

Supernova 测试仪 HTTPS 国密认证配置

网测科技

2021-01-19

目录

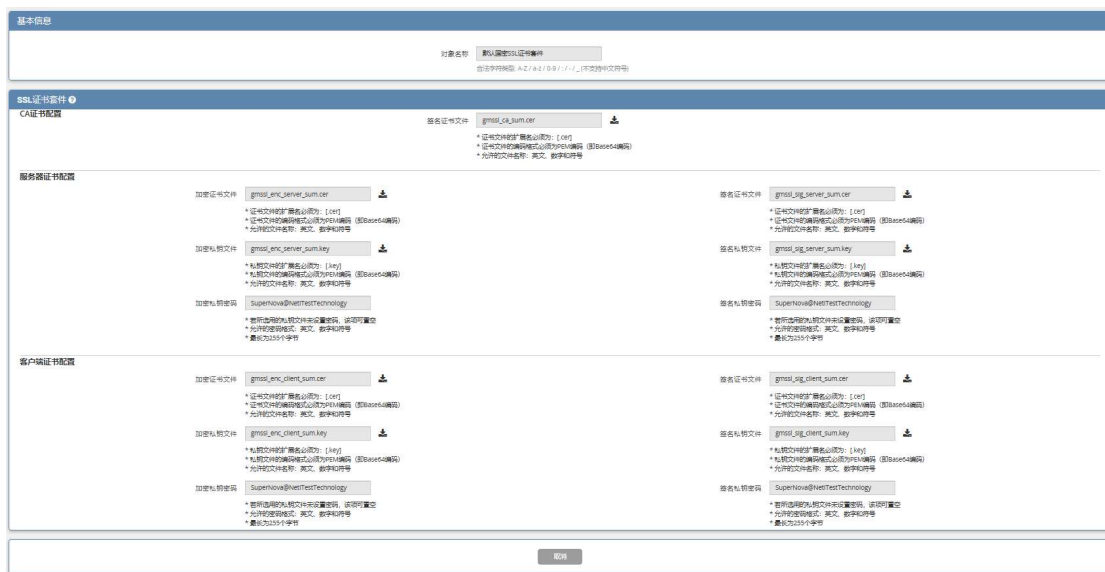
1. 文档说明.....	3
2. 配置 SSL 证书套件.....	4
2.1 上传证书文件.....	4
3. 用例配置及运行.....	5
3.1 HTTPS 国密不认证.....	5
3.1.1 新建用例.....	5
3.1.2 运行界面.....	7
3.1.3 查看报文.....	7
3.2 HTTPS 国密单向认证.....	8
3.2.1 新建用例.....	8
3.2.2 运行界面.....	10
3.2.3 查看报文.....	10
3.2.4 认证失败.....	11
3.3 HTTPS 双向认证.....	12
3.3.1 新建用例.....	12
3.3.2 运行界面.....	14
3.3.3 查看报文.....	14
3.3.4 认证失败.....	15

