Supernova 测试仪
HTTPS 多方式认证配置

网测科技

2021-01-18

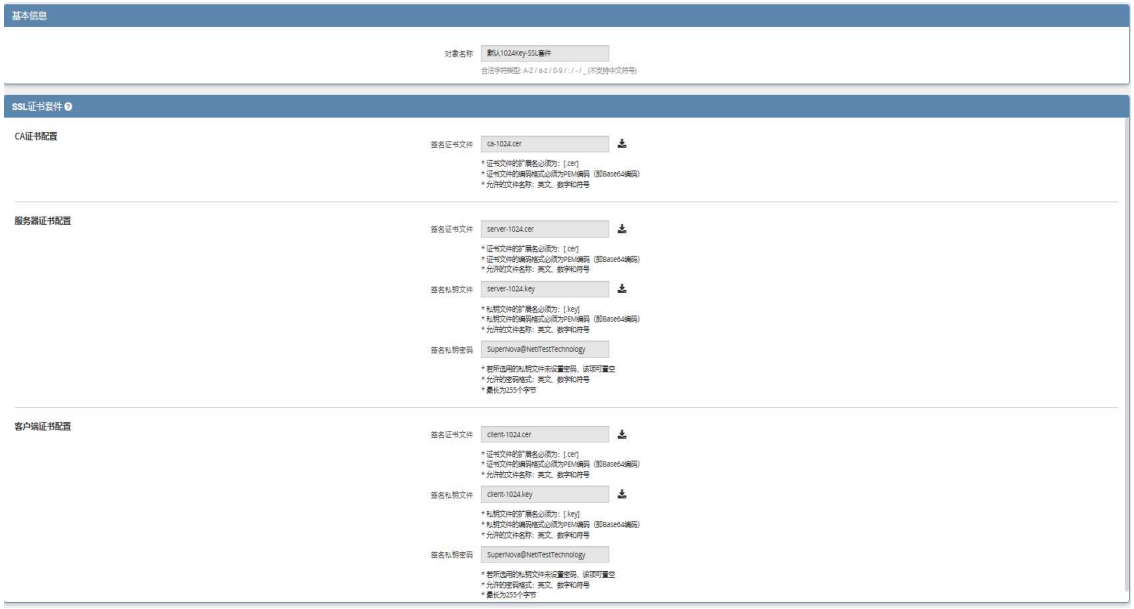
目录

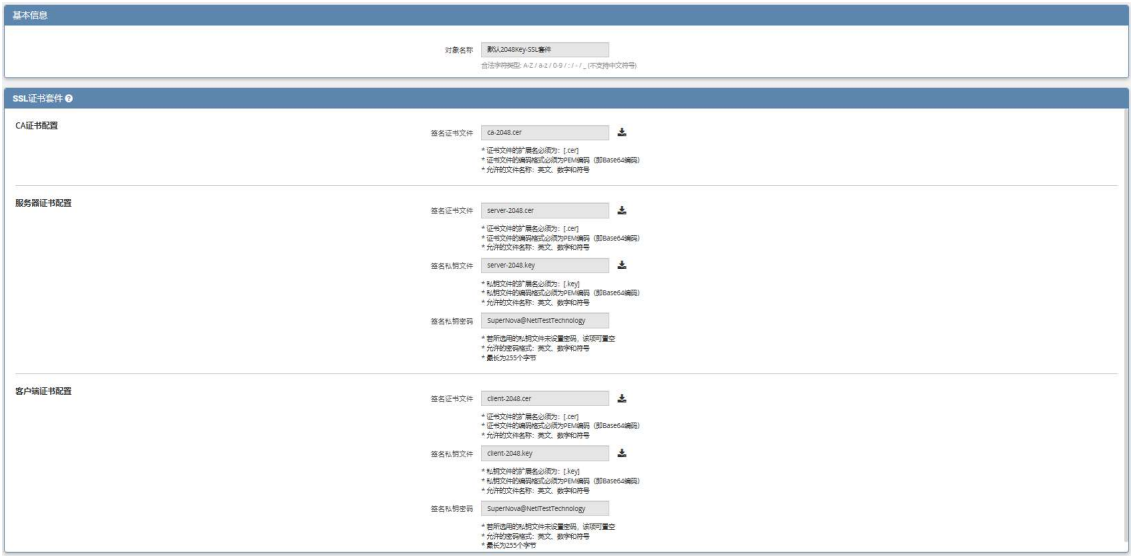
1. 文档说明

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。





2.1 生成证书

在这里简单介绍一下 openssl 制作证书的过程，也可以使用其他证书生成工具生成证书。openssl 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 ca1.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 openssl 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 ca1.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.....................+++
e is 65537 (0x10001)
Enter pass phrase for ca1.key:
Verifying - Enter pass phrase for ca1.key:
[root@mail test2]#
```

2）生成 CA 自签名证书

命令：openssl req -new -x509 -days 365 -key ca1.key -out ca1.cer

```
[root@mail test2]# openssl req -new -x509 -days 365 -key ca1.key -out ca1.cer
Enter pass phrase for ca1.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 国家简称
State or Province Name (full name) []:HN 省级名称
Locality Name (eg, city) [Default City]:AY 市级名称
Organization Name (eg, company) [Default Company Ltd]:WC 公司名称
Organizational Unit Name (eg, section) []:QA 组织机构名称，可以不填
Common Name (eg, your name or your server's hostname) []: 可以不填
Email Address []: 电子邮箱，可以不填
[root@mail test2]#
```

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
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) []:TEST
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:      可以不填
An optional company name []:      可以不填
```

