SSL-Proxy Solution for HTTPS Decryption

Hillstone Networks Inc.

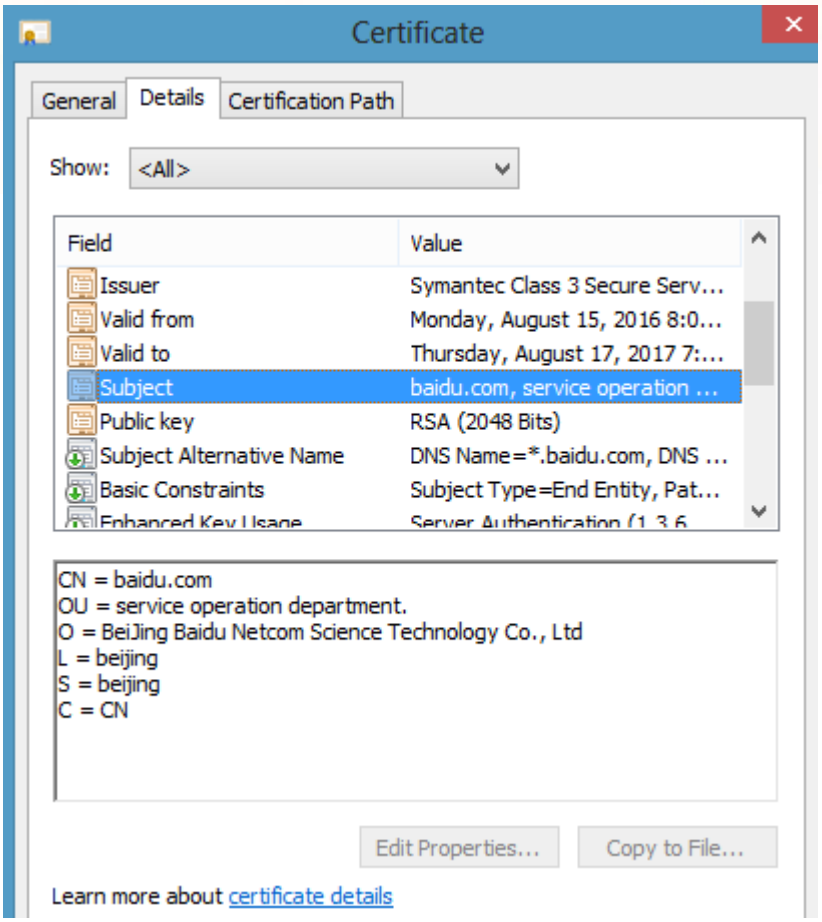
Index

1 Request Analysis

Secure Sockets Layer (SSL) is a computer networking protocol for securing connections between network application clients and servers over an insecure network, such as the internet. Due to numerous protocol and implementation flaws and vulnerabilities, SSL was deprecated for use on the internet by the Internet Engineering Task Force (IETF) in 2015 and has been replaced by the Transport Layer Security (TLS) protocol. While TLS and SSL are not interoperable, TLS is backwards-compatible with SSL 3.0

When a Web browser tries to connect to a website using SSL, the browser will first request the web server identify itself. This prompts the web server to send the browser a copy of the SSL Certificate. The browser checks to see if the SSL Certificate is trusted - if the SSL Certificate is trusted, then the browser sends a message to the Web server. The server then responds to the browser with a digitally signed acknowledgement to start an SSL encrypted session. This allows encrypted data to be shared between the browser and the server. You may notice that your browsing session now starts with https (and not http).

In order to provide public key to client, HTTPS site is using certificate issued by CA organization, you can find in client the below information:



To assure the security of sensitive data when being transmitting over networks, more and more websites adopt SSL encryption to protect their information. The device provides the SSL proxy function to decrypt HTTPS traffic. There are three work modes: Require mode, Exempt mode, Offload mode. Here we will test the first two modes.

