

# Supernova 测试仪 HTTPS 多方式认证配置

网测科技

2021-01-18



i =1.
নি

文档说明	3
配置 SSL 证书套件	4
2.1 生成证书	5
2.1.1 生成 CA 证书(根证书)	5
2.1.2 生成服务器证书	6
2.1.3 生成客户端证书	7
2.1.4 验证服务器和客户端证书	9
2.2 上传证书和私钥文件	9
用例配置及运行	10
3.1 HTTPS 不认证	10
3.1.1 新建用例	11
3.1.2运行界面	13
3.1.3 查看报文	13
3.2 HTTPS 单向认证	14
3.2.1 新建用例	14
3.2.2 运行界面	16
3.2.3 查看报文	16
3.2.4 认证失败	16
3.3 HTTPS 双向认证	18
3.3.1 新建用例	19
3.3.2 运行界面	21
3.3.3查看报文	21
3.3.4 认证失败	21
	文档说明         配置 SSL 证书套件



# 1. 文档说明

本文档主要介绍 HTTPS 多方式认证配置和测试过程。HTTPS 证书认证方式默 认不认证,支持单向认证和双向认证。随着需求的不断改变,可能会对用例配置 进行修改和升级,从而改变配置过程,所以有任何问题,请联系我们的售前或售 后支持人员。



### 2. 配置 SSL 证书套件

SSL证书套件配置,用于支持各种 HTTPS 用例的运行和运行期间的证书认证。 各个证书文件之间的所属关系为:客户端证书文件、服务器证书文件,均由 CA 证书文件所签发。系统有默认 1024Key-SSL 证书套件和默认 2048Key-SSL 套件, 可以使用证书生成工具制作一套证书上传至系统。系统要求证书文件的扩展名必 须为:[.cer],编码格式必须为 PEM 编码,私钥文件的扩展名必须为:[.key], 编码格式必须为 PEM 编码。

	对象名称	數以1024key-SSL事件
		可は学校学校を行うたちになることで、「今代は学校大学生」
SSL证书套件 ❼		
CALLHECE	签名证书文件	ca-1024.cer 🛓
		* 证书文件的扩展名义词为: [xe] * ①中文化的图形成为《历为DALABER (Filterendule)
		* 允许拉文件名称: 東文、数字和符号
10-47 1827 ++339年		
BRASHIL TRUE	签名证书文件	server-1024.cer 🛓
		* 回代文字合体/編集的/2017; [ctr] * 回代文字合編集的/2017/PEN/編集 (第Dessedu编辑)
		* 允许的文件名称: 英文, 数字和响号
	签名私钥文件	server-1024.key
		* 化规以件设定 [#420] (77): [ //ey] * 和规以冲的编辑版记》(例为PD/M编码 (例Dare64编码)
	MARY BOTH	* 地理UX+安存: 東区、数字UFF号
	******	* 教学市局など、RCでによって観察会社、ATRATING
		1.11120日11日11日11日11日11日 ・1.1112日11日11日 季約に知られな可
客户端证书配置	*****	vitare 1033 ray.
	EDE MAIT	<ul> <li>空気気が含蓄積の通知: 1.001</li> </ul>
		* 运行文件的编辑规模式公理为FDV编辑(图Dassed编辑) * 分开的文件名称: 美文、教学和中于号
	签名私钥文件	clent 1024 key
		* 私规文/书的扩展在必须为: [Jay]
		* 私理文件的编码能式必须文PFD/编码(即Base6-5编码) * 允许相文文件名称: 英文、 数字和1件号
	签名私制密码	Superviova@NetTextTechnology
		* 若所送有妙处的文件来设置经济,就同时置应 * 分析说有效表示,本文、此文的用导
		* 量长为255个字节
基本信息		
基本信息	対象名称	Rubanny salar
基本信息 	対象名称	
基本信息 55.证书监持 @	対象名称	
基本信息 SSL语注意件• <b>の</b> CA証明知知	対象名称	
基本信息 SSL证计案件 ● CAE+HAE	対象名称 磁名证书文件	第3,200009933年           出版市物版E A2/A2/09/2/1-1_(环境時代所用)           ● 03,204007           ● 03,204007           ● 14,200007           ● 14,200007           ● 14,200007
基本信息 SSL证书监持 @ CA延书記録	对象名称 签名证书文件	
基本信息 SSL证字监件 ● CAEHR28	対象名称 盛名正书文件	
基本信息 SSLE小监件 @ CAE+标题 服务指证 442图	双數名称 双數名称 签名证书文件 签名证书文件	Buladery Solate           Buladery Solater           Buladery Buladery Buladery Buladery Buladery           *Schoolster
基本信息 SSLE注金件の CAE+和2国 服务員連书起語	対象名称 至去正书文件	Image: Source
基本信息 SSL证计监督← ● CA证书起策 服务描述书起策	対象名称 整名证书文件 整名证书文件	Billubarry 933.841           Stability 12/12/09/11/1, (FT20)402/FE)           Gabalacer           Chabren (Stability): (end)           Chabren (Stability): (end)           Chabren (Stability): (end)           Stability: (end)           Chabren (Stability): (end)      <
基本信息 SLE非監件 CAE状態質 服务描述作取資	<b>対象名</b> 取	BL30000900000000000000000000000000000000
基本信息           SSL证卡监件 ●           CAE+和2           服务描述中起致	对最名称 整名证书文件 签名证书文件	Bulgeony Soutier           Schematic Act Act O Schull, (Interpredention)           Interpreter Schuller, Interpreter Schule
基本信息 SSLE小監件 @ CAE+和公園 服务指任和公園	対截名年 整名证书文件 整名证书文件 整名私物文件	Buladorey State
基本信息 SSLE:非監件 @ CAIE+特定面 服务高速:特定面	対象名年	Image: Source Source           Image: Source Source           Image: Source Sourc
基本信息 55L语士監件 CA诺和松園 服务保证书記酒	双象名称	Exclusiony society           ±0509980 A2142109211-1_01739952793)           ±0509980 A2142109211-1_01739952793)           ±0509980 A2142109211-1_01739952793)           ±0509980 A2142109211-1_017399527930           ±0509980 A2142109211-1_017399           ±0509980 A2142109211-1_017399           ±0509980 A2142109211-1_01739           ±0509980 A2142109211-1_01739           ±0509980 A2142109211-1_01739           ±0509980 A2142109211-1_01739           ±05091980 A2142109211-1_0173           ±050919780 A2142109211-1_0173
基本信息           SL证书条件●           CA证书条理           服务描述书轮围	对最名称 至名正书文件 至名正书文件 至名礼物文件 後名礼物文件	Butzballery Statieff           2:84799882. Az1 Az1 CO 9 (Sriv.) (ST32)9402395)           4:82344 corr         4           4:82344 (ST 2010)         5           5         5           5         5           5         5           5         5           5         5           5         5           5         5           5         5           5         5           5         5           5         5           5         5           5         5           5         5
基本信息           SSL電子當件 ●           CAE+#空間           服务器匠 作空間           客户编译书配置	ガ酸表示     酸高に可文件     酸高に可文件     酸高に可文件     酸高に加文件     酸高に加文件     酸高に加文件     酸高に加文件     酸高に加文件     酸高に加文件	BLADARRY 93388           200709001 A21A210 921/11_00229402990           CASSIGN
<u>基本信息</u> <u>55L版</u> +於監督		BL20000 950384           E1899988 A274210971/11/1072090079)           CASBECT           CASBECT </th
	22歳4年 第名2442件 第名2442件 第名45月24日 第名45月24日 第名45月24日 第名45月24日 第名45月24日 第名45月24日	Image: Source
基本信息 SSL证件监督 CA证件批算 服务描述件批算 客/+编述件批算	22847 22827 22827 22827 2287 2287 2287 2	Butcherry State#           Extension Act Act On Statut, (INTERPHONE)           Image: Statut act Act Act On Statut, (INTERPHONE)           Image: Statut act A
	22条条节 服装记电众件 服装记电众件 服装机机算机 服装机的算件 服装机的算件	PLADATOR 900884           2000000 900884           2000000 A21A210 9111/1 (002940096)           Packadar           A           Packadar           C           Packadar           A           Packadar           Packadar           A           Packadar           Packadar           Packadar           Packadar           Packadar           Pa
基本信息           SSLE中監件 Ø           CAE+和公園           服务描述 仲紀西           SANAE 仲紀西	、 、 、 、 、 、 、 、 、 、 、 、 、	Bullating Staget           1            1           1           1           1           1           1           1           1           1           1           1           1           1      <
	、 () () ) ) ) ) ) ) ) ) ) ) ) ) )	Image: Source Source           Section of Source