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 ca1.cer -keyfile ca1.key -in server1.csr -out server1.cer

```
[root@mail test2]# openssl ca -policy policy_anything -days 365 -cert ca1.cer -keyfile ca1.key -in server1.csr -out server1.cer
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ca1.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 3 (0x3)
        Validity
            Not Before: May  5 03:27:46 2019 GMT
            Not After : May  4 03:27:46 2020 GMT
        Subject:
            countryName               = CN
            stateOrProvinceName       = HN
            localityName              = AY
            organizationName          = WC
            organizationalUnitName    = QA
            commonName                = TEST
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                70:82:30:9F:D0:C6:2C:3A:71:3A:B9:59:21:11:0C:DA:40:72:1B:7A
            X509v3 Authority Key Identifier:
                keyid:AB:77:74:67:9D:7E:5F:F6:B1:8C:87:00:48:46:3D:A4:95:AF:13:2D

Certificate is to be certified until May  4 03:27:46 2020 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

证书信息

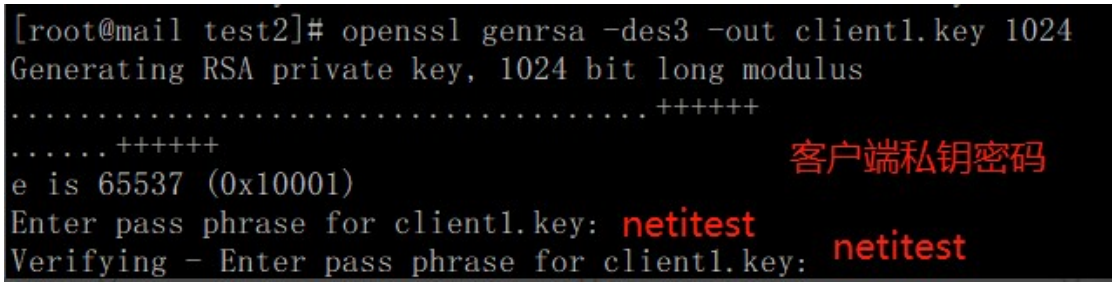
成功

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

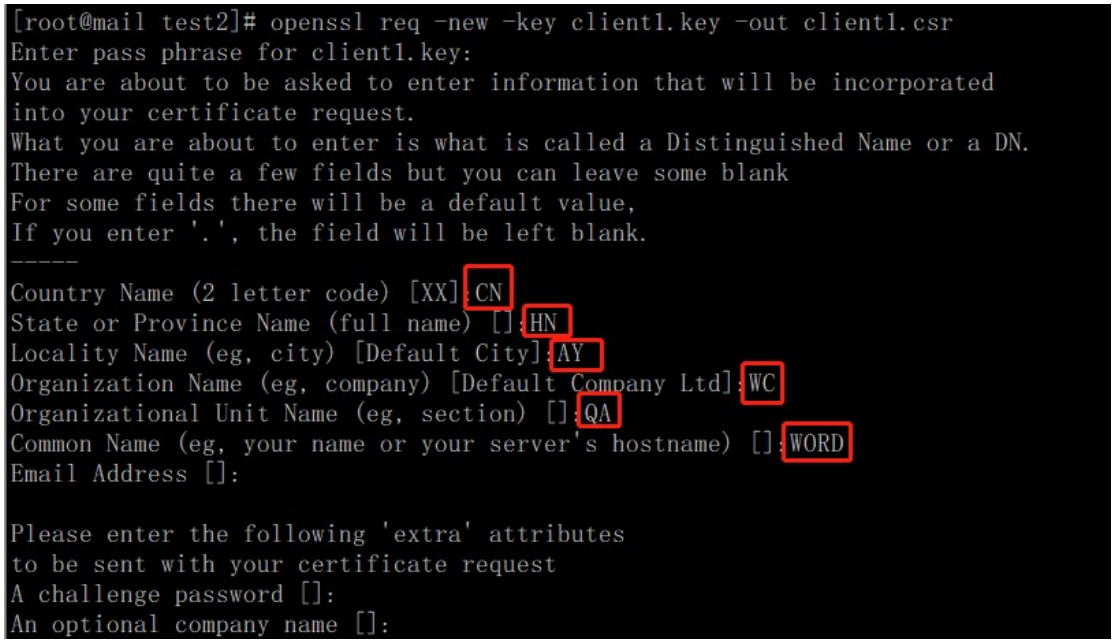
输入相应的密码设定，如图所示：



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



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 ca1.cer -keyfile ca1.key -in client1.csr -out client1.cer

```
[root@mail test2]# openssl ca -policy policy_anything -days 365 -cert ca1.cer -keyfile ca1.key -in client1.csr -out client1.cer
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ca1.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4 (0x4)
        Validity
            Not Before: May  5 03:36:10 2019 GMT
            Not After : May  4 03:36:10 2020 GMT
        Subject:
            countryName               = CN
            stateOrProvinceName       = HN
            localityName              = AY
            organizationName          = WC
            organizationalUnitName    = QA
            commonName                = WORD
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                02:F7:3C:7A:61:2F:27:CC:49:E4:AC:F0:8A:CE:41:A7:CB:71:44:BB
            X509v3 Authority Key Identifier:
                keyid:AB:77:74:67:9D:7E:5F:F6:B1:8C:87:00:48:46:3D:A4:95:AF:13:2D

Certificate is to be certified until May  4 03:36:10 2020 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

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 ca1.cer server1.cer

openssl verify -CAfile ca1.cer client1.cer

```
[root@mail test2]# openssl verify -CAfile ca1.cer server1.cer
server1.cer: OK
[root@mail test2]# openssl verify -CAfile ca1.cer client1.cer
client1.cer: OK
```