2 Solution

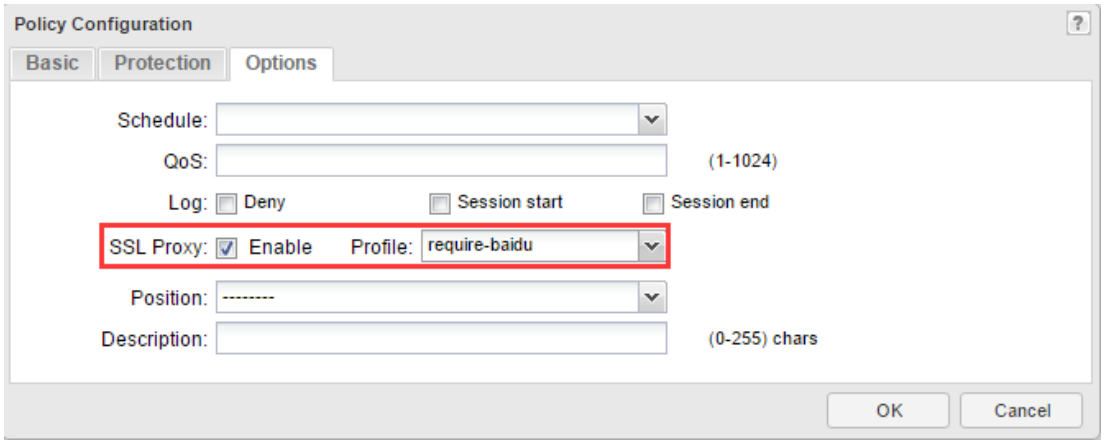
Hillstone FW deployed at network exit in routing mode, firmware: SG6000-M-5.5R3.bin

2.1 Require-mode SSL proxy for HTTPS websites

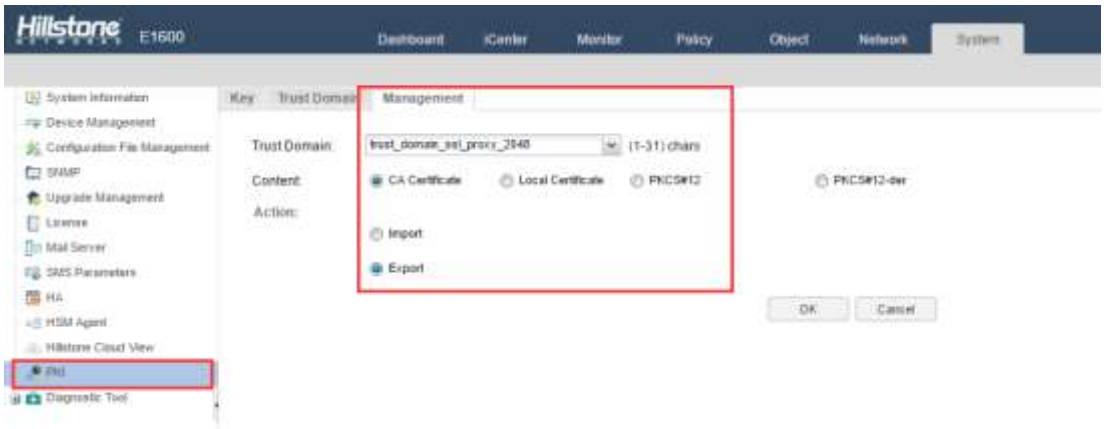
（1） Create SSL-proxy profile

```
sslproxy-profile "require-baidu"
        mode require
        description baidu-proxy
        cert-subject-name baidu.com
exit
```