#### 2.1 生成证书

在这里简单介绍一下 openss1 制作证书的过程,也可以使用其他证书生成工 具生成证书。openss1 默认信息存放方式 PEM 格式。一般证书生成过程:私钥文 件->证书请求文件->证书文件。

环境: Centos 7.4、openssl 1.0.2 创建生成证书的文件夹并进入: mkdir /home/test2 cd /home/test2

#### 2.1.1 生成 CA 证书(根证书)

1) 生成 CA 证书私钥

命令: openssl genrsa -des3 -out cal.key 2048

运行时会提示输入密码,此密码用于加密 key 文件(参数 des3 是加密算法, 也可以选用其他安全的算法),之后每当需读取此文件(通过 openss1 提供的命 令或 API)都需输入密码。输入相应的密码设定,如图所示:

[root@mail test2]# openssl genrsa -des3 -out cal.key 2048 Generating RSA private key, 2048 bit long modulus .....+++ e is 65537 (0x10001) Enter pass phrase for cal.key: Verifying - Enter pass phrase for cal.key: [root@mail test2]#

2) 生成 CA 自签名证书

命令: openssl req -new -x509 -days 365 -key cal.key -out cal.cer





#### CA 在签名时,可能会出现如下错误:

Using configuration from /etc/pki/tls/openssl.cnf Enter pass phrase for cal.key: /etc/pki/CA/index.txt: No such file or directory unable to open '/etc/pki/CA/index.txt' 140021678679968: error:02001002: system library: fopen: No such file or directory: bss\_file.c: 402: fopen('/etc/pki/CA/index.txt','r') 140021678679968: error: 20074002: BIO routines: FILE\_CTRL: system lib: bss\_file.c: 404:

执行下述命令可解决:

touch /etc/pki/CA/index.txt

touch /etc/pki/CA/serial

echo 00 > /etc/pki/CA/serial

### 2.1.2 生成服务器证书

1) 生成服务器私钥

命令: openssl genrsa -des3 -out server1.key 1024

输入相应的密码设定,如图所示:

在配置 SSL 证书套件时,服务器证书配置->私钥密码处需要填写此密码。

2) 生成服务器证书请求文件

命令: openssl req -new -key server1.key -out server1.csr



[root@mail test2]# openssl req -new -key server1.key -out server1.csr Enter pass phrase for server1.key: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [XX]:CN Locality Name (eg, city) [Default City]:AY Organization Name (eg, company) [Default Company Ltd]:WC Organizational Unit Name (eg, section) []:QA Common Name (eg, your name or your server's hostname) []:TEST Email Address []: Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []:

3) 使用 CA 根证书对服务器证书进行签名

命令: openssl ca -policy policy\_anything -days 365 -cert cal.cer

-keyfile cal.key -in server1.csr -out server1.cer



2.1.3 生成客户端证书

1) 生成客户端私钥

命令: openssl genrsa -des3 -out client1.key 1024



输入相应的密码设定,如图所示:

[root@mail test2]# openssl genrsa -des3 -out	client1.key 1024
Generating RSA private key, 1024 bit long mo	dulus
······ ++++++	
++++++	<b>安</b> 卢洪秋 钥 宓 码
e is 65537 (0x10001)	
Enter pass phrase for client1.key: netitest	a sata sat
Verifying - Enter pass phrase for client1.ke	y: netitest

在配置 SSL 证书套件时,客户端证书配置->私钥密码处需要填写此密码。

2) 生成客户端证书请求文件

命令: openssl req -new -key client1.key -out client1.csr

[root@mail test2]# openssl req -new -key client1.key -out client1.csr Enter pass phrase for client1.key: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [XX] CN State or Province Name (full name) [] HN Locality Name (eg, city) [Default City] AY Organization Name (eg, company) [Default Company Ltd] WC Organizational Unit Name (eg, section) [] QA Common Name (eg, your name or your server's hostname) [] WORD Email Address []: Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []:

3) 使用 CA 根证书对客户端证书进行签名

命令: openssl ca -policy policy\_anything -days 365 -cert cal.cer -keyfile cal.key -in client1.csr -out client1.cer



#### HTTPS 多方式认证配置



### 2.1.4 验证服务器和客户端证书

使用 CA 证书验证服务器和客户端证书命令:

openssl verify -CAfile cal.cer serverl.cer

openssl verify -CAfile cal.cer client1.cer

```
[root@mail test2]# openssl verify -CAfile cal.cer server1.cer
server1.cer: OK
[root@mail test2]# openssl verify -CAfile cal.cer client1.cer
client1.cer: OK
```

验证通过后,将文件打包,下载到工作电脑上,解压,方便将证书和私钥文 件导入系统。

#### 2.2 上传证书和私钥文件

1) 打开 Supernova 测试仪的 Web 界面,输入账号登录。

2) 对象->SSL 证书套件, 点击"增加", 创建一个新的 SSL 证书套件。

🚫 M测科技	111 🕐 📻 😪 🖌 👬 🔔 11194 1938 1938 2019 1044 1044 admin		V20.12.06	Super	rnova-88
网络拓扑	SSL证书窨件				
协议校进项					
SSLiZ-HIMH	【 · 翻 耳脉 点击增加,增加一个新的SSL证书套件			<b>N</b> 49	
有效數荷组	KUXJ服小板開發,从能設用的英菜,如果包裹與低了酸的低量,比如菜用头目,成支季菜,適点也完建,芳以一个时的酸,进行操作,				
TCL版本	□ 编号 各字	5418	究離	导出	关联数量
104:101-2014	1 默认1024Key-S5L数件	/	20		0
with Direct	2 联站2040Key-551数钟	1	2	<b>B</b>	0
Semicologia	3 取认周期5551迁代费件	1	2		0
HIIP卿劳29题					
TCP這機板	显示行版: 70 ✓ 1-3 of 3				- <b>1</b>
18/89240					



