

Supernova 测试仪 HTTPS 国密认证配置

网测科技

2021-01-19





1.	文档说明
2.	配置 SSL 证书套件
	2.1 上传证书文件
3.	用例配置及运行
	3.1 HTTPS 国密不认证
	3.1.1 新建用例
	3.1.2运行界面
	3.1.3 查看报文
	3.2 HTTPS 国密单向认证
	3.2.1 新建用例
	3.2.2 运行界面10
	3.2.3 查看报文10
	3.2.4 认证失败1
	3.3 HTTPS 双向认证12
	3.3.1 新建用例12
	3.3.2运行界面14
	3.3.3查看报文14
	3.3.4 认证失败1



1. 文档说明

本文档主要介绍 HTTPS 国密算法认证配置和测试过程。本产品实现的是国密的 SM3 摘要算法,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

国密证书套件配置,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。系统有一个默认国密证书套件,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。

			対象名称	戰以關密SSL证书審件				
				☆法学符狭型: AZ/82/09/:/-/_(不支	 制作文符号)			
SL证书寄件 ②								
CAILEBIC								
			签名证书文件	gmssl_ca_sum.cer	2			
				*证书文件的扩展和公顷为:[cer] *证书文件的编码模式必须为PEM编码 (图) *允许的文件名称:英文、数字和符号	lase64编码)			
服务器证书配置								
	加密证书文件	gmssl_enc_server_sum.cer 🛃				签名证书文件	gmssl_sig_server_sum.cer	
		* 証地交相部が開発が現代):[cer] * 証地交相的論明相式の(成为PEN編明 (版Base64編明) * 元神紀文神名称: 第二、数字和符号					* 征书文州的扩展者必须为:[cer] * 征书文州的建築地位の初方にM属码(図Base64 * 行用的文件名称: 美文、数学和符号	余 (5)
	加密私销文件	gmssl_enc_server_sum.key				签名私物文件	gmssl_sig_server_sum.key	
		*私物文件的計算者必须为:[key] *私物文件的编码格式必须为PEN编码(图Base64编码) *允许的文件名称:两文、数字和符号					*私物文件的扩展名必须为:[key] *私物文件的编码输送必须为PEM编码(图Baset4 *允许的文件名称:英文、数字和符号	(第33)
	加密私胡密码	Supernova@netiTestTechnology				签名私钥密码	SuperNova@NetTestTechnology	
		* 君所造用的制银文件未必量使得,该项可量交 * 允许的建筑格式:英文、数字和符号 * 最終为255个字书					* 若所造用的私朋文件未设置安码,该项可置空 * 允许的密码格式: 英文: 数字和符号 * 最长为235个字句	
客户端证书配置								
	加密证书文件	gmssl_enc_client_sum.cer				签者证书文件	gmssl_sig_client_sum.cer	0
		* 这些文神的扩展者必须为:[cer] * 证书文评的编码推动应该为PEM编码(图Base64编码) * 元冲和文中名称: 建文、数字和符号					* 运书文用的扩展名公顷为:[cer] * 运书文用的编码地区必须为PEM编码(即Base64 * 元消的文件名称: 美文、数字和符号	(HEE)
	加密私销文件	gmssi_enc_client_sum.key				签名私钥文件	gmssl_sig_client_sum.key	
		* 私知文中的計"勝名公司力:[key] * 私知文中的論詞構成公司为Ent编码(图Based-2编码) * 允许的文件名称: 英文、数字和符号					* 私物文件部計量者必须为:(Jay) * 私物文件的编码编式必须为FEM编码(图Basesa * 允许的文件名称:英文、数字和符号	(第23)
	加密检测密码	SuperNova@NetiTestTechnology				签名私初密码	SuperNova@NetiTestTechnology	
		* 若所透用的私相交并未设置密码,该项可置空 * 允许的密码格式:英文、数字和符号 * 最长为255个字节					* 若所透用的私物文件未定量密码,该项可量空 * 允许的密码推动:英文、数字和符号 * 最长为235个字节	

2.1 上传证书文件

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, SSL 证书套件类型选择国密。

◎ 网测科技			V20.12.06	Supe	rnova-88D					
网络拓扑	SSL证书查件									
协议线选项 SSL证书案件	・ ・ 電話 2 動物 点击増加一个SSL 证书者件 KU/1線不低機相、月底時時時代表、這些意識相違的構成量、比較原情局、发生参数、現点の表現、現用一个新的分散、进行操作。									
TCI BIOK	□ 编号 名 7	编辑	克隆	导出	关联股量					
income and	1 默认1024Key-55L要件	1	2	R	6					
*************************************	2 野山2048Key-SSL搬件	1	20		1					
HTTP事务列表	3 数以面临551迁并撤往	1	创	B.	0					
TCP流模板	墾示行號: 10 🗸 1-3 of 3				< 1 >					
媒体对象										