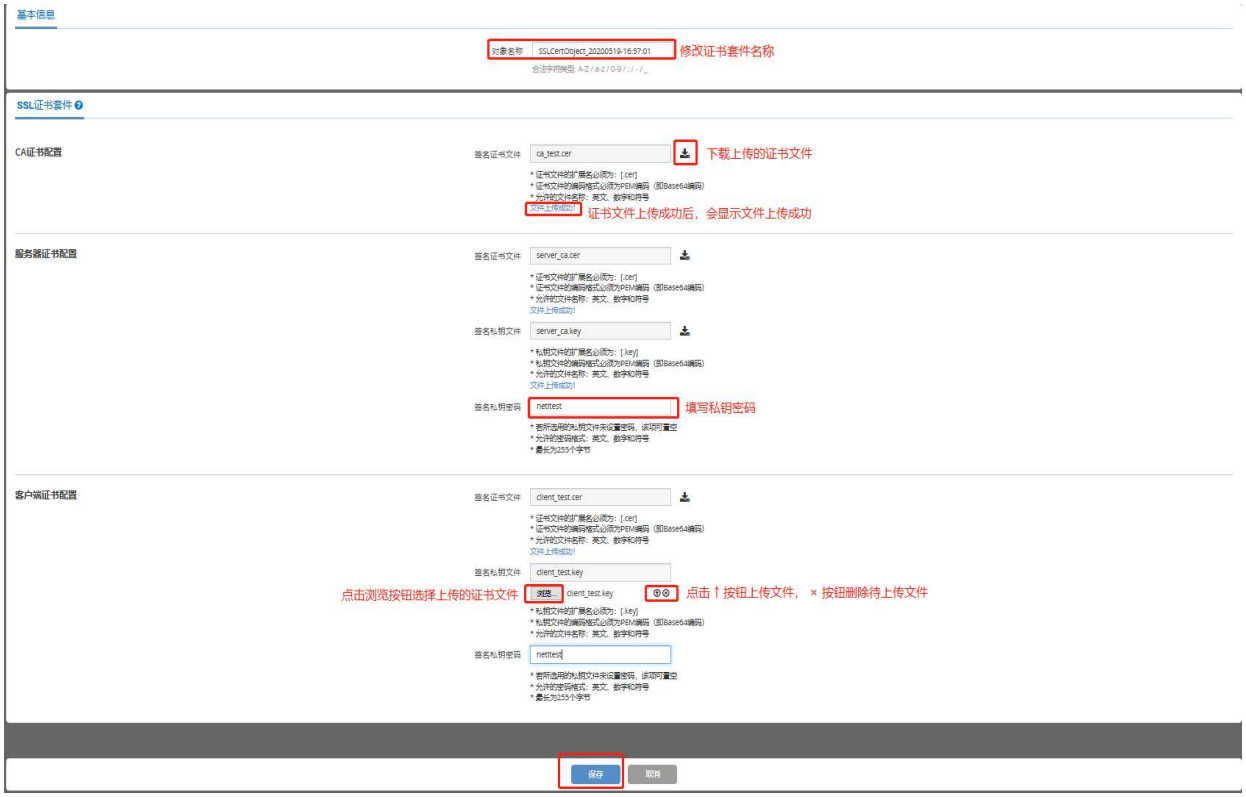
验证通过后，将文件打包，下载到工作电脑上，解压，方便将证书和私钥文件导入系统。

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。

3）选择相应的证书和私钥文件上传系统，保存。

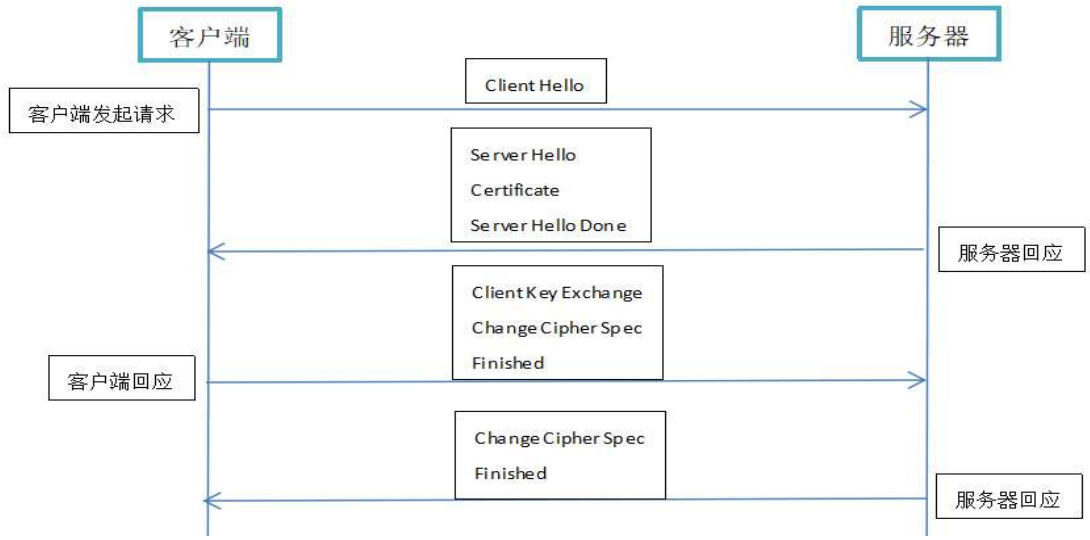


3. 用例配置及运行

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。

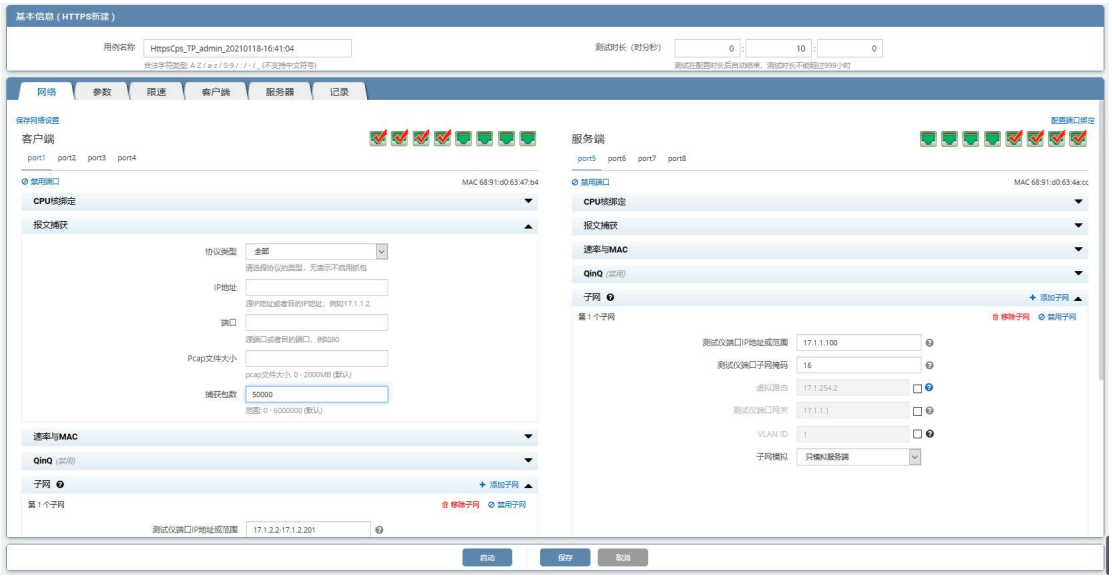
握手过程的简易流程图：



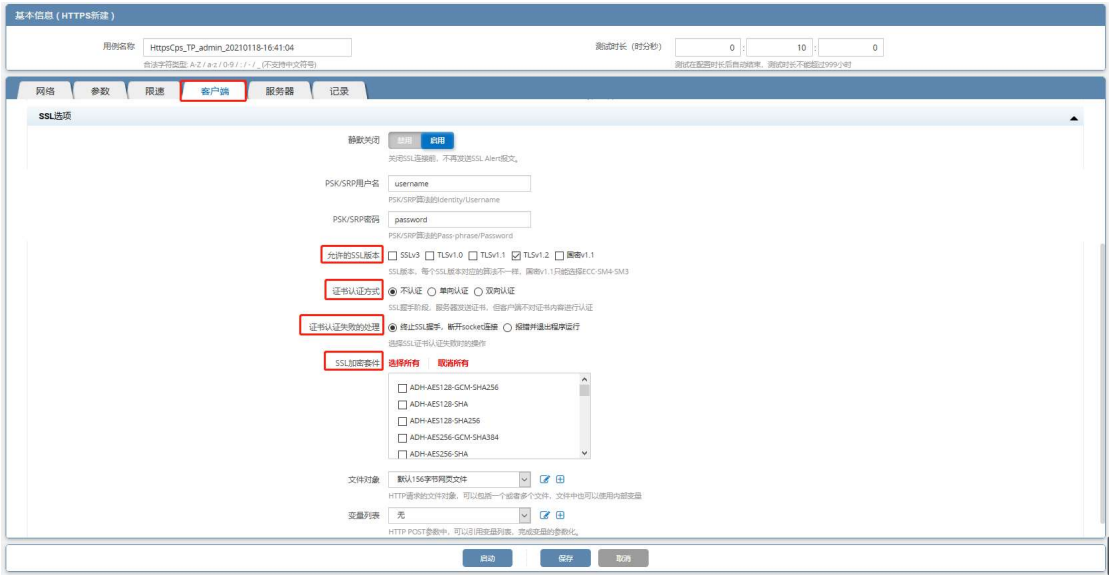
3.1.1 新建用例

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。