3)选择相应的证书和私钥文件上传系统,保存。

基本信息	
 2.妻&书	t <u>ss.Centogect_20206519-16-57-01</u> 修改证书套件名称 创新物理是AZIAS1091/1-/_
SSL证书套件 O	
CA证书配置 通常证书文件	o.pst.cer     下载上传的证书文件       * 正代文件结常最近因为:Pointal (Ellowscalle)     - (Edlowscalle)       * 证代文件编辑编载记载为Pointal (Ellowscalle)     - (Edlowscalle)       * 近代的空間表: 水子時間     - (Edlowscalle)       * 近代的空間表: 水子時間     - (Edlowscalle)       * 近代市町回: 征书文件上传成功后,会显示文件上传成功
<b>服务器证书配置</b> 适名证书文件	Server (2.0.07     まの) (20)     までのでなどが 新たん(あか) (20)     モーカンやお湯時に広ん(のか)をの場所()     ・ とかせいからか、ホナ、約からの時     ・ 大いないからか、ホナ、約からの時     ・ アルビスの(2)     ・ アルビスの(2)
强名机钢文件	sener_calay ** 戦烈な特徴 無名(初か: [Jay] * 気気なや結果的などの初からい場所(低)(2000+14時(低)低)(2000+14時(低)) * 力がないたまた。天気、約年の内号 大力に上げ低の7
<b>举名机物定</b> 码	nettet: - 都長海政地方式中本公室登場、英次写置空 - 法対対数時時式、東次、数本以降号 - 豊か力に以入学市
<b>客户编证书配置</b> 道名证书文件	(ient_text.cer         上           * 正式交流的常知最近の第次。[ant]         *           * 正式交流的学校和考试         (Blazersal)(第)           * 大川空大和各時、東文、数学校和特         *           * 大川空大和各時、東文、数学校和特         *
產者8.85%中 点击浏览按钮选择上传的证书文件	Gener, text.key         Goo         点击 † 按钮上传文件, × 按钮删除待上传文件           * MID2/ed/massfeed.dbtp://Logi         Goo         点击 † 按钮上传文件, × 按钮删除待上传文件           * MID2/ed/massfeed.dbtp://Logi         Globard.samp           * MID2/ed/massfeed.dbtp://Logi         Globard.samp           * MID2/ed/massfeed.dbtp://Logi         Globard.samp
查去15.将空语 -	nettesd * 世界通過部分从的文件未必重要的,並同可重益 * 分析地理研究式,来文、数字和符号 * 最近2135 今年可
	Ria Internet

### 3. 用例配置及运行

### 3.1 HTTPS 不认证

HTTPS 证书认证方式为"不认证"时,用例配置只需要服务器证书配置。 握手过程的简易流程图:





### 3.1.1 新建用例

1)通过 web 登录测试仪, 依次点击用例 -> 网关设备测试 -> HTTPS -> 新 建,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。

选择用例选项
IP版本 () v4 () v6 () 混合
受测设备工作模式 💿 透明模式(TP) 🚱
○ 路由模式(NAT) ②
网络配置 默认模板 ~
端口绑定 🗌
确定取消

### 2) 进入用例配置页面, 配置网络信息, 可设置报文捕获查看详细报文交互。

用例名称	HttpsCps_TP_admin_2021 法字符提型: A-Z / a-z / 0-9 /	0118-16:41:04 /・/_(不支持中文符号)			测试时长 (时分秒)	0 : Richnenklenner, Richk	10 : 0 不能起过999小时		
网络参数 月	良速 有户端	服务器	1 <b>2</b>						
网络设置									52.003
户端			<b>V</b>	😻 👿 🛡 🔍 🔍	服务端				₹ ₹ 🛛
ort1 port2 port3 port4					port5 port6 port7 po	rt8			
<b>点用油口</b>				MAC 68:91:d0:63:47:64	◎ 疑用鏡口				MAC 68:91:d0:63
CPU核绑定				-	CPU核绑定				
段文捕获					报文捕获				
	40.000447RI	4.05			速率与MAC				
	1/1 UCHCall	请法规协议的类型,无索示不	高用抓包						
	IP地站上				QinQ (部用)				
		通P地址或者目的IP地址,例	\$017.1.1.2		子网 😡				+ 添加子!
	第日				篇1个子网				自移除子同 ② 禁用
		源號口或者目的號口, 例如8	D			测试仪端口IP地址或范围	17.1.1.100	ø	
	Pcap文件大小		ma01.			测试仪端口子网掩码	16	0	
	1077.0197	pcap32(+), (1), 0 - 2000MB (	RANA)			虚拟路由	17.1.254.2		
	THESE CLOCK	范围: 0 - 6000000 (新认)				测试仪频口网关			
Sat-I)MAC				•					
linQ (禁用)				•		于网络队	HISKING	*	
一网 😡				+ 源加子网 🔺					
1 个子网				◎ 移除子网 ② 禁用子网					
	测试仪端口IP地址或范围	17.1.2.2-17.1.2.201	0						



3) 点击 客户端,编辑设置客户端证书认证配置,证书认证方式默认不认证。

基本信息(HTTPS监律)	
用的名称 HttpsCps_TP_admin_20210118-16.41.04 会话中符英型。A2/a2/0-9/:/-/_(不更物中文符号)	潮話はおする(1953년0) 0   10   0   0   0   0   0   0   0   0
网络 参数 限速 客户端 服务器 记录	
aaugayi 靜默均引	ADD
PSK/SRP测产者	Username 5%/5592ElaB/ornthy/Username
PSK/SRP##8	patoword FSKSFF用进設Preso phrase Pressword
(元)(中的)553.1版(本)	
证书认证方式(	2015年1月18日,國政國政國主任,國際小學社会同時的展開任任王 第1247년 (1948年1月)(1959年1月)
证书认证失败的处理(	開設の行法化汽油化学品を含ます。 ● 後下2011年上、単分のConfigure () 設置制度不適当用に ● 後下2011年上、単分のConfigure () 設置制度不適当用に
<u>59.1008766</u>	Abrikation         Abrikation           Abrikation         Abrikation
文件对象	BK人155年76月3224 ITTで通知につく金倉事ぐなた、文化中心可以認用の結束曲
交量列表	光 2 C2 日 HTTP POST分割中、可以引用史品列集、元点安全的分割化。
	Ria) (27)

4) 点击 服务器,编辑设置服务端证书认证配置,服务器证书配置选择 2.2 章节配置的 SSL 证书套件,使用的是其中的服务器证书配置部分,点击保存用例 的配置。

基本信息(HTTP\$新建)						
用的名称: HttpsCps_TP_admin_20210118-16:41:04 由法学和规型 A21ez/09/::/1-(_(不见時中交符号)	勝助な時候(時時) 0 1 1 1 1 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1					
网络参数 限速 客户端 服务器 记录						
15. (19) (19) (19) (19) (19) (19) (19) (19)	443 HTTF-超数器IRE19, REE 0 - 64.535 更比の回水のSAE集 図 了 ( ) 更影明密目のには HEBT+HEB的器型を描述目的 Server: rgur37 3 Content: Type: Learneril					
	启动 仪存 欺消					