3)选择相应的证书文件上传系统,保存。



3. 用例配置及运行

3.1 HTTPS 国密不认证

HTTPS 国密认证方式为"不认证"时,用例配置只需要服务器证书配置。

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。

	IP版本
受测设	备工作模式 💿 透明模式(TP) 😨
	○ 路由模式(NAT)
	网络配置 默认模板 ~
	靖□绑定 □



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_2	2210119-08:44:43	测试时长(时分秒) 0 ;	10 0	
	合法学符类型: A-Z/a-z/0-5	9/:/-/_(不支持中又符号)	測试在配圖可长后日初起來。這	地位时长不稳超过999小时	
网络 参数 存网络设置 客户端 port1 port2 port3 pc	Q 限速 AF		■ ■ 服务端 port5 port5 port7 port3	5	Remo:
2 茶用鏡口		MAC 68:	10:63:47:b4 Ø 禁用骗口		MAC 68:91:d0:63:4a:
CPU核绑定			▼ CPU核绑定		-
报文捕获			▲ 报文捕获		-
	协议类型		速率与MAC		•
	ID-HD-H-I-	SALESARINARSARILL, JORJAN MINISHER	QinQ (飾用)		•
	11 Albai	課IP地址或者目的IP地址,例如17.1.1.2	子网 0		+ 添加子网 。
	第口		篇1个子网		由 移除子网 ◎ 禁用子网
		源跳口或者目的跳口,例如80	测试仪画□□P地址或范围	17.1.1.100	0
	Pcap文件大小		测试仪端口子网掩蔽	周 16	0
		pcap文件大小, D - 2000MB (默认)	虚权路由	17.1.254.2	
	播試包数	范围: 0 - 6000000 (默认)	测试仪端口网	¥ 17.1.1.1	
速率与MAC			- VLAN I	D 1	0
			乙四倍		

3) 点击 客户端,编辑设置客户端证书认证配置,允许的 SSL 版本选择国密,证 书认证方式默认不认证, SSL 加密套件选择 ECC-SM4-SM3。

基本信息(HTTPS新建)	
用制容称 Https:Cps_TP_admin_20210119-08:44-43 会法学符號型 み2 / a=2 / 0-9 / 1-1」(不支持中文符号)	構成性学校(4550年) 0 10 : 0 現在生産活性が成立になった。現在なたで不能能になってきて
网络 参数 限速 高户端 服务器 记录	
SSL选项	•
静政分	287 <u>回回 697</u> 光行以上回訳, 不利2025以, Ann(仮文,
PSK/SRP用/P	VSG0PE32g1gecntoyUbername
PSK/SRPB	词 password PXXXI20PILE#Phase-of-race/Fassword
允许和JSSL	年 3543 日 1547.0 日 1547.1 日 1547.2 図 開発の13 556 日本 1557.5 日本 1
证书认证	
正形认证失效的	 ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・
SSLJDB	HT BIFFRE
	☑ ECCSM45M3
文件3	2歳 載以155年市間党文件 図 2 日 HTTP電気和201412歳 可以出版→一位素多个文件、文学中の可以使用の病定量
変編3	
	(FEELENERS) (2011) - Constructional Construction Construction (Construction)
	840 677 BXA

4) 点击 服务器,编辑设置服务器证书认证配置,服务器证书配置选择 2.2 章节 配置的 SSL 国密证书套件,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 (HTTPS新建)				
用例名称 Https 合法字符	iCps_TP_admin_20210119-08:44:43 研題: A-2 / a-z / 0-9 / : / - / _ (不支持中文符号)	测试时长(时分秒)	0 : 10 ; 测试在配置时长后自动结束,测试时长不能超过999小时	0
网络参数限	3連 客户端 服务器 记 HTTPS服务器編口 服务器证书起置 HTTP回应先	22 443 HTTPS服装器(1日、 振振 0 - 65.535 家の風間なら見中的時本 (1日) 御り時に起からし見中的は+0日間別 後近 中的点前の) Someric Sign(10) Content-Type: Leadhaml		