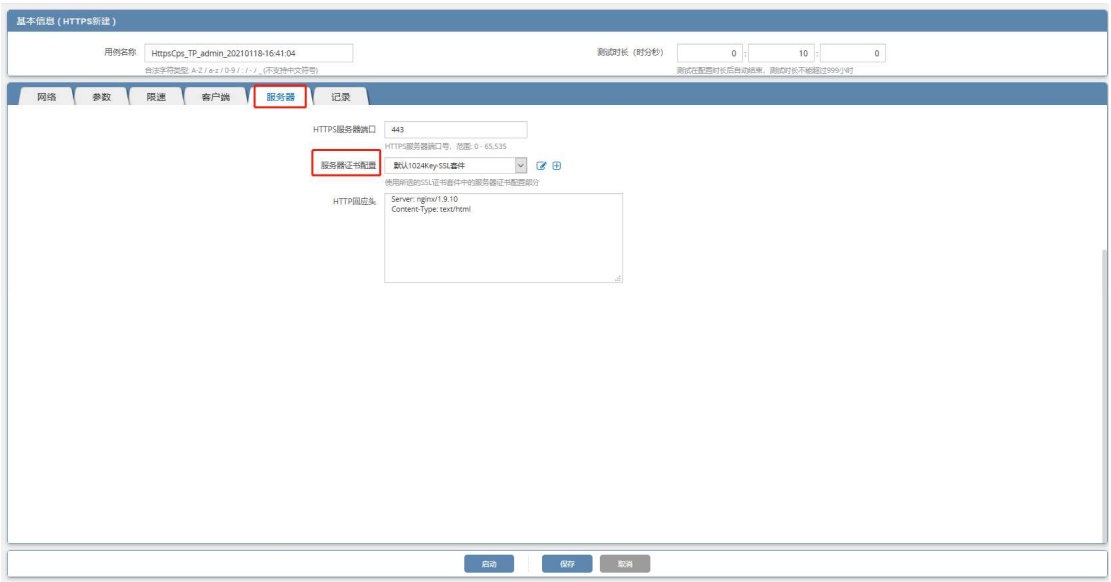
2）进入用例配置页面，配置网络信息，可设置报文捕获查看详细报文交互。



3）点击 客户端，编辑设置客户端证书认证配置，证书认证方式默认不认证。

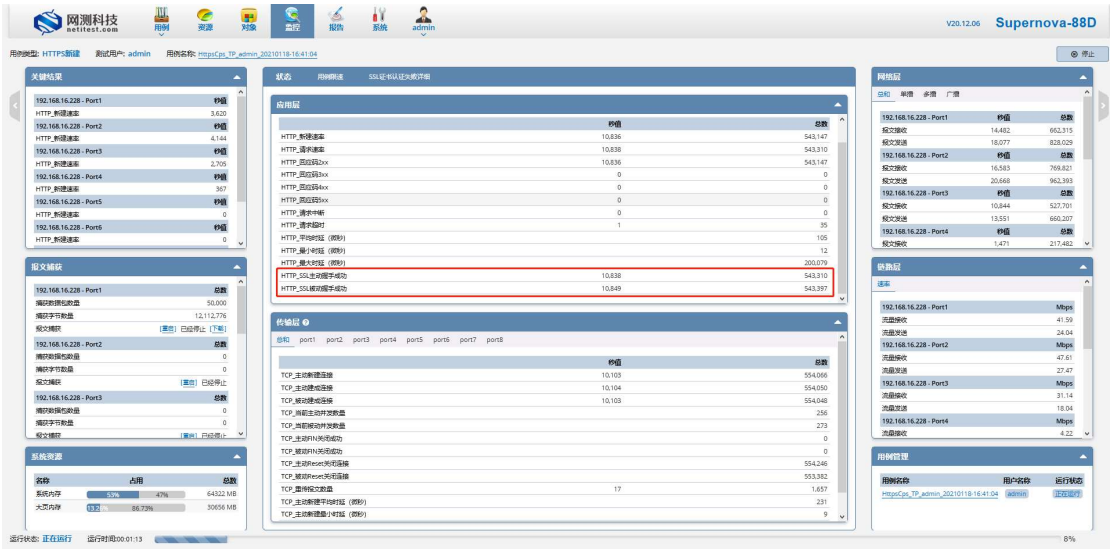


4）点击 服务器，编辑设置服务端证书认证配置，服务器证书配置选择 2.2 章节配置的 SSL 证书套件，使用的是其中的服务器证书配置部分，点击保存用例的配置。



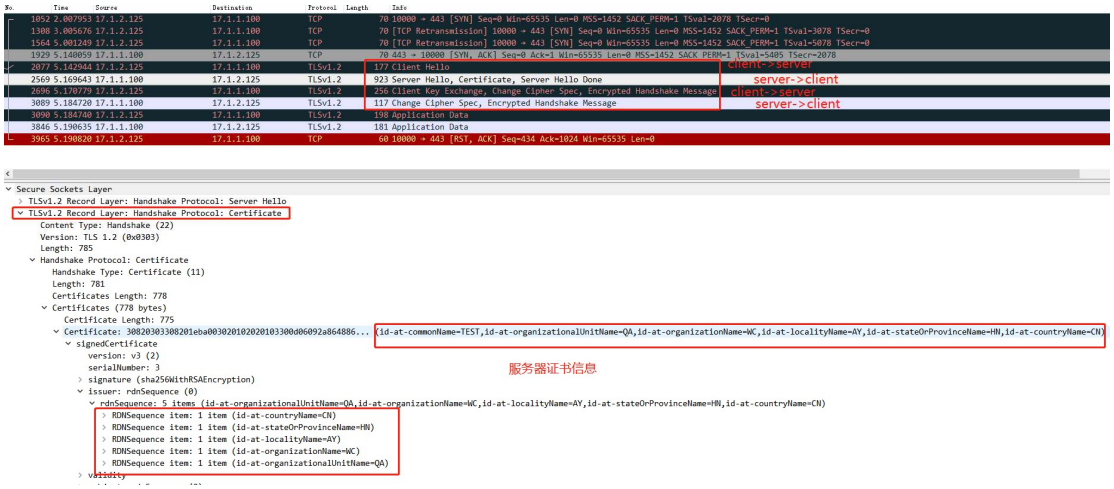
3.1.2 运行界面

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

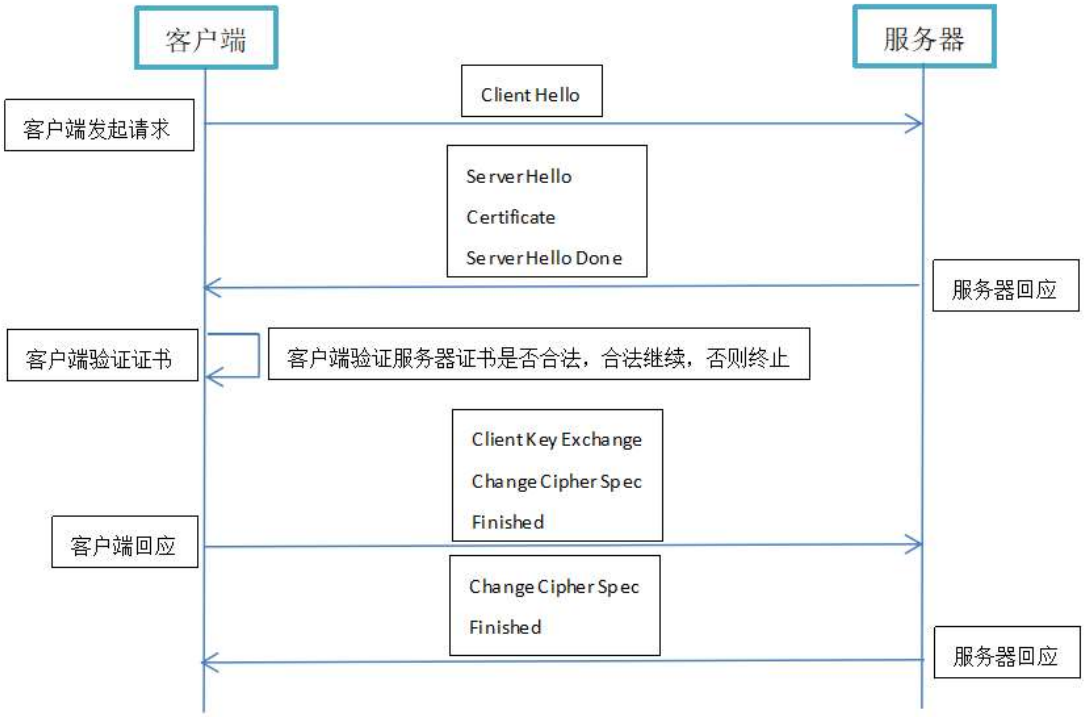
