240	110,30
		HTTP_国应码200	1,248	22,400	mx.2.15	4,992	94,08
		HTTP_国应码2xx	1,248	22,400			
		HTTP_回应码3xx	0	0			
		HTTP_回应码4xx	0	0			
		HTTP_回应码5xx	0	0			_
机包		HTTP_回应码总数	1,248	22,400	链路层 Mbps ♥		
		HTTP_接纹响应超时异常♀	0	0	10.00		
92.168.13.231 - Port1	忠数	HTTP_量传请求响应超时0	0	0 🗸	10.44		
的情况的思想	10,000				192.168.13.233 - Port1		Mb
訳字句数量	2,922,940	15/11/2		-	流量接收		13
		总和 V port1 V port2			流量发送		9
92.168.13.233 - Port2	8.8		紗值	总数	192.168.13.233 - Port2		Mbg
民政法包設量	10,000	TCP_主动新建_TXSYN	1,248	22,432	流量接收		9
获字节数量	2,922,646	TCP_主动建成_RXSYNACK	1,248	22,432	流量发送		17
61	[重启]已经停止[下数]	TCP_被动新建_RXSYN	1,248	22,432			
		TCP_被动建成_RXLASTACK	1,248	22,432			
		TCP_新建失败数量	0	0			
		TCP_新建中断数量0	0	0			
		TCP_服文授递_PSHACK	7,488	134,557	171010000		_
on person	-	TCP_报文接收_PSHACK	7,488	134,525	田朝国语		
称 占	用总数	TCP_授文发送_单独ACK	0	0	用例名称	用户名称 逆	行状
航内存 (57.44%	42.56% 15991 MB	TCP_服交接收_单独ACK	0	0	HttpsCps_Provy_admin_20	2201287e admin II	E在运
	13% 6080 MB	TOP 系包雷语报文教展	0	0	HEATER VVII	108500 MAGe of errors	

4.报文验证

tester_192.168.13.233_pc	rt1.pcap				-
文件(图 编辑(图) 税则(例)	RUNG MERC SHEA) 统计(5) 电活仪 无线(20) 3	日本日本語の正		
	D den a 2 4 3	ા 🚍 🚍 ચલલ 👳			
Apply a display fulter "	" (Ctr1-/)	12 3 3	2 2 2		
120 2 259701	Source	Jestination	Fratacol La	ngta into 1100 Comune Mella Constituiente Comune Mella Dana	^
130 2.358/01	111.1.1.223	111.1.1.2	TLSVI.I	1109 Server Hello, Certificate, Server Hello Done	
131 2.358702	111.1.1.223	111.1.1.2	TLSVI.I	1109 Server Hello, Certificate, Server Hello Done	
132 2.356764	111.1.1.225	111.1.1.2	TLSVI.I	1109 Server Hello, Certificate, Server Hello Done	
124 2 259706	111 1 1 222	111 1 1 2	TLSv1.1	1100 Server Hello, Certificate, Server Hello Done	
135 2 358708	111.1.1.223	111 1 1 7	TI Sv1 1	1109 Server Hello, Certificate, Server Hello Done	=
136 2 358700	111 1 1 223	111 1 1 2	TISV1.1	1999 Sarvan Hallo, Cratificata, Sarvan Hallo Dona	
137 2.358711	111.1.1.223	111.1.1.2	TI Sv1.1	109 Server Hello, Certificate, Server Hello Done	
138 2.358894	111.1.1.2	111 1 1 223	TI Sv1.1	400 Client Key Exchange, Change Cipher Sper, Encrypted Handshake Message	_
139 2.359081	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
140 2.359268	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	_
141 2.359456	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	_
142 2.359643	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
143 2.359839	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
144 2.360024	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
145 2.360210	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
146 2.360398	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
147 2.360585	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
148 2.360769	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
149 2.360958	111.1.1.2	111.1.1.223	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
<					>
Type: 8 (Echo	(ping) request)				^
Code: 0					
Checksum: 0x66	577 [correct]				
[Checksum Stat	us: Good]	客户	端为加密报文		
Identifier (BE): 0 (0x0000)				
Identifier (LE): 0 (0x0000)				
Sequence number	er (BE): 0 (0x0000)			
Sequence number	r (LE): 0 (0x0000)			
Response tran	<u>ie: 21</u>				
/ Data (18 Dytes	0		_		×
0000 08 55 0e 35	cd 34 68 91 d0 6	3 4c bc 08 00 45 00	5-4h - cL - E		
0010 00 2e 00 00	40 00 ff 01 9a e	b 6t 01 01 02 6t 01	· · · · · · · · · · · · · · · · · · ·		
0020 01 07 00 00 0030 6f 76 61 40	49 65 74 69 54 6	5 73 74 00 72 4e	ova@Neti Test		
00000 01 70 01 40	40 05 74 05 54 0		ordeneer rese		
					激活 Windows
					转到"设置"以激活 Windows。
○ 2 tester_192.168.13.	233_portl.peap			分組: 10000 · 已要示: 10000 (100.0%)	Profile: Default