3.1.2 运行界面

					V20.12.06 \$	upernova
HTTPS新聞 教徒用中: admin	用例名称 <u>HttpsCps_TP_adm</u>	in_20210119-08:44:43				
建结果	-	状态 用MREA S11 至年以至失败消度			网络层	
12 168 16 228 - Port1	200	Conversion			急和 単滑 多指 广播	
	1.408	应用层		^		
2 168 16 228 - Port2	100		1911	总数 ^	192.168.16.228 - Port1	40. 4
TTP_新建建车	1,536	HTTP_新建速率	4,566	615,535	10X1990 5.6	69 711.7
12.168.16.228 - Port3	00	HTTP_请求建图	4.566	616,170	NOCES 7.0	// 889,8
TTP NERAL	1,508	HTTP_REER2xx	4.566	615.535	192.168.16.228 - Port2 8	ML
2.168.16.228 - Port4	6011	HTTP_回应码3xx	0	0	11×1500 6.1	81 775.9
TP_#REE#IE	114	HTTP_国应码4cx	0	0	102 LEE 10 220 Days	17 970.1
2.168.16.228 - Port5	2011	HTTP_周臣與5xx	0	0	192.168.16.228 - Port3	10 5
TP_新建速率	0	HTTP_请求中新	0	0	56.03900 0.0	09 759.3
2.168.16.228 - Port6	200	HTTP_请求超时	0	25	80002	48 949,1
TP 新弹速震	0	HTTP_平均时候(00秒)		2,999	192.168.16.228 - Port4	น ร
	•	HTTP_@/J4782 (826)		41	- BOCHER -	61 22300
0 ME 65		HTTP_最大时延(即秒)		400,105	BBR	
		HTTP_SSL主动属手成功	4,566	616,170	and the second se	
2.168.16.228 - Port1	82N	HTTP_SSL被助握新成功	4.660	616.557	18/4	
研教課任政量	50.000			~	102 168 16 228 - Port1	MP-
获字节数量	14,836,340				(二) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	21
交捕获	(重度) 已经带止 (下載)	信頼長 0		<u>^</u>	THE WORK	10
2.168.16.228 . Port2	939	皇和 port1 port2 port3 port4 port5 port6 port7 port8		^	192 168 16 228 - Port2	M
存取描名政府	0				法册编收	23
民学节数量	0		640	总数	流展波涛	10
time:	(重度) 已经停止	TCP_主动标键进展	4,567	618,605	192,168,16,228 - Port3	M
12 168 16 228 - Port3	0.00	TCP_王动嵯纷渐缓	4,568	618,549	流動爆攻	22
CONTRACTOR IN CONTRACTOR OF CONT	0	TCP_RENDERED T	4.568	618.549	流量发送	10.
成本行動量	0	「い」二朝王が汗波範囲		256	192.168.16.228 - Port4	Mb
文欄 存	(ERI PR#)			267	120100	
在资源	<u> </u>	10.P_#0201100000000		610,447	用例管理	
				620,443		
称 占用	总数	TCP_STORMONOUTS	17	616,404	用制名称	用户名称 运行
統內存 52.64% 47	(36% 64322 MB	ILF_ENTERSONE	13	6,711	HttpsCps_TP_admin_20210119-08:44:43	admin IE6
英内存 1512 86.75%	30656 MB	ICT_INVICETYON (MM2)		3,181		

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

3.1.3 查看报文

报文中可以看到 GMSSLv1 的握手过程和服务器所使用的证书信息。

No.	Tine	Source	Destination	Protocol	Leagth	SrePert	DatFort Info		
Г	403 3.035238						443 10000 → 443 [SYN] Seq=0 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 MSS=1452 SACK_PERM=1		
	659 3.036430	17.1.1.100	17.1.2.2	TCP	62	443	10000 443 + 10000 [SYN, ACK] Seq-0 Ack-1 Win-65535 Len-0 MSS-1452 SACK_PERM-1		
*				GMSSLv1			443 Client Hello client → server		
	1102 3.041562	17.1.1.100	17.1.2.2	GMSSLv1	1228	443	10000 Server Hello, Certificate, Server Key Exchange, Server Hello Done Server → client		
	1217 3.843878	17.1.2.2	17.1.1.100	GMSSLv1	311	10000	443 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message <u>client</u> → server		
	1610 3.125583	17.1.1.100	17.1.2.2	GMSSLv1	145	443	10000 Change Cipher Spec, Encrypted Handshake Message server → client		
				GMSSLv1	219	10000	443 Application Data		
	2195 3.186212	17.1.1.100	17.1.2.2	GMSSLv1	203	443	10000 Application Data		
L	2196 3.186241	17.1.2.2	17.1.1.100			10000	443 10000 → 443 [RST, ACK] Seq=475 Ack=1407 Win=65535 [TCP CHECKSUM INCORRECT] Len=0		
<									
v s	ecure Sockets Layer								
>	GMSSLv1 Record Layer:	Handshake Protor	ol: Server Hello						
~	GMSSLv1 Record Layer:	Handshake Proto	ol: Certificate						
	Content Type: Hand	shake (22)							
	Version: GMSSL 1.0	(0x0101)							
	Length: 1023								
	✓ Handshake Protocol	: Certificate							
	Handshake Type:	Certificate (11)							
	Length: 1019								
	Certificates Len	gth: 1016							
	✓ Certificates (10)	16 bytes)		服务器端证书文件信息					
	Certificate Length: 592								
	> Certificate:	308201f2308201990	20900c6248e6989fa82c9300a06082a (pk	cs-9-at-emailAddress	=server@test.c	om,id-at	commonName=server,id-at-organizationalUnitName=Test Group,id-at-organizationName=Neti Software,id-at-localityNam.		
	Certificate L	ength: 508							
	> Certificate: .	308201+83082019d0	20900c6248e6989fa82ca300a06082a (pk	cs-9-at-emailAddress	=server_enc@te	st.com,1	d-at-commonName=server,id-at-organizationalUnitName=Test Group,id-at-organizationName=Neti Software,id-at-localit		
2	GMSSLv1 Record Layer:	Handshake Proto	ol: Server Key Exchange						
1 2	> GRSSLVI Record Layer: nandsnake Protocol: Server nello Done								