### 3.1.2 运行界面

测试用例配置完成之后,点击运行启动 HTTPS 测试用例,启动后进入监测页面。

HTTPS新建 影式用户: admin	用例名称 HttpsCps_TP_edmi	in_20210118-16:41:04					
键结果	-	<b>状态</b> 用制用版 SSLETK从在大地详细			网络层		
92.168.16.228 - Port1	19 <u>6</u>	des P			皇和 単橋 多橋 广播		
ITTP_新疆建态	3,620	n max			192 168 16 228 - Port1	的值	(A)(5
2.168.16.228 - Port2	9 <u>0</u>		砂值	88 <sup>(1</sup>	杨文物的	14.482	662.31
TTP_新疆速率	4,144	HTTP_新建速车	10,836	543,147	杨文/短期	18,077	828.00
2.168.16.228 - Port3	9 <u>@</u>	HTTP_请代邀车	10,838	543,310	192.168.16.228 . Port2	86	
TTP_新建递系	2,705	HTTP_医应码2xx	10.836	543,147	经立场的	16.583	769.83
2.168.16.228 - Port4	स्त्र	HTTP_围窟碉3xx	0	0	80.25	20.668	962.3
TTP_新建递高	367	HTTP_图应码4xx	0	0	192.168.16.228 - Port3	彩曲	
2.168.16.228 - Port5	स्था	HTTP_ERCERTSXX	0	0	经全接收	10.844	527.7
TTP_新疆速率	0	HTTP_请求中断	0	0	62-0-19-16	13.551	650.2
2.168.16.228 - Port6	9 <u>ű</u>	HTTP_请求编辑	1	35	192.168.16.228 - Portá	1965	
TTP_新疆速率	0	HTTP_平均的延(初秒)		105	经交换的	1.471	217.4
24672		HTTP_#C1532 (809)		200,079	BBB		
		HTTP_SSL主动服手成功	10,838	543,310			
92.168.16.228 - Port1	总数	HTTP_SSL被动爆手成功	10.849	543,397	1244		
認動課也改量	50.000			~	192 168 16 228 - Port1		Mb
<b>获字节数量</b>	12,112,776	(114)E 0			IS HIGHLY		41
· 現 教 文 制 校 史	(重合) 已经停止 (下載)	tenda U		-	2010		24
12.168.16.228 - Port2	88	創和 port1 port2 port3 port4 port5 port6 port7 port8		^	192 168 16 228 - Port2		M
(20)留行政员	0				THE R		47
(1)水竹約員	0		19 <u>0</u>	总数	2010/01/01		37
	(王忠) P###it	TCP_主动制建压接	10.103	554,066	192.168.16.228 . Port3		Mb
0.450.45.000 0		TCP_主动建成连续	10,104	554,050	7月120		31
100.10.220 - PORTS	SN	TCP。被动建成连续	10,103	554,048	治局方法		18
NAMESON CONTRACTOR OF CONT	0	TCP_菌酮主动并发数量		256	192.168.16.228 - Port4		Mb
OCT HIMME	Contraction of the second	TCP。当初被动并没数量		273	· 市局地位		4
N MRG	1	TCP_主动用N关闭成功		0			_
<b>先资源</b>	<b>A</b>	TCP_被动FIN关闭成功		0	用例管理		
		TCP_主动Reset关闭连接		554,246			
(称 占用	SM	TCP_被动Reset关闭重接		553,382	用例名称	用户名称	运行
統內存 53%	47% 64322 MB	TCP_面接配改設量	17	1.657	HttpsCps_TP_admin_20210118	16:41:04 admin	TEG
		T(P = Haster (200)		281			

# 3.1.3 查看报文

报文中可以看到 SSL/TLS 的握手过程和服务器所使用的证书信息。

So. Time	Source	Destination	Protocol Length	Info	
- 1052 2.00	7953 17.1.2.125	17.1.1.100	TCP	70 10000 + 443 [SYN] Seg=0 Win=65535 Len=0 MSS=1452 SACK PE	RM=1 TSval=2078 TSecn=0
1308 3.00				70 [TCP Retransmission] 10000 - 443 [SYN] Seg=0 Win=65535 L	
1564 5.00				70 [TCP Retransmission] 10000 → 443 [SYN] Seq=0 Win=65535 L	
1929 5.14	0059 17.1.1.100	17.1.2.125	TCP	70 443 → 10000 [SYN, ACK] Seq-0 Ack-1 Win-65535 Len-0 MSS-1	1452 SACK PERM=1 [Sva1=5405 TSecr=2078
2077 5.14	2944 17.1.2.125	17.1.1.100	TLSv1.2	177 Client Hello	client->server
2569 5.16	9643 17.1.1.100	17.1.2.125	TLSv1.2	923 Server Hello, Certificate, Server Hello Done	server->client
2696 5.17				256 Client Key Exchange, Change Cipher Spec, Encrypted Hands	shake Message client->server
3089 5.18	4720 17.1.1.100	17.1.2.125	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message	server->client
3090 5.18	4740 17.1.2.125	17.1.1.100	TLSv1.2	198 Application Data	
3846 5.19	0635 17.1.1.100	17.1.2.125	TLSv1.2	181 Application Data	
L 3965 5.19	0820 17.1.2.125	17.1.1.100	TCP	60 10000 + 443 [RST, ACK] Seq-434 Ack-1024 Win-65535 Len-0	
<					
✓ Secure Socke	ts Layer				
> TLSv1.2 R	ecord Layer: Handshal	ke Protocol: Server Hello			
✓ TLSv1.2 R	ecord Layer: Handshal	ke Protocol: Certificate			
Content	Type: Handshake (22	2)			
Version	: TLS 1.2 (0x0303)				
Length:	785				
✓ Handsha	ke Protocol: Certifi	icate			
Hand	shake Type: Certific	ate (11)			
Leng	th: 781				
Cert	ificates Length: 778				
✓ Cert	ificates (778 bytes)				
Ce	rtificate Length: 77	15			
✓ Ce	rtificate: 308203033	08201eba003020102020103300	d06092a864886	(id-at-commonName=TEST,id-at-organizationalUnitName=QA,id-at	t-organizationName=WC,id-at-localityName=AY,id-at-stateOrProvinceName=HN,id-at-countryName=CN)
~	signedCertificate				
	version: v3 (2)				
	serialNumber: 3			服务器证书信息	
	> signature (sha256	WithRSAEncryption)			
	✓ issuer: rdnSequer	nce (0)			
	✓ rdnSequence: 5	items (id-at-organization	alUnitName=QA,id-	at-organizationName=WC,id-at-localityName=AY,id-at-stateOrPr	ovinceName=HN,id-at-countryName=CN)
	> RDNSequence	item: 1 item (id-at-countr	yName=CN)		
	> RDNSequence	item: 1 item (id-at-state0	rProvinceName=HN	)	
	> RDNSequence	item: 1 item (id-at-locali	tyName=AY)		
	> RDNSequence	item: 1 item (id-at-organi	zationName=WC)		
	> RDNSequence	item: 1 item (id-at-organi	zationalUnitName	-QA)	
	> validity				
		1.003			



### 3.2 HTTPS 单向认证

HTTPS 证书认证方式为"单向认证"时,用例配置需要 CA 证书配置、服务器证书配置,且服务器证书文件是通过 CA 证书文件签发的。单向认证要求服务器有证书,客户端对服务器进行验证。



单向认证的简易流程图如下:

### 3.2.1 新建用例

1)通过 web 登录测试仪,依次点击用例 -> 网关设备测试 -> HTTPS -> 新 建,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。

IP版本	● v4 ○ v6 ○ 混合
受测设备工作模式	<ul> <li>透明模式(TP)</li> </ul>
	○ 路由模式(NAT)
网络配置	默认模板 ~
端口绑定	



H-F/ER/UNTERO

2) 进入用例配置页面, 配置网络信息, 可设置报文捕获查看详细报文交互。

用例名称	HttpsCps_TP_admin_20 合法字符简整: A-Z / a-z / 0-9	210118-16:52:08 /:/-/_(不支持中文符号)			测试时长(时分秒)	0): Idaaliintiiseenkä, Mikris	10 : 0 7401212999/141	]	
网络参数	限速 有户端	服务器	记录						
洞路设置				<b>**••••</b>	服务端				
port1 port2 port3 port4	•				port5 port6 port7 por	18			
「無用満口				MAC 68:91:d0:63:47:b4	⊘ 競用調口				MAC 68:91:d0:63:4a
CPU核鄉定				•	CPU核绑定				
报文捕获				-	报文捕获				-
	协议类型	全部	*		速率与MAC				
		请选择协议的类型,无表 ·	元不启用抓包		QinQ (150用)				,
	IP地均	IIIIP195100#ERIP1951	@0017112		子网 😡				+ 漆如子网
	282				第1个子网				自 総除子网 Ø 業用子网
		透明口或者目的第口。例	080			测试仪纳口IP地址或范围	17.1.1.100	0	
	Pcap文件大小		m (8821)			测试仪端口子网境码	16	0	
	捕获何志	soood	O (ALV)			虚拟路由	17.1.254.2	0	
		范围: 0 - 6000000 (武认)				题试仪端口网关		0	
速率与MAC				-		VLAN ID		0	
QinQ (創用)				-		子网機拟	只機拟服务铸	~	
子网 🛛				+ 漆加子网 🔺					
第1个子网				● 移除子网 ◎ 魚用子网					
	测试仪端口IP地址或范围	17.1.2.2-17.1.2.201	Θ						