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。



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。



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

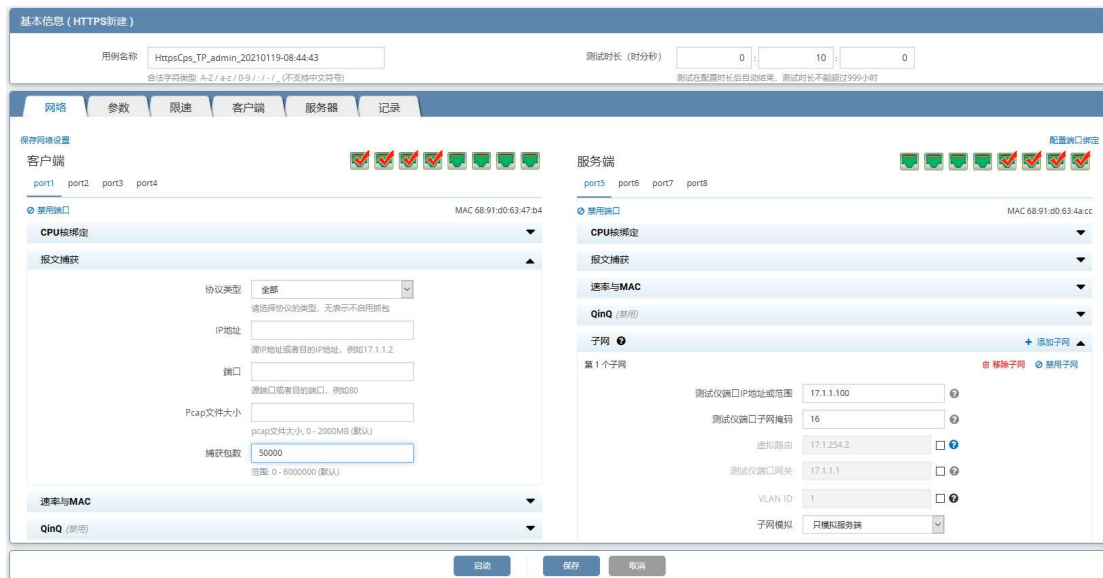
HTTPS 国密认证方式为“不认证”时，用例配置只需要服务器证书配置。

3.1.1 新建用例

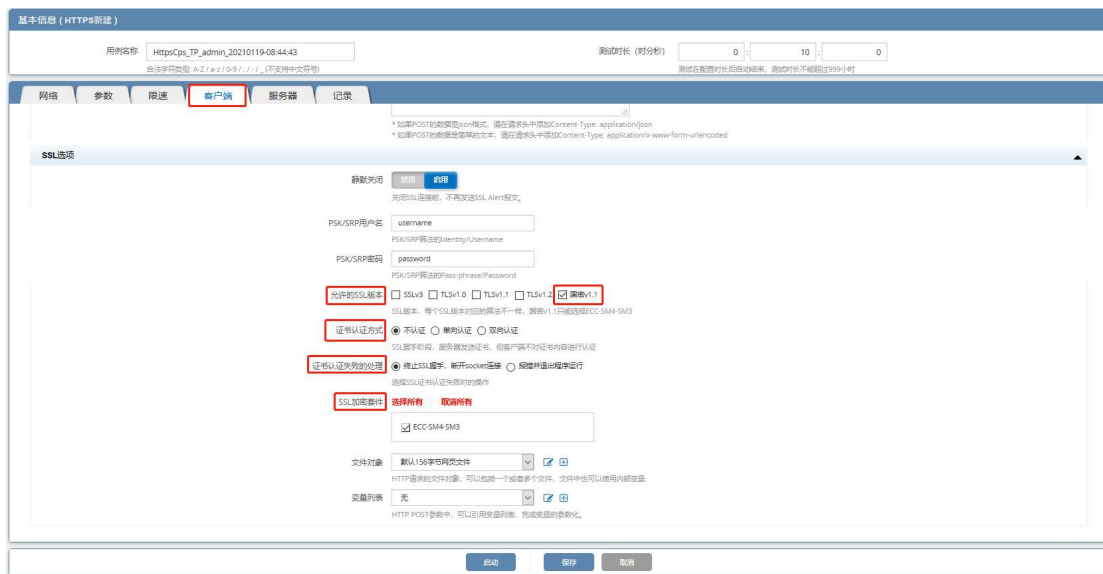
1) 通过 web 登录测试仪，依次点击用例 -> 网关设备测试 -> HTTPS -> 新建，单击增加，在弹出的选择用例选项中，编辑用例网络选项，根据需要修改配置参数，然后点击确定，进入用例配置页面。



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。



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。

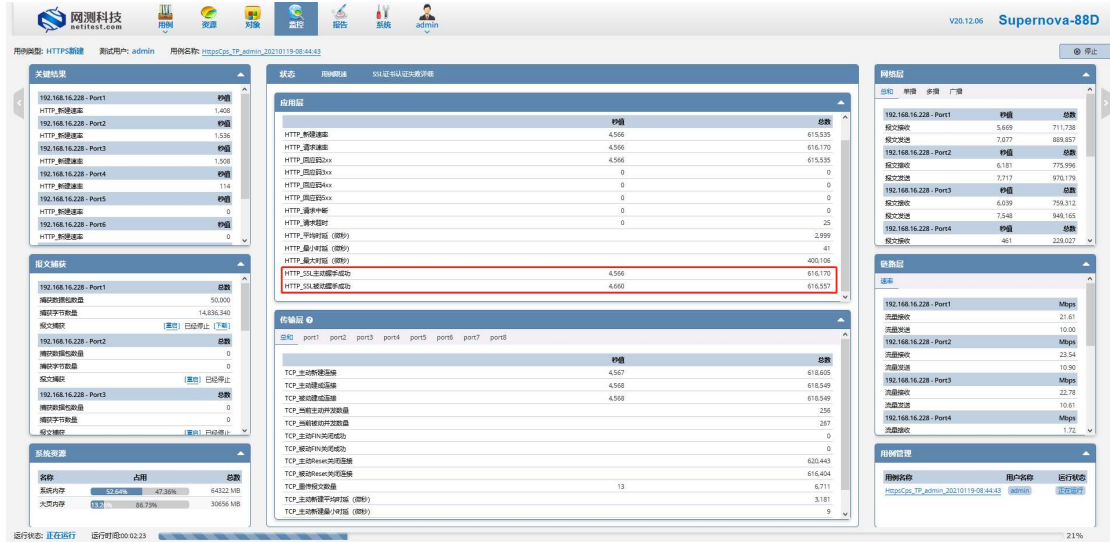


4) 点击 服务器，编辑设置服务器证书认证配置，服务器证书配置选择 2.2 章节配置的 SSL 国密证书套件，使用的是其中的服务器证书配置部分，点击保存用例的配置。