3.2 HTTPS 国密单向认证

HTTPS 国密证书认证方式为"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。

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。

网络配置 默认模板 >
端□绑定 □

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(HTTP\$新建)									
用例名称 HttpsCps_TP_adn 台法字符类型 A-Z / a	min_20210119-09-05-39 b-z / 0-9 / : / - / _ (不安培中交符号)	教徒时长(时分秒) 0 · · · · · · · · · · · · · · · · · ·	10 : 0						
网络参数限速 有	户端 服务器 记录								
保存网络@重 客户端 port1 port2 port3 port4		服务端 port5 port6 port7 port8							
◎ 常用演□	MAC 68:91:d0:63:47:b4	⊘ 葉用跳口	MAC 68:91:00:63:4a.cc						
CPU核绑定	•	CPU核绑定	•						
报文捕获	*	报文捕获	•						
10	120 金部 ~	速率与MAC	-						
	请选择协议的类型,无案示不应用原因	QinQ (###)	•						
	IP地址 SintensiveteExemptos 20071112	子网 😡	+ 添加子网 🔺						
	2017 KOALINYH EINI3Y KOAL, 990417.1112	第1个子网	◎ 移除子网 ② 颜用子网						
	潮涛口成者目的講口,使約800	测试仪施口IP地址或范围	17.1.1.100						
Pcap文	2件大小	测试仪端口子网播码	16						
	ptap文件大()、0 - 2000/MB (新认)	虚拟路由	17.1.254.2						
390	BECE2版 50000 地田: 0 - 6000000 (現代人)	测试仪端口网关	17.1.1						
Land Protoco									
		子网機拟							
QinQ (訪用)	÷	1 100000	2000/00/00/						
子网 🛛	◆ 液如子同 ▲								
第1个子网 测试仪跳口IP地址	◎ 膠除子网 ② 氯用子网 公式范围 17.1.2.2·17.1.2.201								
	前动	Geter Boles							



基本信息(HTTPS新建)

3) 点击 客户端,编辑设置客户端证书认证配置,允许的 SSL 版本选择国密,证 书认证方式选择单向认证,SSL 加密套件选择 ECC-SM4-SM3。CA 证书配置选择 2.2 章节配置的 SSL 国密证书套件,使用的是其中的 CA 证书配置部分。

用例名称 Https:Cps_TP_admin_20210119-09-05-39 会法平符驾起 AZ/+z2/09/1/-/_(不变時中实符号)	第6501HE (05569) 0
网络参数 限速 春户端 服务器 记录	
SSL选项	*
靜歐美術	
	與冠ssl连腕筋,不再发进ssl Alen级文
PSK/SRP用户名	username
	PSK/SRP 再进始idently/Username
PSK/SRP電码	password PDW/DDPE3M/Dass-inhosei/Passumrd
允许的SSL版本	
	SSL版本、每个SSL版本对应的图测不一样、阐明v1.1页版色影GECC SM4 SM3
证书从证方式	O xute ● #mute O xubite
	SSI墨手阶段。 服务管理进行中, 查内特地理CA在中的资产中的有限进行认证
CALEDROR	■2000年3月19日
证书认证失败的处理	● 终止SSI握手, 新开socket建築 ○ 務勝并還出國家运行
	图#SSUE 书以证书的推动作
SSL力BE微件	选择新有 取消所有
	☑ ECC-SM4-SM3
2,114,31,88	
变量列表	无 🗸 🕼
	HTTP POST意数中,可以引用安量列表,完成安量的意数化。
	15:30 1677 1838