报文中可以看到 SSL/TLS 的握手过程和服务器所使用的证书信息。



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。

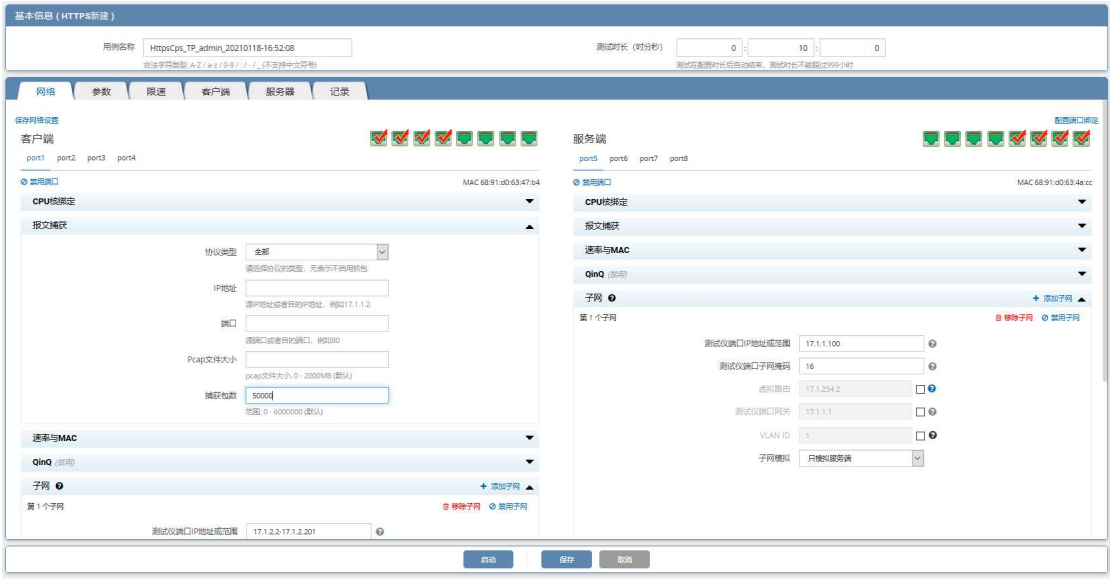
单向认证的简易流程图如下：



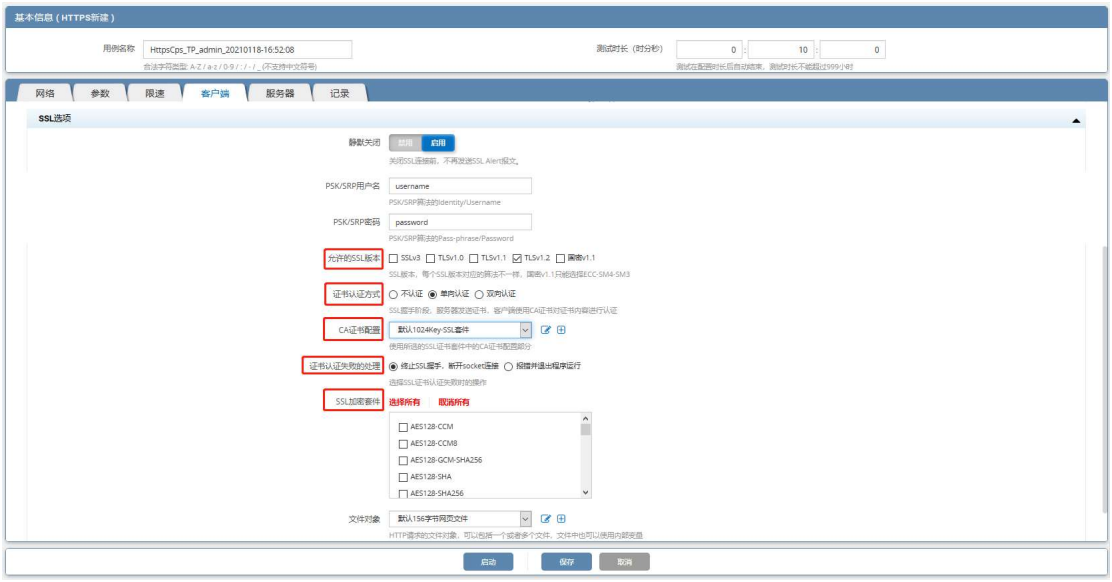
3.2.1 新建用例

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。

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。



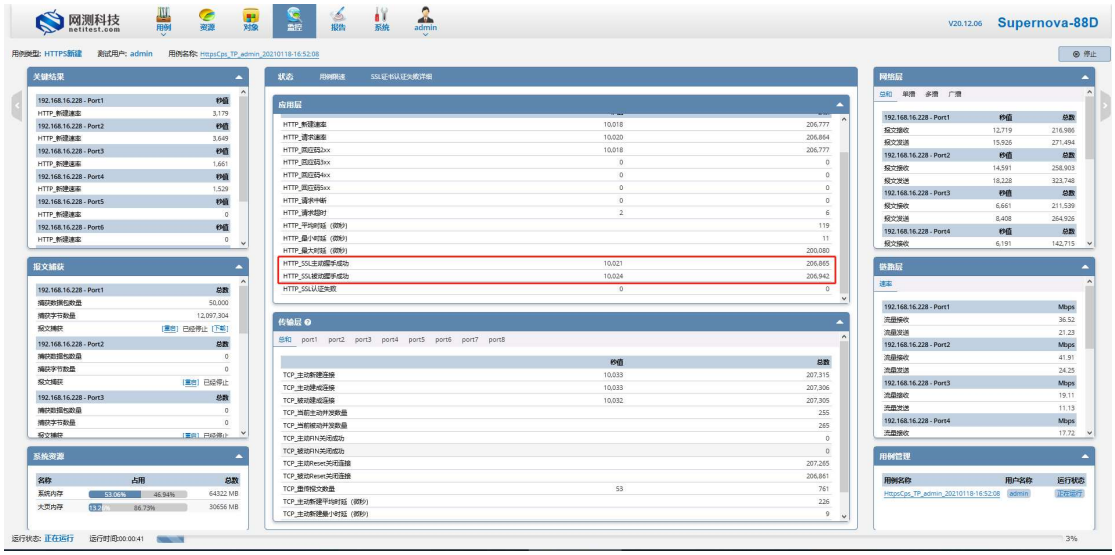
3）点击 客户端，编辑客户端证书配置，认证方式选择单向认证。CA 证书配置选择 2.2 章节配置的 SSL 证书套件，使用的是其中的 CA 证书配置部分。