3) 点击 客户端,编辑客户端证书配置,认证方式选择单向认证。CA 证书 配置选择 2.2 章节配置的 SSL 证书套件,使用的是其中的 CA 证书配置部分。

用的高称 HttpsCps_TP_admin_20210118-16-52-08	周回式が長(セジンゼ) の   10   10   0   0   0   0   0   0   0
网络 参数 限速 酱户端 服务器 记录	
SSL选项	•
勝野半田	
	关闭SSL语频前,不再说进SSL Alert跟文。
PSK/SRP用户名	username
	PSK/SRP第法的Identity/Username
PSK/SRP密码	pessword
	PSN/SRP第注的Pass-phrase/Password
允许的SSL版本	□ SSU3 □ TLS/1.0 □ TLS/1.1 ☑ TLS/1.2 □ 開始/1.1
27.022.127.000	Sauga, minasugaangaa mina menya na menya na minasuka na sa
AT TANKED STA	○ パベル ● ● キャンペ ○ MPTWL ■ SSE選手的後、服务器変換です。 客户論使用CA正当的正当内算进行人在
CA证书配题	#X11024Key551#24
	使用所包的SSL证书都件中的CA证书配置称分
证书认证失败的处理 (	◎ 终止SSL需手。新开socket医输 ○ 报题并通出程序运行
· · · · · · · · · · · · · · · · · · ·	选辑SSLE书认证失明时的操作
SSL加限撤往	通過等所有 - 戰頭所有
	ABS128-CCM
	AES128-CCM8
	Active devision action
文件对象	默认156字节网页2014 🗸 📝 🕀
	HTTP读求的文件对象。可以包括一个或者多个文件,文件中也可以使用内裁要量
	Eta) 9277 809

4) 点击 服务器,编辑服务端证书配置,服务器证书配置选择 2.2 章节配置 的 SSL 证书套件,使用的是其中的服务器证书配置部分,点击保存用例的配置。

用例名利	HttpsCps_TP_admin_20210118-16:52:08 台法宇符提型: A-Z / a-z / 0-9 / : / · / _ (不受時中交	符号)	第6位対任( (1959年) 0  : 10 ]: 0  第6に注意式目分に近いなが用。第10分に不可能についっとす
网络 學致	展進 (	记录 HTTPS服务器纳口 服务器证书配置 HTTP回应头	443       MT117-BERSBERZER, INDE 0-60.535       BRULD24A, SSDBERG       BRULD24A, SSDBERG-RECHARGERED       Server, regime 18.10       Content Type: text/tranil



### 3.2.2 运行界面

测试用例配置完成之后,点击运行启动 HTTPS 测试用例,启动后进入监测页面。

HTTPS新建 教武用户: admin	用例名称 <u>HttpsCps_TP_edm</u>	in_20210118-16:52:08					
雖結果		<b>联合</b> 用制制度 SSLEH以任何数详细			网络层		
92.168.16.228 - Port1	200	( design			980 年初 多期 广瀬		
TTP_#REMAIL	3,179	DY Hiller			103 168 16 338 Beest	60.0T	-
92.168.16.228 - Port2	90	HTTP_新建施室	10,018	206,777	Constant Section of the section of t	13,710	216.00
TTP_教徒建建	3,649	HTTP_请求連起	10.020	206.864	10.0340	15.036	210.90
2.168.16.228 - Port3	90	HTTP_萬匠码2x	10.018	206.777	192 168 16 228 - Port2	100	01
TTP_新建速率	1,661	HTTP_直应码3xx	0	0	10010010000	14 591	258.90
92.168.16.228 - Port4	रुख	HTTP_属匠码4xx	0	0	1000 Mile	18.228	323.74
TTP_新建速率	1,529	HTTP_周庄65xx	0	0	192 168 16 228 - Port3	10,000	01
2.168.16.228 - Port5	छन्न	HTTP_请求中断	0	0	12:11:00	6.651	211.53
TP_新疆速率	0	HTTP_请求组9月	2	6	100-01000	0,001	364.03
2.168.16.228 - Port6	90	HTTP_平均的延(微妙)		119	103 108 40 338 Dented	1000	
TP_新疆連本	0	HTTP_@dwitki (806)		11	132,100,10,220 - P0104	6 191	142.71
		HTTP_最大时延(微妙)		200,080		9,131	146.11
e anti-		MTTP_SSL主动爆车成功	10.021	206,865	「「「「「「」」		
		HTTP_SSL被动握手成功	10.024	206,942			
2.168.16.228 - Port1	28	HTTP_SSLi() 医细胞	0	0	1844		
原数操作数量	50,000			~	102 169 16 239 Dout1		Aller
<b>院李节数量</b>	12,097,304	Conservation of the second sec			THE TOUL TO A DO TO TO		20.0
文捕获	(重合) 已经停止 (下載)	作業はの		<b>^</b>	COLORIS .		30.5
0.168.16.238 Beer?		#10 port1 port2 port3 port4 port5 port6 port7 port8		^	102 102 10 202 0 202		21.
12811941997	0				- Bink		
1232-14 190-18	0		的值	88	20002945		913
	1941 742/74	TCP_主动新建连接	10,033	207,315	3040303		24.1
ADADA	(Ed) Cielivit	TCP_主动建成连续	10,033	207,306	192.100.10.220 - PORS		10.1
12.168.16.228 - Port3	总数	TCP_被动建成压缩	10,032	207,305	3040000		19.
REESSE	0	TCP_当前主动并发数量		255	102 169 16 239 . 0001		11.
以子17奴皇	0	TCP_当前被动并发数量		265	104.104.10.228 - POR4		17.7
XINK	[王宗] 已经接让 · · ·	TCP_主动FIN关闭成功		0	- makeron		- 0.0
0.7730		TCP_被动印N关闭成功		0	III AND TO		
		TCP_主动Reset场动振输		207.265			
(称 占用	200	TCP_被动Reset关闭连接		206,861	用制名称	用户名称	通行
読内存 53.05% 4	6 94% 64322 MR	TCP_重传报文数量	53	761	HttpsCps TP admin 20210118	16:52:08 admin	TERE
	20050 100	TCP_主动新建平均时延(60秒)		226			(Marcale