4) 点击 服务器,编辑服务器证书配置,服务器证书配置选择 2.2 章节配置的 SSL国密证书套件,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(HTTPS新建)		
用例名称	Https:(ps,TP,admin,20210119-0900539 制設的 前途中認識 A27+a2/0-97777_(不認時中交符号)	任 (8595) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
网络参数	限速 客户端 服务器 记录	
	HTTPS語外語版口 43 HTTPS語外語版口46, 加強 0-65355 家の描述で快速器 家の描述の公式年春年 () 2 3 (第778年20日) 中でで、何の(1735) Content Syst Landford Content Syst Landford	
	前动	200



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 测试用户: admin	用例名称: <u>HttpsCps_TP_admin</u>	20210119-09-05-39					
動構果	-	状态 用例释述 551证书认证共数详细			网络层		
2 168 16 228 - Port1	600T				(1)和 年間 (15月) 「日間		
TP RSPIRE	1,216	極用层		•			
2.168.16.228 - Port2	1240		砂值	en ^	192,106.10.228 - PORT	610	256.2
TP_NEESE	1,280	HTTP_新建建在	3.823	237,573	20-01000	4,825	200,5
2.168.16.228 - Port3	初度	HTTP_请求道察	3.800	237.988	102.469.46.929.0	10039	
TP_新建速率	1,264	HTTP_周压码2xx	3,823	237,573	192.100.10.220 - PORZ	640	222.44
168.16.228 - Port4	96	HTTP_ 周空码3cx	0	0	1200 BIA	6 705	2/0.2
FP_新疆連案	55	HTTP_INEH4xx	0	0	103 169 16 239 Bort2	0,300	540,51
168.16.228 - Port5	96	HTTP_周弦码5xx	0	0	12-1-10-10-20-POILS	4964	270.2
P_#REE	0	HTTP_请求中断	0	0	TRANKA Contract	4,704	200,20
.168.16.228 - Port6	80	HTTP_请求题时	0	9	103.168.16.339 Dourd	404	337.3
P_教授建築	0	HTTP_平均时运((20约)		3,499	192.100.10.220 - POIL4	170	
		HTTP_@04356 (896)		42	JILXIAKI	3/3	101.11
an ar	^	HTTP_最大时间(20秒)		200,088	後期层		
	0	HTTP_SSL主动属手成功	3.799	237,988	have:		_
2.168.16.228 - Port1	28	HTTP_SSL被迫握手成功	3.804	238,261	1846		
7数强位数量	50,000	HTTP SSLIL还完成	0	0 *	192.168.16.228 - Port1		Mbs
末字 节数量	14,836,504	#10F 0			流艇等效		18.1
29612	(三部) 已经停止 (下部)	Trathe U		-	流量发送		8.4
2.168.16.228 - Port2	28	参和 port1 port2 port3 port4 port5 port6 port7 g	port8	^	192.168.16.228 - Port2		Mbp
和評判政章	0				流量接收		19.1
将于节数量	0		Dill	88	洗量发送		8.1
7005	(憲會) 已经停止	TCP_EX7#value#	3.816	243,554	192.168.16.228 - Port3		Mb
168 16 228 - Port 3	450	TCP_EXTREMENT	3.819	245,525	流量接收		18.3
201010-0107-01		1CP_READERD	3,819	245,525	流量发送		8.7
+ <u>北</u> 市政局	0				192.168.16.228 - Port4		Mbp
71612		TCP_markstorr3200m		281	流量操改		1.4
				0			
(資源	A	1.cr_mmoni(#55)83/0		0	用例管理		
				244,745			_
な お と 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	の数	IC-MARKEDOGUESE		241,924	用例名称	用户名称	运行
先内存 52.69%	47.31% 64322 MB		12	4,347	HttpsCps_TP_edmin_202101194	09:05:39 admin	正在
页内存 132 86.739	6 30656 MB	ICP_±RIMRE+RIPISE (6007)		3.603			