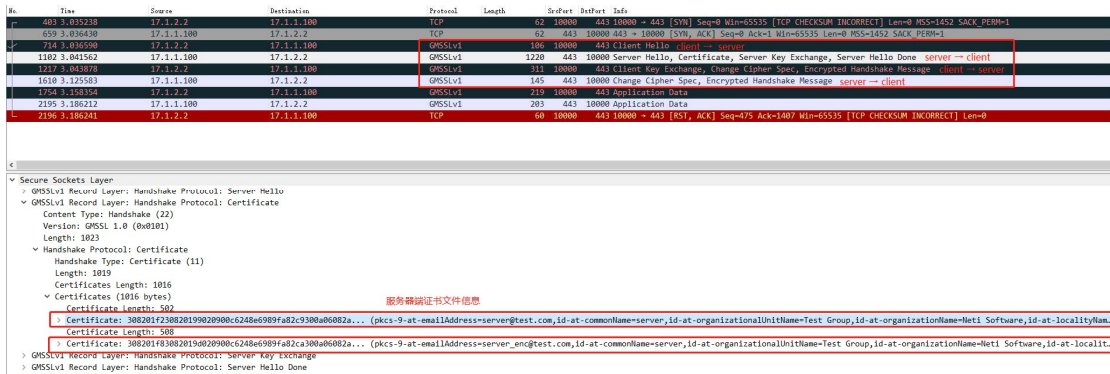
3.1.2 运行界面

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。



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。



3.2 HTTPS 国密单向认证

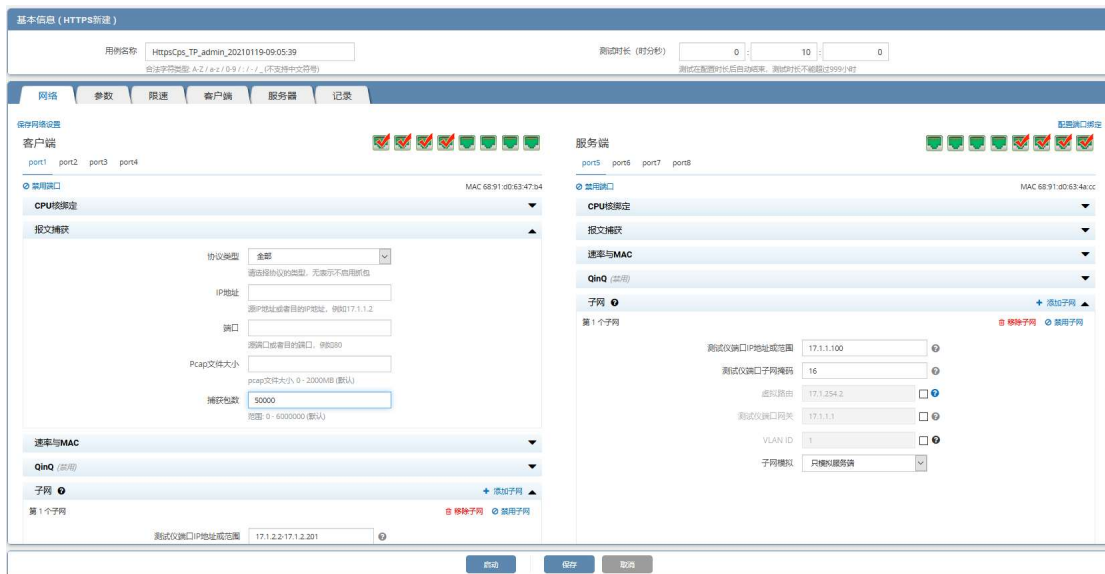
HTTPS 国密证书认证方式为“单向认证”时，用例配置需要 CA 证书配置、服务器证书配置，且服务器证书文件是通过 CA 证书文件签发的。单向认证要求服务器有证书，客户端对服务器进行验证。