### 3.2.3 查看报文

报文中可以看到 SSL/TLS 的握手过程和服务器所使用的证书信息。

The stranded arranged				
1188 3.121663 17.1.2.65				
1444 5.116982 17.1.2.65				
1700 9.107584 17.1.2.65			70 [TCP Retransmission] 10000 → 443 [SYN] Seq=0 Win=	
2065 15.069 17.1.1.100	17.1.2.65	TCP	70 443 + 10000 [SYN, ACK] Seq=8 Ack=1 Win=65535 Len=	8 MSS-1452 SACK_PERM-1 TSval-15326 TSecr-2164
2205 15.070 17.1.2.65	17.1.1.100	TLSv1.2	177 Client Hello	dient->server
2577 15.089 17.1.1.100	17.1.2.65	TLSv1.2	923 Server Hello, Certificate, Server Hello Done	server->client
2705 15.091 17.1.2.65	17.1.1.100	TLSv1.2	256 Client Key Exchange, Change Cipher Spec, Encrypte	d Handshake Message client->server
3089 15.112. 17.1.1.100	17.1.2.65	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message	server->client
3213 15.113 17.1.2.65	17.1.1.100	TLSv1.2	198 Application Data	
3710 15.118 17.1.1.100	17.1.2.65	TLSv1.2	181 Application Data	
- 3853 15.119 17.1.2.65	17.1.1.100	TCP	60 10000 + 443 [RST, ACK] Seq=434 Ack=1024 Win=65535	Len-8
Transmission Control Protocol, Src	Port: 443, Dst Port:	10000, Seq: 1, A	ck: 112, Len: 857	
<ul> <li>Secure Sockets Layer</li> </ul>				
> TLSv1.2 Record Layer: Handshake	Protocol: Server Hell	0		
<ul> <li>TLSv1.2 Record Layer: Handshake</li> </ul>	Protocol: Certificate			
Content Type: Handshake (22)				
Version: TLS 1.2 (0x0303)				
Length: 785				
Handshake Protocol: Certifica	te			
Handshake Type: Certificat	e (11)			
Length: 781				
Certificates Length: 778				
<ul> <li>Certificates (778 bytes)</li> </ul>				
Certificate Length: 775				
<ul> <li>Certificate: 30820303308</li> </ul>	201eba0030201020201033	00d06092a864886.	(id-at-commonName=TEST,id-at-organizationalUnitName=Q	A,id-at-organizationName=WC,id-at-localityName=AY,id-at-stateOrProvinceName=HN,id-at-countryNam
✓ signedCertificate				
version: v3 (2)				
serialNumber: 3			肥冬蚬江北信白	
> signature (sha256Wi	thRSAEncryption)		服力管理口口态	
v issuer: rdnSequence	(0)			
Y rdnSequence: 5 i	tems (id-at-organizati	onalUnitName=QA,	d-at-organizationName=WC,id-at-localityName=AY,id-at-st	ateOrProvinceName=HN,id-at-countryName=CN)
> RDNSequence it	em: 1 item (id-at-cour	tryName=CN)		
> RDNSequence it	em: 1 item (id-at-stat	eOrProvinceName=	HN)	
> RDNSequence it	em: 1 item (id-at-loca	lityName=AY)		
> RDNSequence it	em: 1 item (id-at-orga	nizationName=WC)		
> RDNSequence it	em: 1 item (id-at-orga	nizationalUnitNa	ne=QA)	

### 3.2.4 认证失败

当服务器证书不是由CA证书签发的(CA证书和服务器证书配置来自不同SSL 证书套件)、证书过期等情况时,将会运行失败,系统会做出证书认证失败的处



理,并提示错误信息。下边是 CA 证书和服务器证书配置来自不同 SSL 证书套件的情况。

1) CA 证书配置选择默认 SSL 证书套件, 服务器证书配置选择 2.2 章节配置的 SSL 证书套件。

用例解称 HttpsCps_TP_admin_20210118-16:52:08 会法学院問題、A-Z / a-z / D-9 / : / - / (不受持中文符号)	(時間時時、(時分校) 時間時時、(時分校) 時間時時、日本時時時、日本時時代の一般におります。 第20日日、日本時間、日本時間、日本時間、日本時間、日本時間、日本時間、日本時間、日本
SOFTER	
(約400-5-12)	All
	Sector Market Control
PSK/SRP用户名	username PSK/SRP#i=#20ternity/Username
PSK/SRP繼码	patisword
	PSK/SRP碑注含Pass-phrase/Password
分约年4055L版本	SSU4 [ TLSM.0 [] TLSM.1 [2] TLSM.2 [] 108804.1
27-402127-4	SSL版本, 电ASSL版本对应的描述F一样, 图MM-1.FH/MB/BEECC-SM4-SM3
LETTINGED SL	51.截至前後。顧勞難說通知书,進合機構用CA征指的征书的尊進行认证
CA证书配题	#XU1024Key-SSL要件
	使用所造的SSL证书整件中的CA证书配图的分
证书认证失败的处理	○ 後止SSI票#, WFFootee证据 ● 招继并退出展映画行 证书认证失败处理选择报错并退出程序运行
SCI TROPING	1219534_E10A_E20W19E3MFB
and the second sec	
	AE5128-CCM8
	AE5128-GCM-SHA256
	AE5128-SHA
	∏ AES128 SHA256 ¥
文件对象	戦以156年市現党文件 ✓ ♂ 日 HTTP予定時では対象。可以接所一个成長条个文法、文法中心可以降田の前用員
	sTab 9477 \$538
其本信息(HTTPS新建)	
用例名称 HttpsCps_TP_admin_20210118-16:52:08	測试時长(時分泌) 0 : 10 : 0
台油宇符器型: A-Z / a-z / 0-9 / : / - / _ (不支持中文符号)	演出石配過时长后自动结束,演出时长不能超过999/ej
网络参数 限速 客户端 服务器 记录	
HTTPS服务器纳口	443
	HTTPS服务器第二号,范ェ 0-65.535
服务课证书配置	
	使用所造的551证书都行中的服务器位书配置部分
HTTP回应头	Server: nginx19.10 Content-Type: text/html
	lh.

2)用例运行失败,报错提示客户端验证服务器证书失败。

🚫 网测科技 🚆 🤗 📕	<b>S</b> #19	<b>公</b> 服務	影統	Angen V20.12	55 Supernova-88D
				▲ 失败	
				106月2日 - 同次第75 (106月2日) 10月1日 - 日本第二日 10月1日 - 日本 10月1日 - 日本 10月11日 - 日本 11月11日 - 日本 11月111日 - 日本 11月1111日 - 日本 11月1111111111111111111111111111111111	
				port port1 verify peer cert error: (7) certificate signature failure	
				tester_192.168.16.228_sort1.pcap 🗸 💽 不能	

 3)查看报文,服务器给客户端发送证书等信息后,客户端验证服务器证书, 终止与服务器的通信。





### 3.3 HTTPS 双向认证

HTTPS 证书认证方式为"双向认证"时,用例配置需要 CA 证书配置、客户 端证书配置、服务器证书配置,且客户端证书文件、服务器证书文件,均是通过 CA 证书文件签发的。双向认证要求服务器和客户端双方都有证书,客户端对服 务器进行认证,服务器也要对客户端进行认证。

\_\_\_\_\_

双向认证的简易流程图如下:





### 3.3.1 新建用例

1)通过 web 登录测试仪, 依次点击用例 -> 网关设备测试 -> HTTPS -> 新 建,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。

选择用例选项
IP版本 ● v4 ○ v6 ○ 混合
受测设备工作模式 💿 透明模式(TP) 😮
○ 路由模式(NAT) ⑧
网络配置 默认模板 ~
端口绑定
確定取消