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。

No. Tine	Sauroa	Jestination.	Troteoel Lengt	h SreFort	DatFort Info	
F 403 3.026903	17.1.2.2	17.1.1.100	TCP	62 10000	443 10000 → 443 [SYN] Seq=0 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 MSS=1-	452 SACK_PERM=1
659 3.032293	17.1.1.100	17.1.2.2	TCP	62 443	10000 443 - 10000 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=	1
714 3.032440	17.1.2.2	17.1.1.100	GMSSLv1	106 10000	443 Client Hello	
1102 3.037351	17.1.1.100	17.1.2.2	GMSSLv1	1220 443	10000 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
1217 3.039737	17.1.2.2	17.1.1.100	GMSSLv1	312 10000	443 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
1610 3.140469	17.1.1.100	17.1.2.2	GMSSLv1	145 443	10000 Change Cipher Spec, Encrypted Handshake Message	
1750 3.180575	17.1.2.2	17.1.1.100	GMSSLv1	219 10000	443 Application Data	
2195 3.194378	17.1.1.100	17.1.2.2	GMSSLv1	203 443	10000 Application Data	
L 2196 3.194406	17.1.2.2	17.1.1.100	TCP	60 10000	443 10000 → 443 [RST, ACK] Seq-476 Ack-1407 Win-65535 [TCP CHECKSUM INCORR	ECT] Len-0
<						
Version: GMSSL	1.0 (0x0101)					
Length: 1023						
✓ Handshake Prot	ocol: Certificate					
Handshake Ty	pe: Certificate (11)					
Length: 1019	9					
Certificates	s Length: 1016					
✓ Certificates	(1016 bytes)					
Certifica	te Length: 502					
Certifica	te: 308201f230820199020900c	6248e6989fa82c9300a06082a (pkcs-9-at-emailAddress=serv	er@test.com,id-at	-commonName=server,id-at-organizationalUnitName=Test Group,id-at-organization	Name=Neti Software,id-at-localityNam.
✓ signed	Certificate					
seri	alNumber: 14277693302608921	1289				
> sign	ature (iso.2.156.10197.1.50	91)			no de prover de letteres	
> issu	er: rdnSequence (0)				版务器证书信息	
> vali	dity					
> subj	ect: rdnSequence (0)					
> subj	ectPublicKeyInfo					
> algorit	thmIdentifier (iso.2.156.10	197.1.501)				
Padding	1: 0					
encrypt	ted: 304402202f54584b218e82	2fbf9080584f864a56b2aba24c				
Certifica	te Length: 508					
✓ Certifica	te: 308201f83082019d020900c	6248e6989fa82ca300a06082a (pkcs-9-at-emailAddress=serv	er_enc@test.com,i	d-at-commonName=server,id-at-organizationalUnitName=Test Group,id-at-organizat	tionName=Neti Software,id-at-localit
✓ signed	Certificate					
seri	alNumber: 14277693302608921	1290				
> sign	ature (iso.2.156.10197.1.50	31)				
> issu	er: rdnSequence (0)					
> vali	dity					
> subj	ect: rdnSequence (0)					
> sub1	ectPublicKeyInfo					
> algorit	thmIdentifier (iso.2.156.10	197.1.501)				
Padding	2: 0					
encrypt	ted: 3046022100d73313b619be	0da6d43f677451773cf39bae5c				
> GMSSLv1 Record La	ayer: Handshake Protocol: 5	erver Key Exchange				
> GMSSLv1 Record La	aver: Handshake Protocol: S	erver Hello Done				
	-					



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 证书配置选择默认国密 SSL 证书套件,服务器证书配置选择其他的国密 SSL 证书套件。

	用例名称	HttpsCps_T	P_admin_202	210119-09:13:24	~17.8k		現成の計法(約5分秒) 0 ; 10 ; 0 日日 10 : 0 日日 10 : 0
网络	***	限速 】	秦户端	服务器	Y	记录	
SSL选项				1	1		•
						粉浆	HERE RESS. Average.
						PSK/SRP月	PSC 309 #325/gendty/Username
						PSK/SRI	客研 password PSr/SSP端注能Plass-binase/Password
						允许的SS	
						证书认证	D 生代性
						CAIE	33.2019年8. 图382020年8月,每770年8月47年9月年9月8日9月20日 图 图: 100,2019年9月 图 CA证书选择国密SSL证书套件,服务器编证书选择不一致的其他证书套件 Paragewore underforce are segment
					证书	认证失败的	○ #此555.20年、新开始の考虑後期 9 局間神道出現実計で 出版のに注41.12年後町198月市
						SSL108	家:: 24所作 102所作 [E] CCC3M-945
						文件	939 BULING THREAD: V C 🕀
						变	
							HTTP PGST§BR/P, PLUGHREELMUB, JOSEELMUSPBROZ,
							ELD 677 008
基本信息 (HTTP	s新建)						
	用例名称	HttpsCps_T	P_admin_202 A-Z / a-z / 0-9 /	210119-09:13:24 /:/-/_(不支持中)	文符号)		RE2015年(8559日) 0 : 10 : 0 別に広志院哲学を告知な知。別にからうな話にないのとき
网络	参数	限速	客户端	服务器		记录	
					нтт	rps服务翻	R[443
					85	经务额证书	HTTPE問題報題49. 他想 0- 05.335
						HTTPE	(思知)(記述)(以上)(王明(中午))(認得論正)(新述)(注 (注)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)
							Constra (ype, texurum
0		コノナ・レ	<i>x</i>	≺டா	L.	L.	
2)月]例]	区门	「大火	χ,	1	诸提示各尸端验证服务器证书失败。
	测科技 litest.com	W	一 资源	開設		E2	送 前 名 服告 新統 admin V20.12.06 Supernova-88D
							▲ 生№