1) 验证报文,可看到客户端为加密报文,服务端为非加密报文



Supernova 测试仪 SSL 卸载用例说明

d tester_192.168.13.233_p	ort2.pcap				- a ×
文件图 编辑图 视图Ⅳ	影特(G) 捕获(C) 分析	f(A) 统计(S) 电活(Y) 无线(W)	工具(1) 帮助(11)		
	S 9 0 0 5 1	🛓 📃 🗏 Q, Q, Q, 🖽			
Apply a display filter	(Ctrl-/)				
No. Time	Satarce	Jestination	Protocol Lan	gth Info	
136 2.360662	222.1.1.200	111.1.1.2	TLSv1.1	133 Change Cipher Spec, Encrypted Handshake Message	
137 2.360674	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
138 2.360675	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
139 2,360676	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	1
140 2,360678	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
141 2.360682	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
142 2.360683	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
143 2.360684	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
144 2.360685	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
145 2.360686	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
146 2.360687	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
147 2.360689	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
148 2,360690	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
149 2,360691	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
150 2.360692	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
151 2.360694	111.1.1.2	222.1.1.200	TLSv1.1	400 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
152 2.361592	222.1.1.200	111.1.1.2	TLSv1.1	133 Change Cipher Spec. Encrypted Handshake Message	
153 2.362320	222.1.1.200	111.1.1.2	TLSv1.1	133 Change Cipher Spec, Encrypted Handshake Message	
154 2.363036	222.1.1.200	111.1.1.2	TLSv1.1	133 Change Cipher Spec, Encrypted Handshake Message	
155 2.363754	222.1.1.200	111.1.1.2	TLSv1.1	133 Change Cipher Spec, Encrypted Handshake Message	
/					~
	. (100.)		1 (100 11)		
> Frame 1: 60 byt	es on wire (480 t	pits), 60 bytes capture	d (480 bits)		î
> Ethernet II, Sr	c: Fortinet_35:co	d:35 (08:50:0e:35:cd:35), Dst: Femrice_03:4c:bd (68:91:00:63:4C:D0)	
> Internet Protoco	of Version 4, Sre	c: 111.1.1.2, Dst: 222.	1.1.200		
* Internet Contro.	I Message Protoco	51			
Type: a (Echo	(ping) request)	the transfer terms have			
Code: 0	ccc c	非加密报义			
Checksum: 0x6	bbt [correct]				
[Cnecksum Sta	tus: Goodj				
Identifier (B	E): 8 (0x0008)	`			
Identifier (L	C): 2040 (0X0000)			~
0000 68 91 d0 63	4c bd 08 5b 0e	35 cd 35 08 00 45 00	h cL E -		
0010 00 2e 00 00	40 00 fe 01 2d	02 6f 01 01 02 de 01	· · · · @· · · · · · · · · · · ·		
0020 01 c8 08 00	66 61 00 08 00	00 53 75 70 65 72 4e	foSuperN		
0030 6t /6 61 40	4e 65 /4 69 54	65 /3 /4	ova@Neti lest		
					20的干 Mindows
					成白 WINGOWS
					转到Weint Windows。
😑 🍸 tester_192.168.13	233_port2.pesp			分组: 10000 - 已显示: 10000 (100.0%)	Profile: Defuelt



5.HTTPS 并发用例特殊配置

1) https 并发用例在"参数"中有启用 ssl 卸载功能按钮, 打开后可使并发连接数量的范围*2。