3.2.1 新建用例

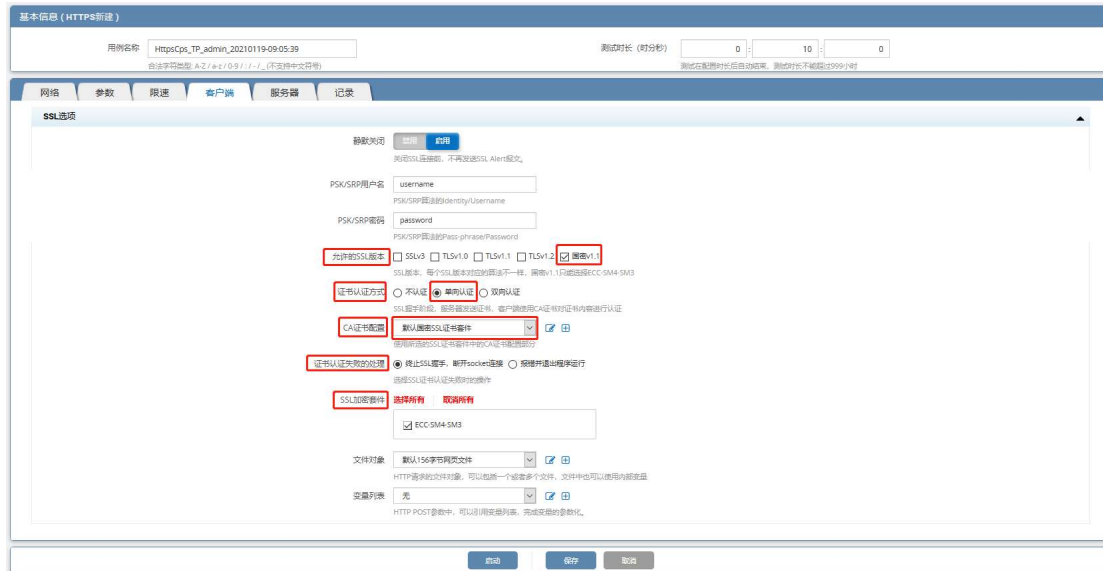
1) 通过 web 登录测试仪，依次点击用例 -> 网关设备测试 -> HTTPS -> 新建，单击增加，在弹出的选择用例选项中，编辑用例网络选项，根据需要修改配置参数，然后点击确定，进入用例配置页面。