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。

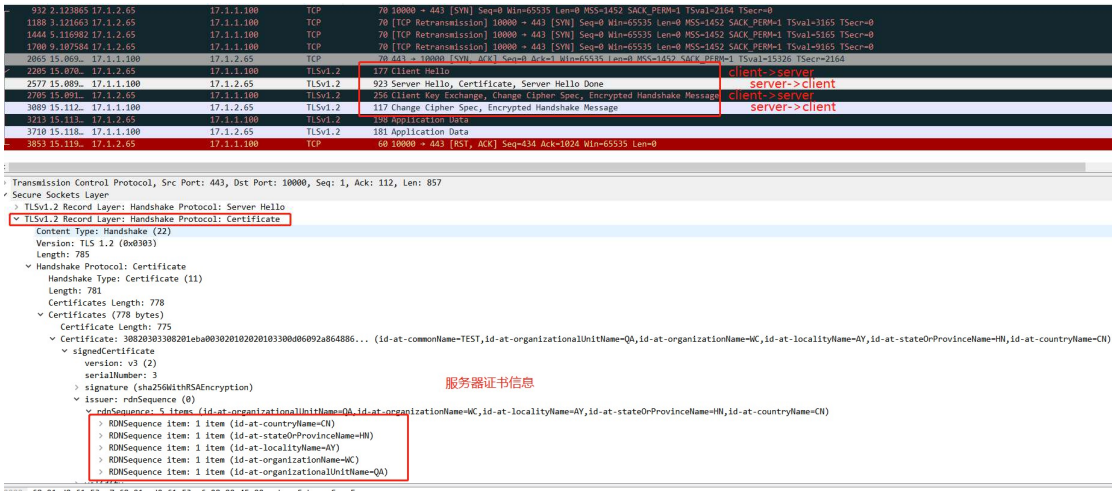
3.2.2 运行界面

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。



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。

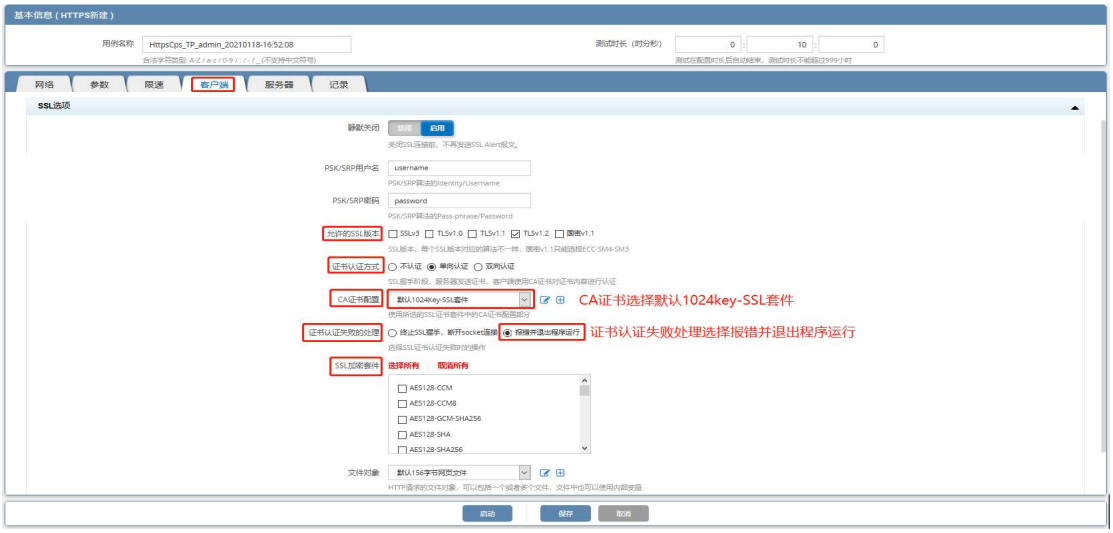


3.2.4 认证失败

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

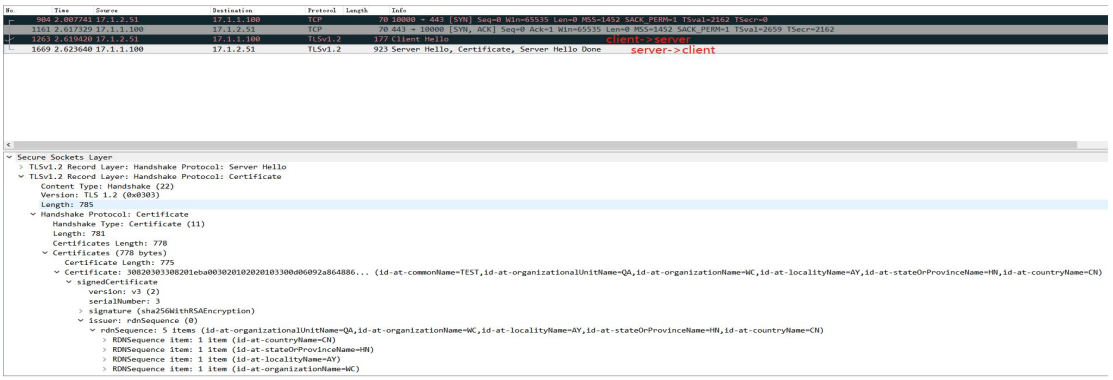
理，并提示错误信息。下边是 CA 证书和服务器证书配置来自不同 SSL 证书套件的情况。

