Project Instruction

This project is to reproduce the demo of netty's abnormal disconnection problem in the process of ssl link multiplexing

Project Function Description

The function of this project is to listen to port 8801, and enable tls mutual authentication, the Https data requested by the client is completely transmitted to another server, and the server response is returned to the client.
It's like an http proxy for nginx
avatar

Project Operating Environment

- jdk 1.8.0_202
- maven 3.8.1
- IntelliJ IDEA Community Edition 2023.1
- netty 4.1.96.Final
- postman 10.17.0
- Windows 10 Professional

Certificate Tree

You can use the XCA to open /src/resources/ssl/ca.xdb to view the certificate tree structure avatar

- The certificate file used by the netty server is /src/resources/ssl/server.jks
- The certificate file used by the postman client is /src/resources/ssl/client/client.crt
- The private key file used by the postman client is /src/resources/ssl/client/client.pem

Quick Start

1. Modify the REMOTE_HOST parameter of the HttpsServerProxy class and replace it with your server IP
2. Run the main method of the HttpsServerProxy class to start

Steps to reproduce

1. Start the HttpsServerProxy main method listening on port 8801
2. Use postman https to request local port 8801 and send the following packet

- postman certificate setting: avatar avatar

- postman demo: /testData/postmanDemo/netty-test.postman_collection.json URL:

```
https://127.0.0.1:8801/sasManage/certificate/add
```

header

```
Content-Type:application/json; charset=utf-8
Accept-Language:en-US
App-Id:sasmgt-tool
App-Version:4.2.0
App-Name:SASMGT+Tool
```

Body

```
{
  "certCn": "wewe",
  "certId": "",
  "certName": "testL4",
  "certPublicKey": "",
  "certRequestJson": "",
  "certSchemeId": "721bb8a1499d617342c419f9e7933373",
  "certVersion": "V2.0",
  "country": "AU",
  "hash": "",
  "hsmId": "c8e1f834d808def2dfd463a2e60dbeab",
  "isProfileNecessary": "",
  "isvId": "",
  "kappidId": "",
  "keyLength": 2048,
  "keyUsage": "32768,128,16,8",
  "locality": "ts",
  "memo": "",
  "organizationName": "ts",
  "parentCertId": "",
  "parentCertSchemeId": "d389aa728d15d598754dfc24192b10e9",
  "permissionDomain": "",
  "product": "",
  "profileId": "",
  "province": "ts",
  "signPermissionTemplateId": "",
  "staffId": "01129ff51e0041858bec2435cdee348e",
  "subjectDataType": 1,
  "synFlag": 0,
  "ukeyId": "",
  "validAfterTime": "2023-08-16 06:46:49",
  "validBeforeTime": "2043-08-16 06:46:49",
  "encAndHashAlgorithm": ["RSA", "SHA-256"]
}
```

3. Use postman for Https mutual authentication on port 8801, reuse the ssl link without disconnecting, and wireshark for packet capture
4. After my test, the netty server will break the link actively when the test reaches 50-120 times. I don't know why. The most serious time is that after forwarding the client data to the later server, the background server will directly break the link before the response data is returned, resulting in a client error
5. The key to the test is to always use keepalive to reuse the connection of the request, do not disconnect in the middle

Test Network Capture Data

Screenshot of self-test error report

- postman error screenshot avatar
- wireshark screenshot postman-> nettyserver avatar nettyserver->remote server avatar
- Connection Error Diagram avatar