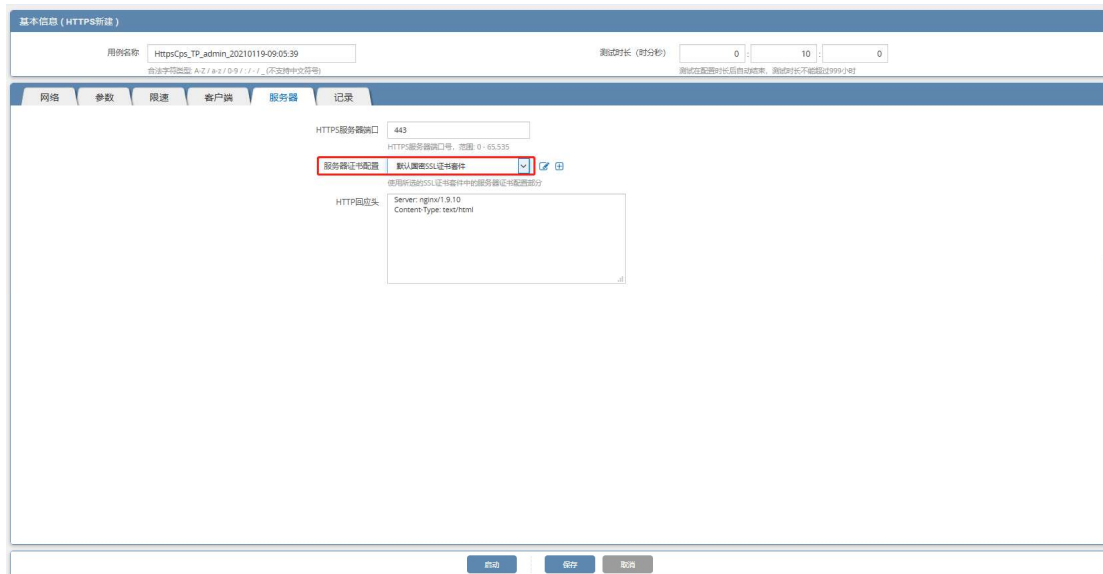
2) 进入用例配置页面，配置网络信息，可设置报文捕获查看详细报文交互。



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。

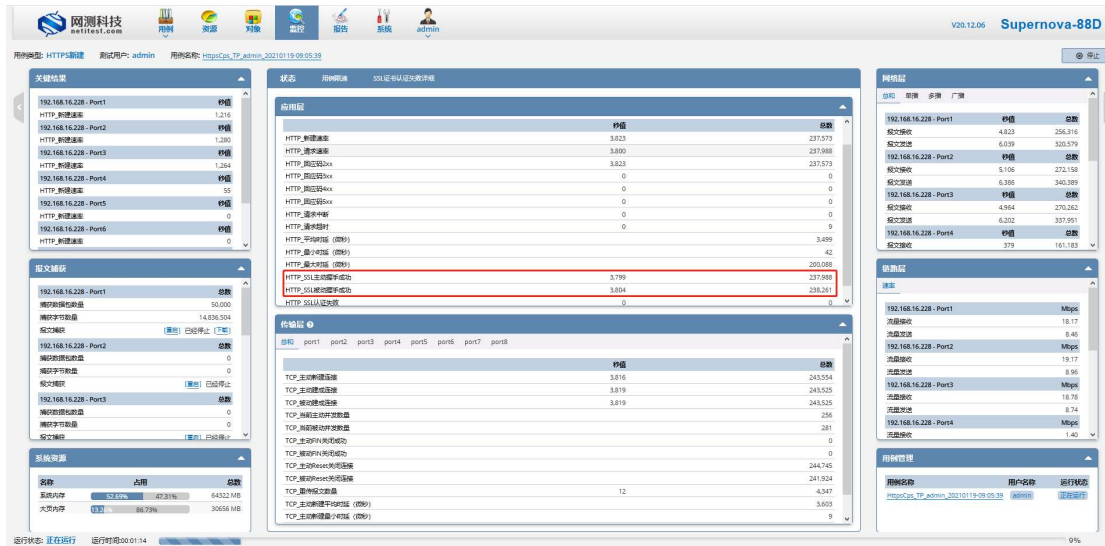


4) 点击 服务器, 编辑服务器证书配置, 服务器证书配置选择 2.2 章节配置的 SSL 国密证书套件, 使用的是其中的服务器证书配置部分, 点击保存用例的配置。



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。

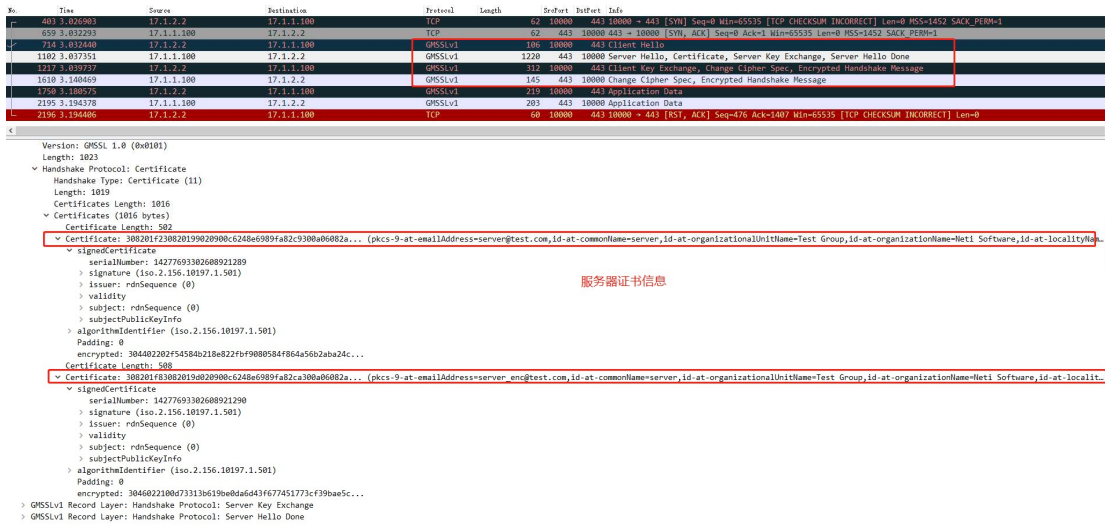


The screenshot displays the NetTest software interface during an HTTPS test case execution. The main window is titled 'Supernova-88D' and shows various monitoring panels:

- 关键配置 (Key Configuration):** Lists test cases for 192.168.16.228 on ports 1 through 6, each with a status of '秒级' (Second-level).
- 应用层 (Application Layer):** A table showing metrics for various HTTP methods and protocols. For example, 'HTTP_新建连接' has a value of 3,823 and a total of 237,573.
- 传输层 (Transport Layer):** A table showing metrics for TCP and TLS connections. For example, 'TCP_主动新建连接' has a value of 3,816 and a total of 243,554.
- 系统资源 (System Resources):** Displays system usage statistics such as CPU (52.69%), Memory (47.31%), and Disk (66.79%).
- 网络层 (Network Layer):** Shows network-related metrics for different ports.
- 用例管理 (Case Management):** A table listing the test cases being executed, including their names and execution status.

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 screenshot shows a network traffic capture tool displaying the details of an SSL/TLS handshake. The top part shows a list of captured packets with columns for Time, Size, Source, Destination, Protocol, Length, and Info. The selected packet (No. 1182) is a TLSv1.1 packet from 172.1.1.100 to 172.1.1.100, containing a Server Hello, Certificate, and Server Hello Done.