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。



2）用例运行失败，报错提示客户端验证服务器证书失败。

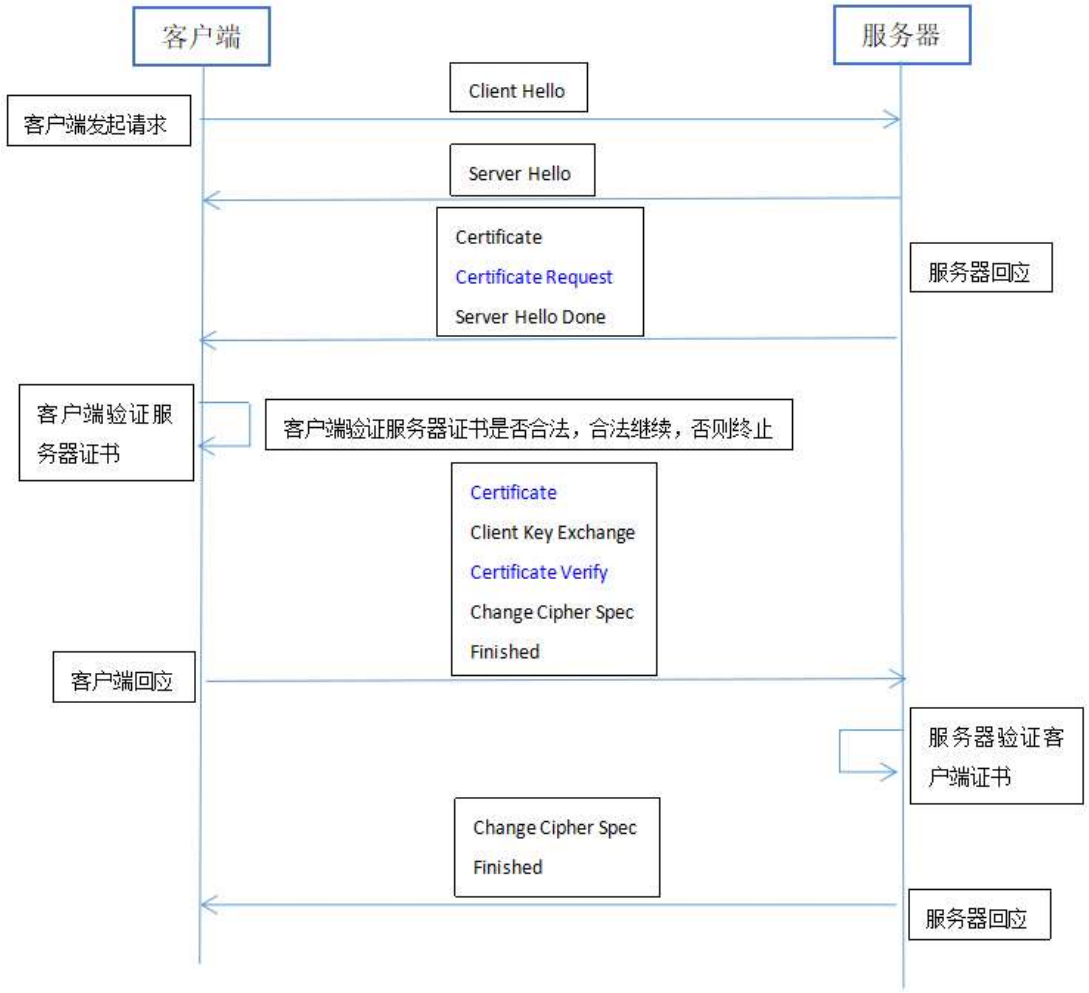
3）查看报文，服务器给客户端发送证书等信息后，客户端验证服务器证书，终止与服务器的通信。