#### 2) 进入用例配置页面, 配置网络信息, 可设置报文捕获查看详细报文交互。

基本信息(HTTPS新建)				
用例名称 HttpsCps_TP_admin_202 合法字符类型。AZ/az/09/	00118-17:12:36 1-7_(不支持中交符号)	劉斌时长(時分秒) 0: 劉武在起語时长后自动結束、劉成时代	10 : 0	
网络 参数 限速 客户端	服务器 记录			
每存网络设置 客户端 port1 port2 port3 port4		服务端 port5 port6 port7 port8		
の無用調白	MAC 68:91:d0:63:47:b4	0 銀用練口		MAC 68:91:d0:63:4a:cc
CPU核绑定	-	CPU核绑定		-
报文捕获	•	报文捕获		•
协议类型		速率与MAC		•
IP\$936	HIGENWOYXXXSAELL JUDIO JUTINI HEIMIEL	QinQ (甜用)		•
	题IP地址或者目的IP地址,例如17.1.1.2	子网 🛛		+ 源如子网 🔺
第日		篇1个子网		會 移除子阿 ② 禁用子网
	遊跳口或者目的跳口, 例如B0	测试仪读口IP地址或范围	17.1.1.100	ø
Pcap又样大小	pcao文件大小、0 - 2000MB (数认)	测试仪线口子网接码	16	Θ
捕获包数	50000	虚约路由	17.1.254.2	
	7588: 0 - 6000000 (銀行人)	测试仪满口闷关		0
速率与MAC	-	VLAN ID		Θ
QinQ (結用)	•	子网模拟	只憐权服务論	Y
子网 🛛	+ 液加子同 🔺			
第1个子网	會 移除子网 O 禁用子网			
测试仪病口IP地址或范围	17.1.2.2-17.1.2.201			
	18130	(\$# Tion		



3) 点击 客户端,编辑客户端证书配置,认证方式选择双向认证。CA 证书 配置选择 2.2 章节配置的 SSL 证书套件,使用的是其中的 CA 证书配置部分,客 户端证书配置选择 2.2 章节配置的 SSL 证书套件,使用的是其中的客户端证书配 置部分。

用例名称 HttpsCps_TP_admin_2 合法字符类型 A-Z / a-Z / a-Z / a-Z	0210118-17:12:36 9 / : / - / _ (不支持中文符号)	期前対任 (時分秒) 0   10   0 期位石配用时任后日394年、期位59代不能期は1999/91
网络 参数 限速 春户端	服务器 记录	
SSL选项		
	静默关闭	SH AH
		关闭SSL道频前,不再发送SSL Alert版文。
	PSK/SRP用户名	(izername
	1.00000700-94	PSK/SRP#jtagidenthy/Username
	PSK/SRP密码	password
		PSK/SRP荷(进的Pass-phrase/Password
	允许的SSL版本	□ SSLV3 □ TLSV1.0 □ TLSV1.1 ☑ TLSV1.2 □ ■®V1.1
		SSL版本,每个SSL版本对应的描述不一样。属eW1.1只能回题ECC-SM4-SM3
	证书认证方式	○不以徑 ○ 単時以徑 ● 双時以徑
		SSL题手阶段。题势骤然逃还书,客户遍供用40正书内需进行认证: 且题务课题求第户端提供证书,并但用CA证书对证书内需进行认证
	CA证书配置	戦化1024Key-SSL暫件 V  ぼ 田
		使用研造的SSL证书题件中的CA证书题图即的分
	客户端证书配置	展代1024Key-SSL器件 ✓ 🕼 🕀
		使用所造的SSL证书暂件中的路户演正书配置即分
	证书认证失败的处理	● 终止SSL题手, 新开Facket语操 ○ 报酬并退出报学运行
		中/据的1000年度3月1日。 1995年1月1日(1995年1月1日)
	SSL加密赛件	进导所有 取游乐有
		AES128-CCM
		AES128-CCM8
		AES128-GCM-SHA256

4) 点击 服务器,服务器证书配置选择 2.2 章节配置的 SSL 证书套件,使用 的是其中的服务器证书配置部分,点击保存,保存 HTTPS 新建用例的配置。

基本信息(HTTPS新建)	
用制築物 HttpsCps_TP_admin_20210118-17:12:36 合法宇持提型 AZ /az / 0-9/:/-/_(不支持中交	第64世界後、(1912年) 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
网络参数 限速 客户端 服务器	记录
R2166 ( ● 823 ( R218 ( 新r <sup>2</sup> 134 ) <u>R2195</u>	ITTPSERGENAL ITTPSERGENAL ITTPSERGENAL ITTPSERGENAL ITTPSERGENAL ITTPSERGENAL ITTPSERGENAL ITTPSERGENAL Severe regenal III Content Syste condition
	<b>£</b> 3à (077) <b>5</b> 5A



### 3.3.2 运行界面

测试用例配置完成之后,点击运行启动 HTTPS 测试用例,启动后进入监测页面。

HTTPS新建 激武用户: admin	用例名称 HttpsCps_TP_edm	in_20210118-16:52:08					0
御結果		<b>北心</b> 用用用用度 551在卡比让在大地计划			网络层		
92.168.16.228 - Port1	190	Column .			980 年初 多期 广瀬		
TTP_新疆建建	3,179	Di Hilan			103 168 16 338 Beest	60.0T	-
92.168.16.228 - Port2	90	HTTP_新發調室	10,018	206,777	Constant Section of the section of t	13,710	214.00
TTP_新疆建型	3,649	HTTP_请求逾差	10.020	206.864	10.0340	15.036	210.90
02.168.16.228 - Port3	90	HTTP_属匠码2xx	10.018	206.777	192 168 16 228 - Port2	100	01
TTP_新建递车	1,661	HTTP_直应码3xx	0	0	10010010000	14 591	258.90
02.168.16.228 - Port4	रुख	HTTP_周回時4xx	0	0	1000 Mile	18.228	323.74
TTP_\$598.84%	1,529	HTTP_氮症的5xx	0	0	192 168 16 228 - Port3	10,000	01
12.168.16.228 - Port5	छन्	HTTP_请求中任	0	0	49-1-12-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	6.661	211.63
TP_新疆速率	0	HTTP_请求提8f	2	6	100-01000	0,001	364.03
2.168.16.228 - Port6	00	HTTP_平均的1%(00秒)		119	103 108 40 338 Dented	1000	
TTP_新建速率	0	HTTP_最小时候 (問約)		11	132,100,10,220 - P0104	6 191	142.71
		HTTP_最大时延(微妙)		200.080		4,191	1444
2 MESE		HTTP_SSL主动爆手成功	10.021	206,865	「「「「「「」」		
	0	HTTP_SSL被助握手成功	10.024	206,942			
2.168.16.228 - Port1	22	HTTP_SSLI() 还完成	0	0	1844		
研教課任政量	50,000			~	102 169 16 239 Dout1		Aller
较字节数量	12,097,304	Converse of the second s			THE TOUL TO A DO TO TO		201
交捕获	(重合) 已经停止 (下載)	<b>传输</b> 层 <b>◎</b>		<b>^</b>	COLORIS .		30.5
11 168 16 218 Beer?	-	Sta port1 port2 port3 port4 port5 port6 port7 port8		^	102 102 10 202 0 202		21.
1281284190	0				- Bink		
12:3:4:10:05	0		64	88	20002945		91.3
NAMES TO A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTIONO	1941 0427-5	TCP_主动新建连接	10,033	207,315	3040303		24.1
ADADA	TEGT CARIFUL	TCP_主动建成连接	10,033	207,306	192.100.10.220 - PORS		10.1
02.168.16.228 - Port3	总数	TCP_被动建成连续	10,032	207,305	3040000		19.1
	0	TCP。当前主动并发数量		255	102 169 16 239 . 0001		APP
18代子 17 軟體	0	TCP_当前被动并没数量		265	104.104.10.228 - POR4		17.7
X 1864	(重度). 已经接让 · · ·	TCP_主动FN关闭成功		0	- makeron		100
N 77 70		TCP_被动FIN关闭成功		0	III AND TO		
		TCP_主动Reset完衍编编		207.265	TO PHIAL		
(称 占用	6M	TCP_被动Reset完旺连接		206,861	用制名称	用户名称	通行
(学のな (1200) 40	64322 MR	TCP,重得很文数量	53	761	Https://ps.TP.admin.20210118	16:52:08 (admin)	TERM
35.00% 40	20055140	TCP_主动新建平均时延(简秒)		226		(Warring)	- dialog