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。

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。

IP版	本 ● v4 ○ v6 ○ 混合
受测设备工作模式	式 💿 透明模式(TP) 🚱
	○ 路由模式(NAT) Ø
网络配	至 默认模板 ~
端口绑;	

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_adm 合法字符类型: A-Z / a	in_20210119-08:44:43 z/0·9/:/-/_(不支持中文符号)	测试时长(时分秒) 0: 测试在配算时长后自动结束。测试	10 : 0 武时长不能超过999小时
网络参数 限速	客户端 服务器 记录		
端设置 白端 rt1 port2 port3 port4		服务端 port5 port6 port7 port8	
朝田	MAC 68:91:d0:63:47:b4	◎ 藤用端口	MAC 68:91:d0:63:4
CPU核绑定	•	CPU核绑定	
报文捕获	•	报文捕获	
协议	2世 全部 ~	速率与MAC	
	请选择协议的类型,无表示不启用抓包	QinQ (鮮用)	
(P)		子网 😧	+ 滾加子网
		第1个子网	自 移除子网 ② 禁用子系
	滚端口或者目的端口 ,例如80	测试仪端口IP地址或范围	17.1.1.100
Pcap文件:	专小	测试仪端口子网掩码	16
1.000	pcap文件大小, 0 - 2000MB (默认)	虚拟路由	17.1.254.2
清 次1	13歳 50000 范囲: 0 - 6000000 (武法)	测试仪端口网关	17.1.1.1
東率与MAC		VLAN ID	1 🛛 🖓
		乙烷烯的	CT MALE (1920 Arr Inte



HTTPS 国密算法认证配置

3) 点击 客户端,编辑设置客户端证书认证配置,允许的 SSL 版本选择国密,证 书认证方式选择双向认证,SSL 加密套件选择 ECC-SM4-SM3。SSL 握手阶段,服 务器发送证书,客户端使用 CA 证书对证书内容进行认证,且服务器要求客户端 提供证书,并使用 CA 证书对证书内容进行认证。

38年1月25(HTTF3新姓)	
用例名称 Https:Cps_TP_admin_20210119-09:19:07 合法字符描述 A-Z / a-2 / 0-9 / : / - (不支持中文符号)	(第22日時代(1955年)) 第1日本(1955年)(19557)(19577)(19557)(19577)(195
网络参数限速 有户端 服务器 记录	
SSL选项	•
静默关闭	- 第211 - 第212 -
PSK/SRP用声名	username
PSK/SRP翻翻	P2/GSI984848deerosylubername password
方行神韵 SSL版法。	PA/JANE BARANCE PRIMA PRIMA PARAMAN SSN 201 − SN 40 − SN 40 − SN 42 (C) BR(4/1) SSN 201 − SN 40 − S
证书以证方式	
こん近半路道	
寨户纳证书配数	の世界におけないに可能すべきないですなどのなどのない 載込ん開始なんに手術部件 ぼぼ (注)
	使用所造的553、征书案件中的客户端还有起票额分
证书认证失暇的说话题	●後止SSI標準、新行Socket連線 ○ 投稿并退出爆斥运行 はExecutionには同じになる時かが必要が
SSL加密额件	
	CC COMP SND
文件对象	取扱い56季节発売文件 マ 2 日 HTT予算機会会社事業 Tubble 一般語書の提供 2 2 1
安徽列表	
	E3th 0377 1008

4) 点击 服务器, 配置服务器端国密证书套件, 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)			
用例名称 HttpsCps_T 合法学符提起,	P_admin_20210119-09-19-07 A27.627.097/7-7_(不说時中文符号)	RSIZ1916(195519) 0 10 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
网络 参数 限速 ((正次) HTTP/服务器() HTTP/服务器() HTTP/服务器() (日本3) (日本		