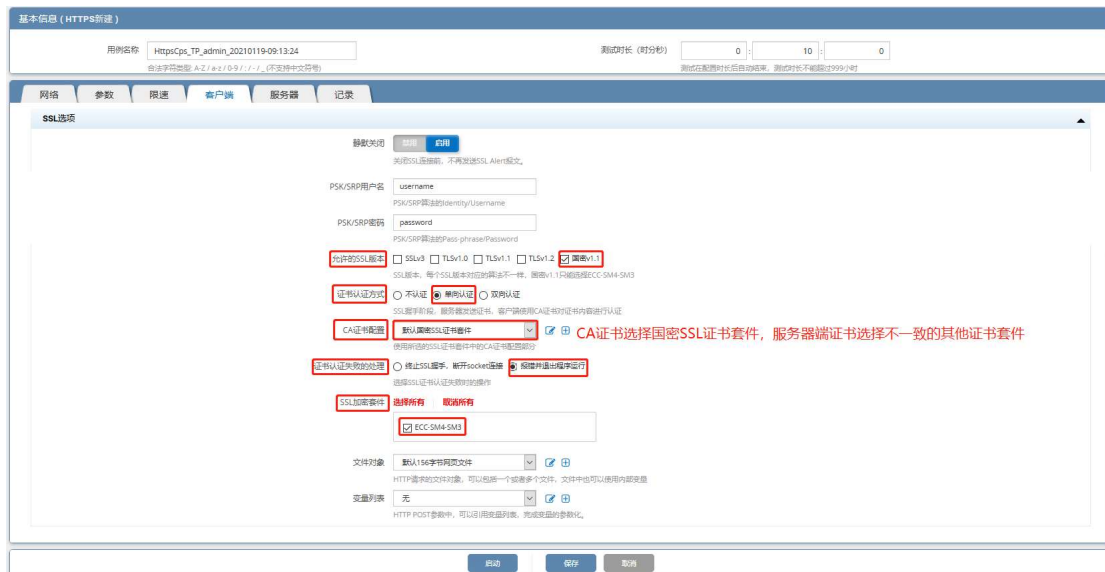
The bottom part shows the expanded details of the Certificate field, including the following information:

- Version: TLSv1.1 (0x0101)
- Length: 1823
- Handshake Protocol: Certificate
- Handshake Type: Certificate (11)
- Length: 1019
- Certificates Length: 1016
- Certificates (1016 bytes):
 - Certificate Length: 582
 - signedCertificate
 - serialNumber: 14277693302608921209
 - signature (iso.2.156.10197.1.501)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - algorithmIdentifier (iso.2.156.10197.1.501)
 - padding: 0
 - encrypted: 304402202f54584b218e822f4f9080584f864a56b2aba24c...
 - Certificate Length: 588
 - signedCertificate
 - serialNumber: 14277693302608921290
 - signature (iso.2.156.10197.1.501)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - algorithmIdentifier (iso.2.156.10197.1.501)
 - padding: 0
 - encrypted: 304602210073313b619be0a6d43f677451773cf39bae5c...

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。



2) 用例运行失败,报错提示客户端验证服务器证书失败。



3.3 HTTPS 双向认证

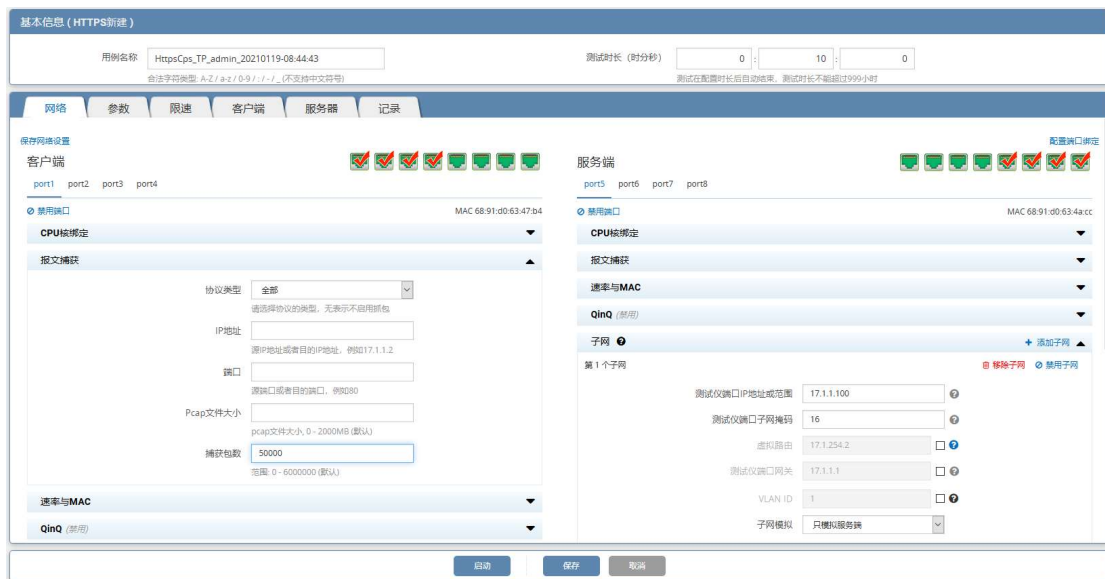
HTTPS 证书认证方式为“双向认证”时，用例配置需要 CA 证书配置、客户端证书配置、服务器证书配置，且客户端证书文件、服务器证书文件，均是通过 CA 证书文件签发的。双向认证要求服务器和客户端双方都有证书，客户端对服务器进行认证，服务器也要对客户端进行认证。