### 3.3.3 查看报文

报文中可以看到 SSL/TLS 的握手过程和服务器所使用的证书信息。

			the first statement of the
1885 17.090 17.2.2.29	17.2.1.100	TCP	70 [TCP Retransmission] 10000 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 SACK_PERM=1 TSval=17192 TSecr=0
2142 24.317 17.2.1.100	17.2.2.29	TCP	70 443 → 10000 [SYN, ACK] Seq-0 Ack-1 Win-65535 Len-0 MSS-1452 SACK_PERM-1 TSval-24625 TSecr-2192
2250 24.319 17.2.2.29	17.2.1.100	TLSv1.2	177 Client Hello client->server
2688 24.323 17.2.1.100	17.2.2.29	TLSv1.2	1506 Server Hello server->client
2870 24.341 17.2.1.100	17.2.2.29	TLSv1.2	390 Certificate, Certificate Request, Server Hello Done Server->client
2997 24.342 17.2.2.29	17.2.1.100	TCP	66 10000 → 443 [ACK] Seq=112 Ack=1765 Win=65535 Len=0 TSval=24461 TSecr=24629
2998 24.342 17.2.2.29	17.2.1.100	TCP	1506 10000 → 443 [PSH, ACK] Seq=112 Ack=1765 Win=65535 Len=1440 TSval=24462 TSecr=24629 [TCP segment of a reassembled PDU]
2999 24.342 17.2.2.29	17.2.1.100	TLSv1.2	607 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message client->serve
4041 24.408 17.2.1.100	17.2.2.29	TCP	66 443 → 10000 [ACK] Seq=1765 Ack=2093 Win=65535 Len=0 TSval=24658 TSecr=24462
4042 24.408 17.2.1.100	17.2.2.29	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message server->client
4169 24.409 17.2.2.29	17.2.1.100	TLSv1.2	198 Application Data
4691 24.414 17.2.1.100	17.2.2.29	TLSv1.2	181 Application Data
4863 24.415 17.2.2.29	17.2.1.100	TCP	60 10000 → 443 [RST, ACK] Seq-2225 Ack-1931 Win-65535 Len-0

### 3.3.4 认证失败

当服务器证书不是由CA证书签发的(CA证书和服务器证书配置来自不同SSL 证书套件)、客户端证书不是CA证书签发的(CA证书和客户端证书配置来自不 同SSL证书套件)、证书过期等情况时,用例将会运行失败,进行证书认证失败 处理,并提示错误信息。下边是CA证书和服务器证书配置来自同一SSL证书套 件,客户端证书选择其他SSL证书套件的情况。

1) CA 证书配置和服务器证书配置选择 2.2 章节配置的 SSL 证书套件,客户



端证书配置选择选择默认 SSL 证书套件。

基本信息(HTTPS新建)	
用例名称 Https:/pt.jf.p.admin.20210118-17.26.43 調査対任 (明9時) 0 1 10 0 0 10 10 0 10 0 10 0 10 0 10	
网络 参数 限速 有户端 服务者 记录	
<b>转数</b> 关闭 <b>2018</b> 为时间以上短期间,不是3000年5月,从14时1月21。	
PSK/SR9IIjA-SG usename	
FSU20PEEJS00emp(Username	
Parkannet Berger Bergerer Berger Bergerer Bergerer Berg Bergerer Bergerer B	
10月1955年 5846 1 1541.0 1541.1 2 1541.2 1 単編4.1	
SUBJECT POLY DEVICE OF THE OF THE OFFICE OF THE OFFICE OFF	
Chall Distribution Contact Distribution     Chall	
REVENUE AND CONTRACT AND CONTRA	
正年以(正天明390月) ○ 使止い風景、単汗ののの活動 ● 宿谷市島山健学会介)	
語意识过明认定网络李姆姆在这样中认此失败处理的力式。	
A5128-600-594256	
A51289445	
文计约编 載40.155年15月52年 🗸 🕼	
exa 977 308	
	_
基本信息(HTTPS新建)	
用時常称 Https/cp_1Tp_admin_20210118-172443 原因伊扬(终分秒) 0 = 10 = 0	
台湾等等設置 A2452/09/1/-1 (不安計等の支持) 第625年5月1日(第636年8月1日) 第625年5月1日(第636年8月1日) 第625年5月1日(第636年8月1日) 第625年5月1日(第636年8月1日) 第635年5月1日) 第635年5月1日(第63555555555555555555555555555555555555	_
网络 参数 限速 备户线 医伤音 记录	
HTTPSER#BMICI 443	
HTTP//··································	
HTTP/IRED. Contemport 9:30	

2)用例运行失败,报错提示服务器验证客户端证书失败。



port port3 verify peer cert error: (7) certificate signature failure

3) 查看报文,服务器给客户端发送证书等信息后,客户端验证服务器证书通过,并发送自己的证书等信息,服务器验证客户端证书,终止与客户端的通信。

F 836 2.098071 17.1.2.17	17.1.1.100	TCP	70 10000 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 SACK_PERM=1 TSval=2139 TSecr=0
1092 3.095932 17.1.2.17			70 [TCP Retransmission] 10000 → 443 [SYN] Seg-0 Win-65535 Len-0 MSS-1452 SACK_PERM-1 TSval-3139 TSecr-0
1348 5.091245 17.1.2.17			70 [TCP Retransmission] 10000 → 443 [SYN] Seq-0 Win-65535 Len-0 MSS-1452 SACK_PERM-1 TSval-5139 TSecr-0
1605 5.856465 17.1.1.100	17.1.2.17	TCP	70 443 → 10000 [SYN, ACK] Seq-0 Ack-1 Win-65535 Len-0 MSS-1452 SACK PERM-1 TSval-6084 TSecr-2139
1713 5.857237 17.1.2.17	17.1.1.100	TLSv1.2	177 Client Hello client->server
2130 5.862488 17.1.1.100	17.1.2.17	TLSv1.2	1586 Server Hello server->client
2131 5.862490 17.1.1.100	17.1.2.17	TLSv1.2	390 Certificate, Certificate Request, Server Hello Done server->client
2253 5.871277 17.1.2.17	17.1.1.100	TCP	66 10000 → 443 [ACK] Seg=112 Ack-1765 Win-65535 Len=0 TSval=5921 TSecr=6087
2254 5.871537 17.1.2.17	17.1.1.100	TLSv1.2	1123 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
			client->serve
<			
> Frame 2254: 1123 bytes on wire (89	984 bits), 1123 bytes c	aptured (8984 b	its)
> Ethernet II, Src: Femrice_01:53:c7	7 (68:91:d0:61:53:c7),	Dst: Femrice_01	:53:c6 (68:91:d0:61:53:c6)
> Internet Protocol Version 4, Src:	17.1.2.17, Dst: 17.1.1	.100	
> Transmission Control Protocol, Src	Port: 10000, Dst Port	: 443, Seq: 112	, Ack: 1765, Len: 1057
Secure Sockets Layer			
> TLSv1.2 Record Layer: Handshake	Protocol: Certificate		
> TLSv1.2 Record Layer: Handshake	Protocol: Client Key E	xchange	
> TLSv1.2 Record Layer: Handshake	Protocol: Certificate	Verify	
> TLSv1.2 Record Layer: Change Ci	pher Spec Protocol: Cha	nge Cipher Spec	
> TLSv1.2 Record Layer: Handshake	Protocol: Encrypted Ha	indshake Message	2