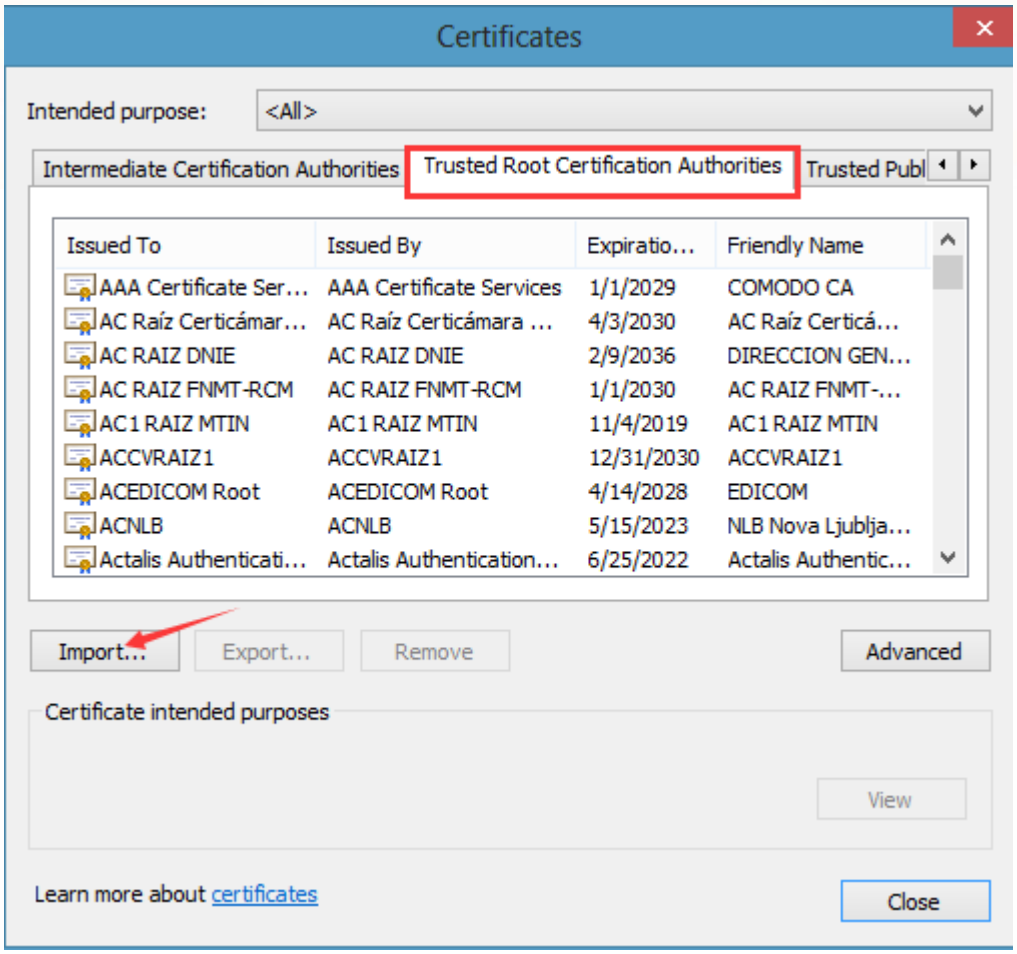
（2） Bind this SSL-proxy profile to policy