3.3.1 新建用例

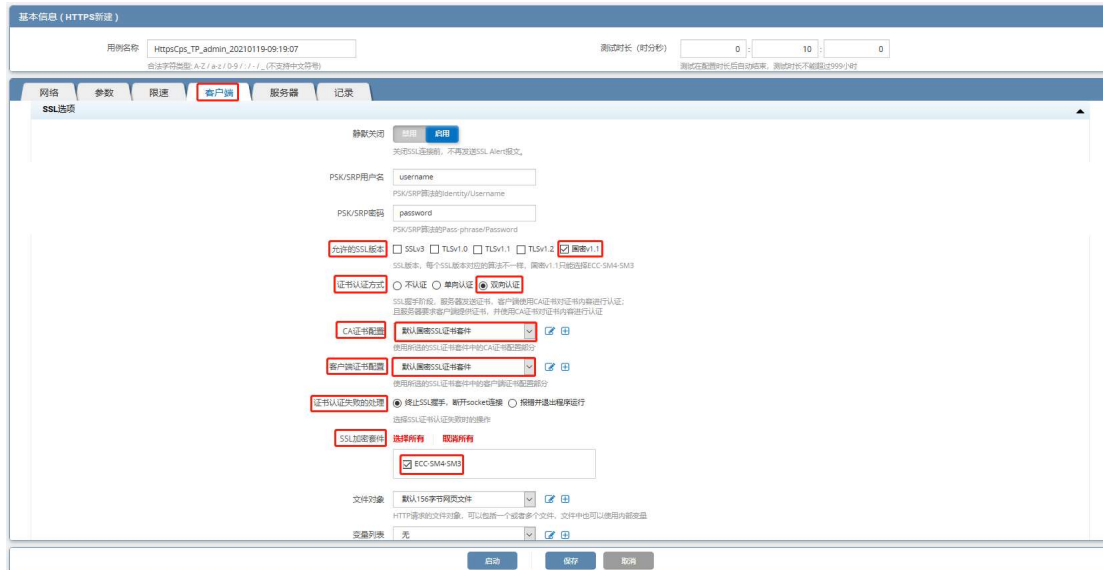
1) 通过 web 登录测试仪，依次点击用例 -> 网关设备测试 -> HTTPS -> 新建，单击增加，在弹出的选择用例选项中，编辑用例网络选项，根据需要修改配置参数，然后点击确定，进入用例配置页面。