3.3.2 运行界面

HITT SAME AGOND - HUMAN	Tuo sente						
缝结果	-	状态用网隙速 SSL证书认证失数详细			网络层		
92.168.16.228 . Port1	196	(market)			<u>总和</u> 单清 多清 广清		
TTP ROPINS	1,216	应用层		^			
92.168.16.228 - Port2	656		194 1	800 [^]	192.168.16.228 - PORTI	611	95
ITTP 教徒主要	1,200	HTTP_新建速车	3,823	237,573	500000	4.825	256.51
92.168.16.228 - Port3	6565	HTTP_请求建立	3.800	237.988	16.5	6,039	320,57
TTP \$500 (R.S.	1,264	HTTP_国应码2xx	3.823	237.573	192.168.16.228 - Port2	6940	.21
92 168 16 228 - Port4	1540	HTTP_回应码3xx	0	0	36573967	5,105	272.15
TTP \$509(A)A	55	HTTP_国应码4xx	0	0	和文定进	6,386	340,38
92 168 16 228 - Port5	1940	HTTP: 開圧弱5xx	0	0	192.168.16.228 - Port3	6940	81
TTD BORRE	0	HTTP ######	0	0	经定任权	4,964	270,26
27 168 16 238 . Borte	100	HTTP 请求提打	0	9	规文发送	6,202	337,95
TTD CAREER	0	HTTP FEBRISE (WER)		3,499	192.168.16.228 - Port4	19 <u>1</u>	8
THE DESIGNATION	~ ~	HTTP #4-1945E (80%)		42	舰文振收	379	161,18
A48.00		HTTP.最大时版(简称)		200,088	1180		
XIIIK	<u> </u>	HTTP SSL中設欄手成功	3.799	237,988	地部局		
07 168 16 228 Port1	0.00	HTTP SSLMEAN制手組动	3.804	238,261	进车		
Same water and the second s	50.000	HTTP SSLLAE供做	0	0 1	in the second se		
1711/1210-18	14 926 504				192.168.16.228 - Port1		Mbp
NOT TOTAL		传输展 ❷		^	法量接收		18,1
COMP.		His part and part part parts parts parts			流量发送		8.4
92.168.16.228 - Port2	总数	the burn burn burn burn burn burn burn			192.168.16.228 - Port2		Mbp
時参援包教量	0		90	23	流量操改		19.1
較字节数量	0	TCP 主动物理学研	3,816	243.554	流量发送		8.9
这種快	[重用] 已经停止	TCP 中設線成準備	3.819	243.525	192.168.16.228 - Port3		Mbp
92.168.16.228 - Port3	28	TOP SCHOLES	3,819	243.525	流量接收		18.7
認想強也改量	0	TCP NETAHANAN		256	流量发送		8.7
純字的数量	0	TCP HEIRFORM		281	192.168.16.228 - Port4		Mbp
	(188) PRR: Y	Tro action al Refts			流量操改		1.4
		TOP Jate Top Jack Febra			Concernance of the Concernance o		_
站资源	^	TCP #20exer#2554		244.745	用例管理		
		TCP #UReset 平民国旗		241,924			
3称 占用	22	TO BARONNA	12	4 347	用例名称	用户名称	1617
B.统内律 52.69% 47.3	51% 64322 MB	The Case of Street Stre	1.14	4,540	HttpsCps_TP_admin_20210119-0	9:05:39 admin	正在

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。

3.3.3 查看报文

报文中可以看到 GMSSLv1 的握手过程和客户端服务器所使用的证书信息。





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默认的国密 SSL 证书套件,客户端证书配置选择其他的 SSL 证书套件。

基本信息(NTTPS新建)
用物名称 NegsCpg,Tp,Janna,20210119-09-19:07 向法子符出版 AZ/ar/09/i/i/_(行法)特示公式符) 別はなどを活動がたEnsiteは、別はなどを必須から
网络 参数 限速 霍卢姆 服务器 记录
SSL造项
静静氏体現 定成 定成 定成 定成 大学院定成をSLAiver版文。
PSK/SR用本名 usemane PSK/SR用本名 pSk/SR用本名
PSk/SRP在词 password PSk/SRP第完封Pass-phrasePassword
11月1日 日本 11月1日日本 11月1日日日本 11月1日日日日日日日日日日
正年代以上支京 ○ 不以を ○ 第時以後 ● 第時時間、「日本市場」の目的時間にはそれであります。 「日本市場合での「日本市場」の目前には、日本市場は、日本市は、日本市場は、日本市場は、日本市は、日本市は、日本市は、日本市は、日本市は、日本市場は、日本市,日本市,日本市,日本市,日本市,日本市,日本市,日本市,日本市,日本市,
ACCERTANT AND ACCENT AND ACCEN
南产酶正報證 時間時回的以上考驗中的影响和回答即 時間時回的以上考驗中的影响和回答即
证##从证券物的建置 ○ ##554#新# ₩开504#活# ● #################################
El comente
文件式機
基本信息(HTTP\$标准)
勝時時後後 Https:fpg,Tp_admin_20210119-09:19:07 第時時時後後後、1952年) 0 10 0 10 0 10 0 10 0 10 10 10 10 10 10
网络参数 限速 客户端 服务器 记录
HTTPS服务機能口 443
使用UNIESSCS公式中部は中や単語的特徴生活を開始的 HTTP国語文 HTTP国語文
2) 用例运行失败,报错提示证书验证失败。