（3） Export CA certificate from FW and import to browser

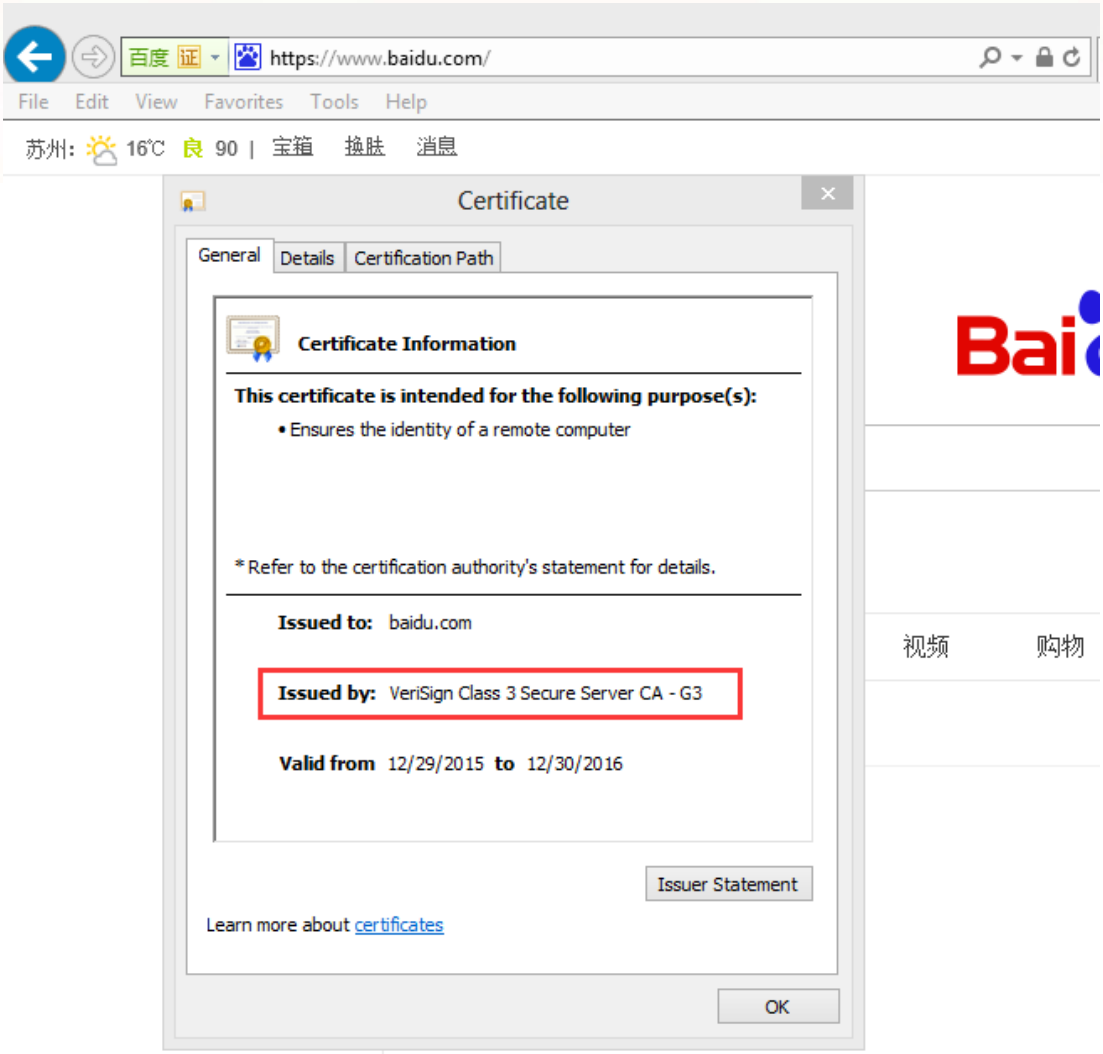


Import the root certificate to the "Trusted Root Certification Authorities" of client browser