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。

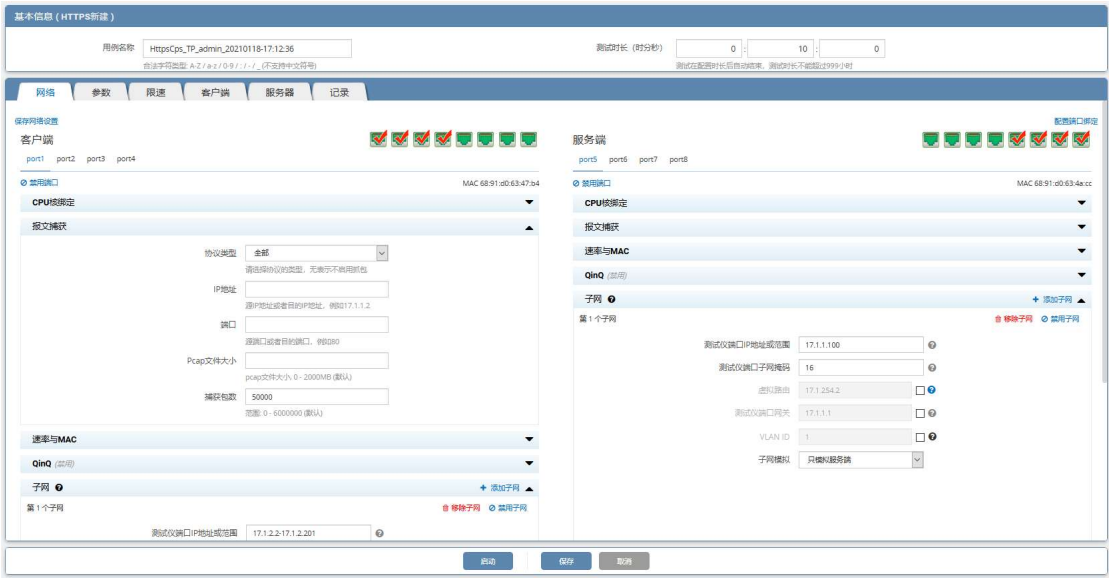
双向认证的简易流程图如下：



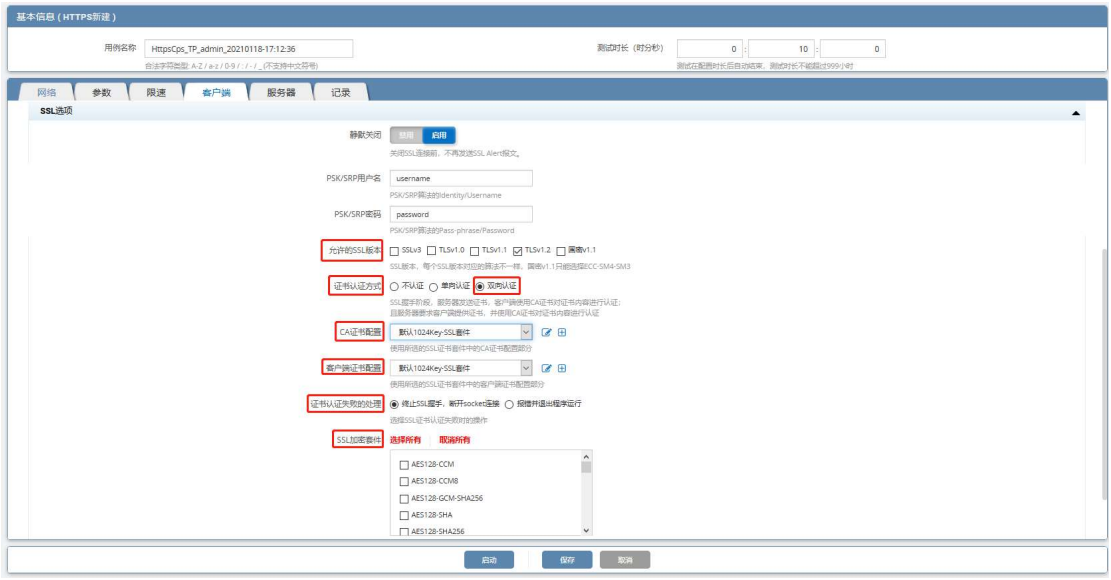
3.3.1 新建用例

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。

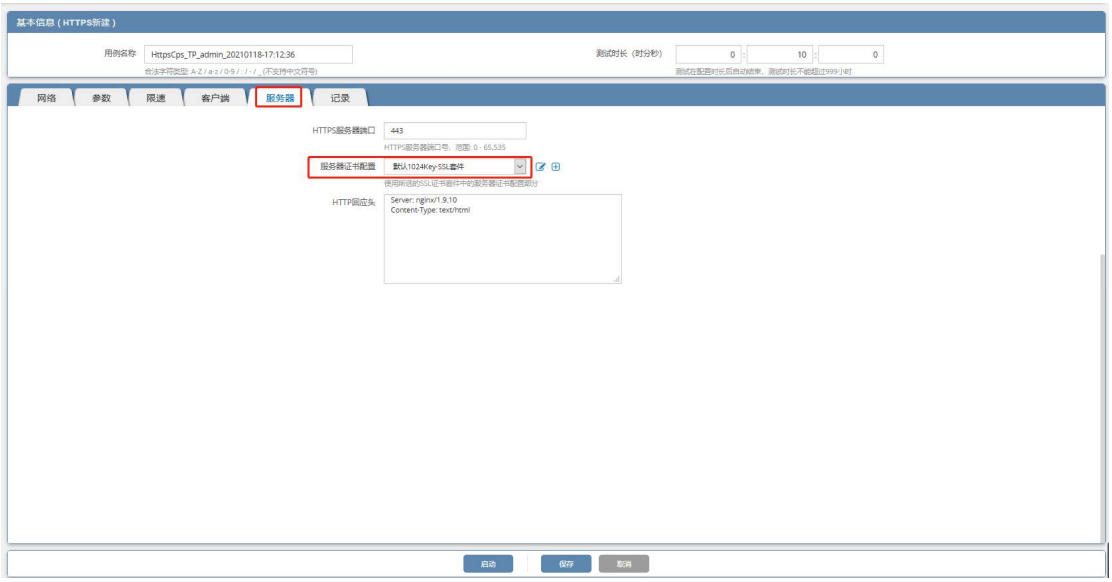
2）进入用例配置页面，配置网络信息，可设置报文捕获查看详细报文交互。



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。

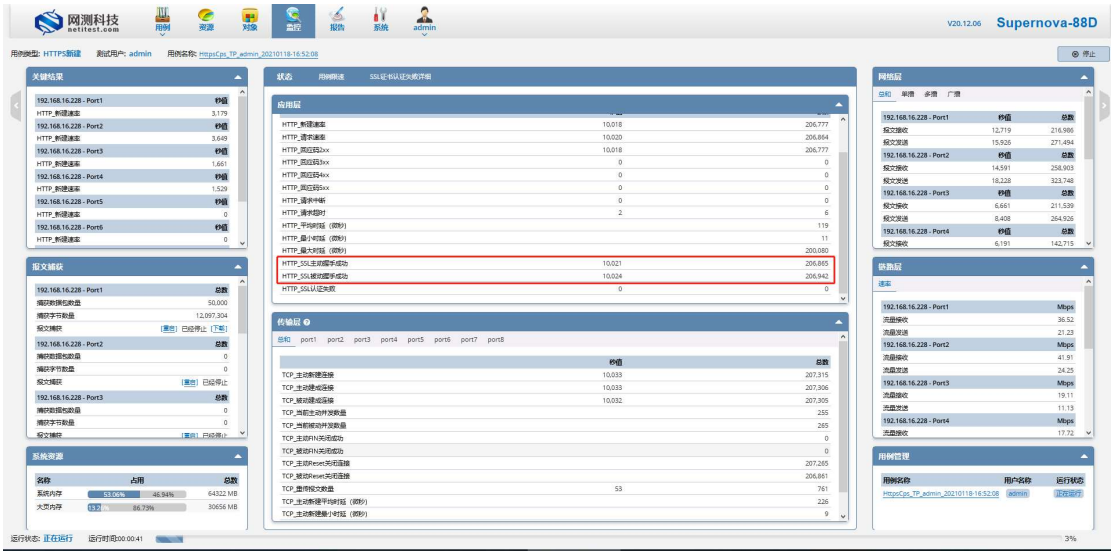


4）点击 服务器，服务器证书配置选择 2.2 章节配置的 SSL 证书套件，使用的是其中的服务器证书配置部分，点击保存，保存 HTTPS 新建用例的配置。



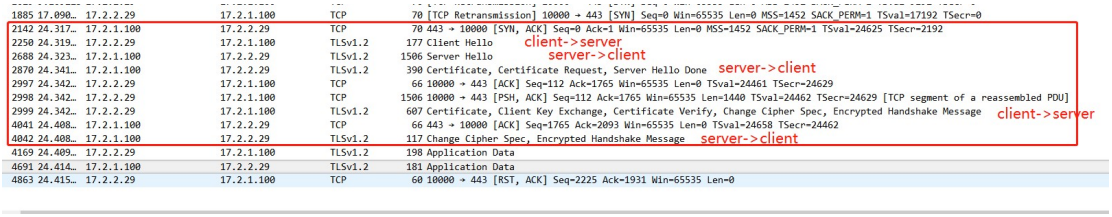
3.3.2 运行界面

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 SSL/TLS 的握手过程和服务器所使用的证书信息。

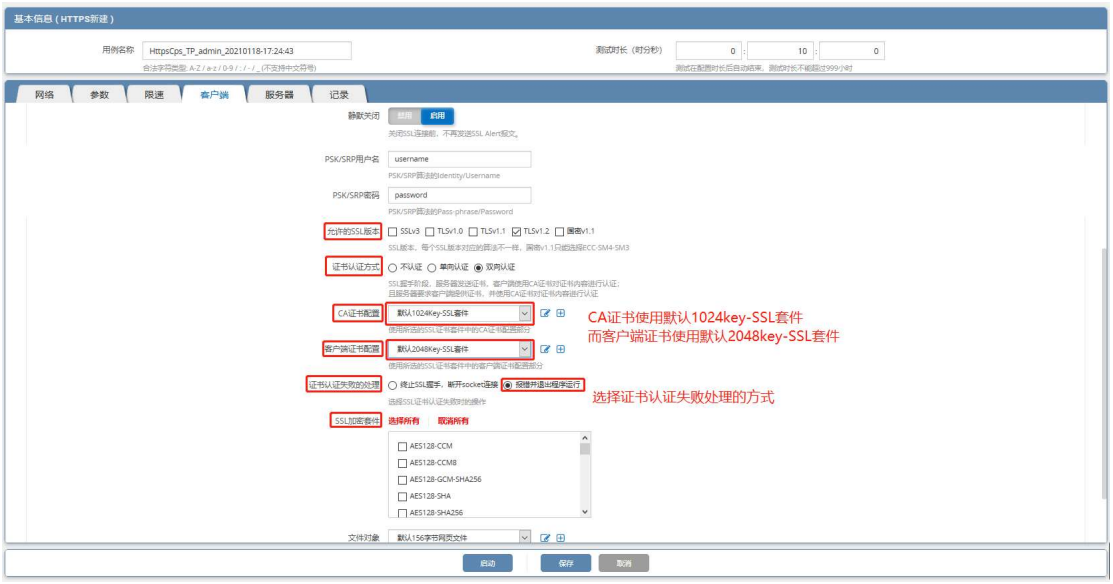


3.3.4 认证失败

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 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。



2）用例运行失败，报错提示服务器验证客户端证书失败。

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。