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。



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。

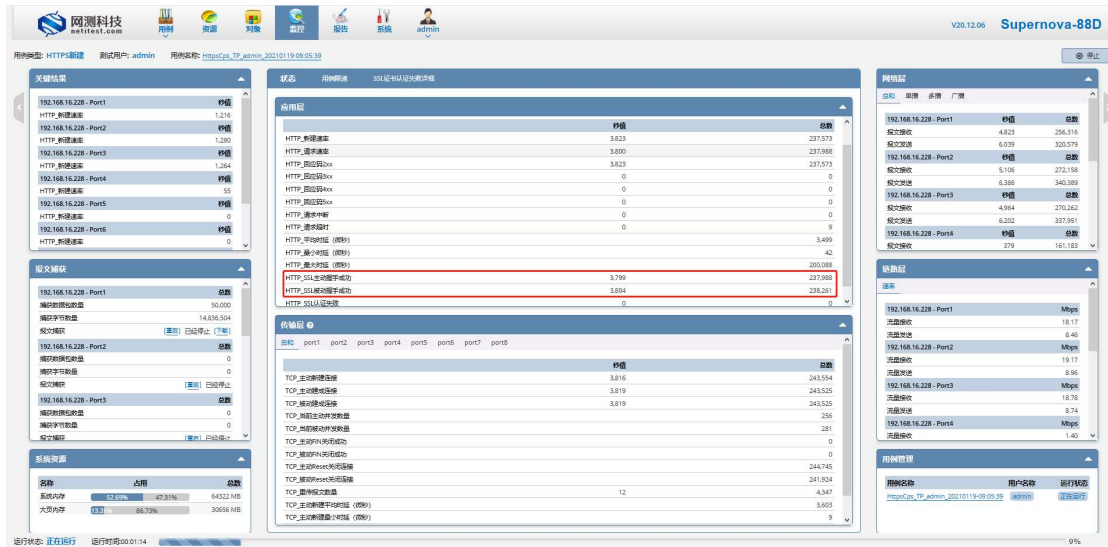


4) 点击 服务器, 配置服务器端国密证书套件, 使用的是其中的服务器证书配置部分, 点击保存, 保存 HTTPS 新建用例的配置。



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。



3.3.3 查看报文

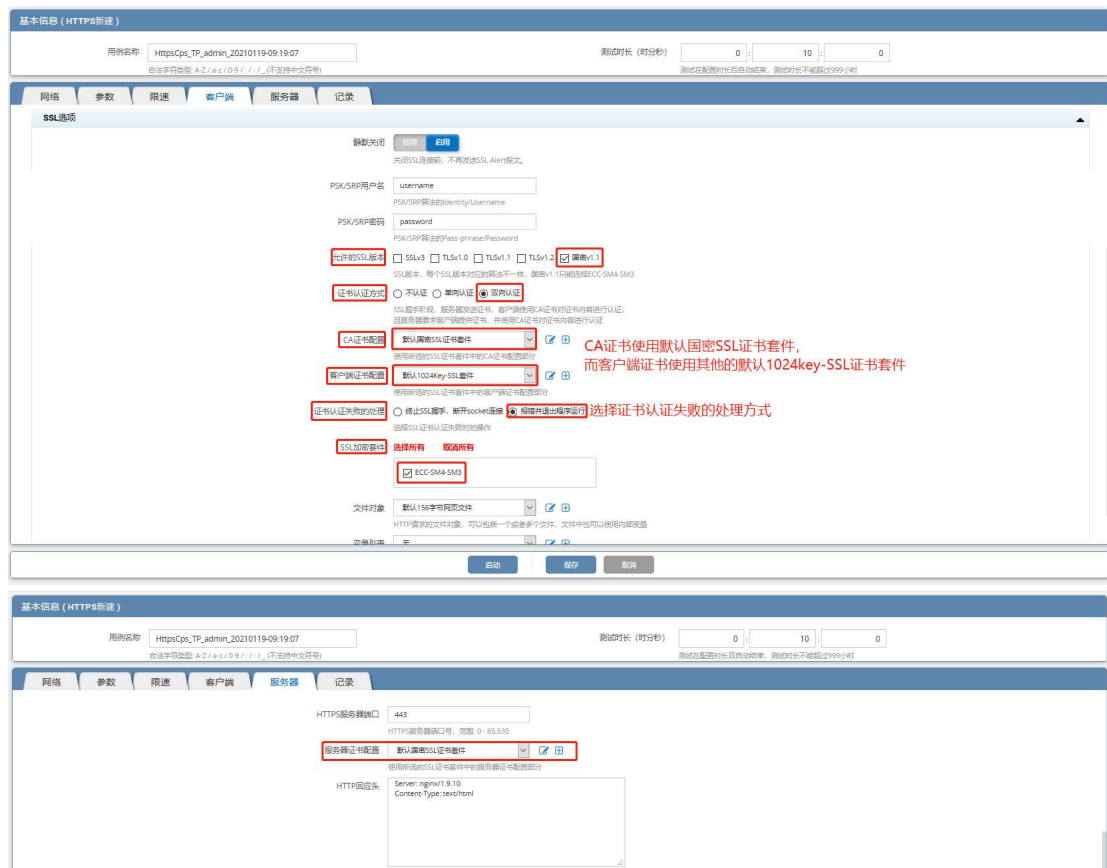
报文中可以看到 GMSSLv1 的握手过程和客户端服务器所使用的证书信息。

No.	Time	Source	Destination	Protocol	Length	SrvPort	DstPort	Info
483	3.035845	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=1452 SACK_PERM=1
859	3.037036	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
713	3.032152	17.1.1.100	17.1.2.2	GMSSLv1	106	10000	443	Client Hello
1106	3.042239	17.1.1.100	17.1.2.2	GMSSLv1	1234	443	10000	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
1192	3.044533	17.1.2.2	17.1.1.100	GMSSLv1	1419	10000	443	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
1610	3.277283	17.1.1.100	17.1.2.2	GMSSLv1	245	443	10000	Change Cipher Spec, Encrypted Handshake Message
1720	3.236981	17.1.2.2	17.1.1.100	GMSSLv1	219	10000	443	Application Data
2122	3.237786	17.1.1.100	17.1.2.2	GMSSLv1	283	443	10000	Application Data
2230	3.248468	17.1.2.2	17.1.1.100	TCP	60	10000	443	10000 → 443 [RST, ACK] Seq=1583 Ack=1421 Win=65535 [TCP CHECKSUM INCORRECT] 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。



2) 用例运行失败,报错提示证书验证失败。