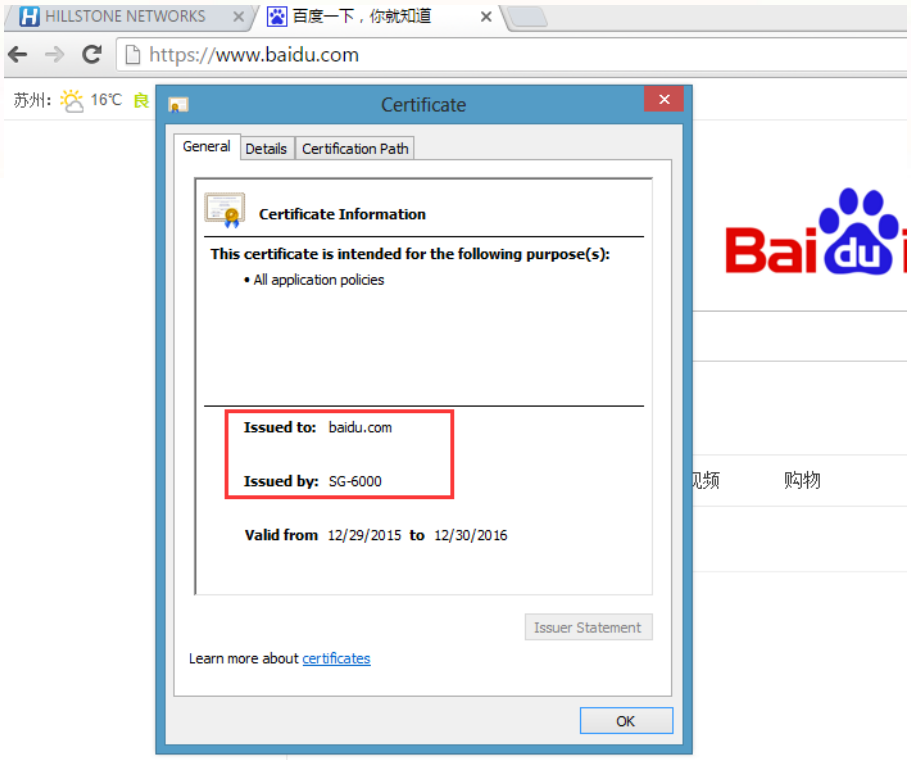


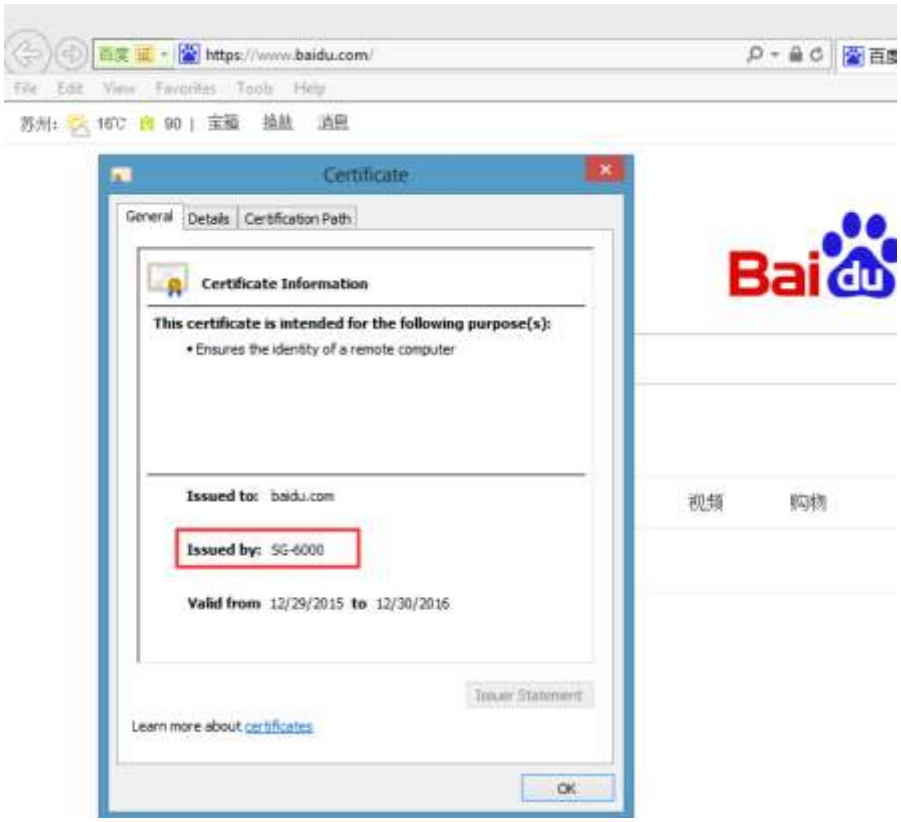
（4） Verify the proxy result

A. Before the proxy



B. After proxy


HILLSTONE NETWORKS
百度一下，你就知道
https://www.baidu.com
苏州: 16℃
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All application policies
Issued to: baidu.com
Issued by: SG-6000
Valid from 12/29/2015 to 12/30/2016
Issuer Statement
Learn more about certificates
OK
视频
购物

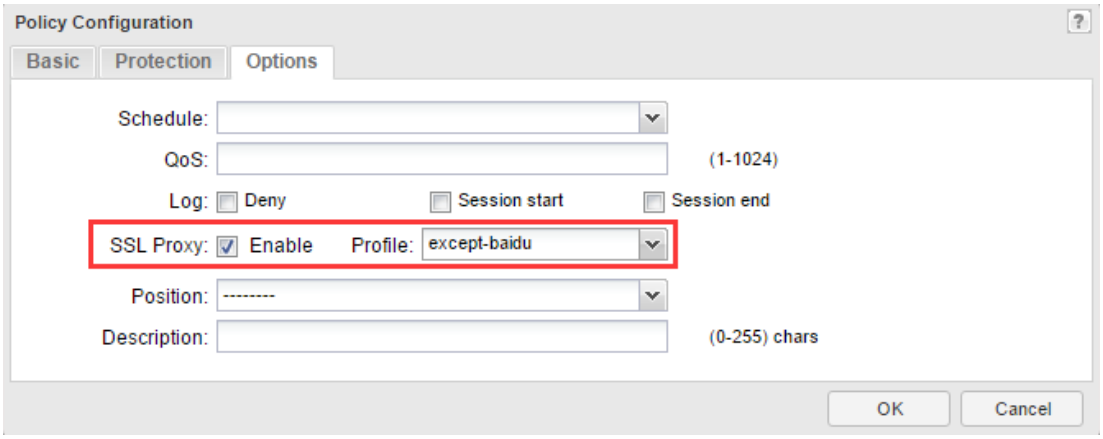

https://www.baidu.com/
苏州: 16℃
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
Issued to: baidu.com
Issued by: SG-6000
Valid from 12/29/2015 to 12/30/2016
Issuer Statement
Learn more about certificates
OK
视频
购物

2.2 Exempt mode SSL proxy, proxy all other websites except baidu

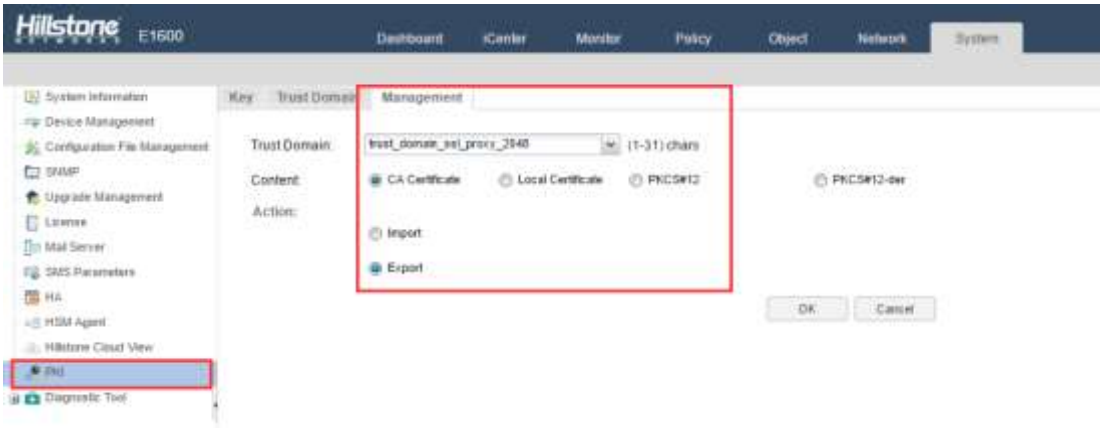
（1） Create SSL-proxy profile

```
sslproxy-profile "except-baidu"
        mode exempt
        description proxy all except baidu
        cert-subject-name baidu.com
    exit
```

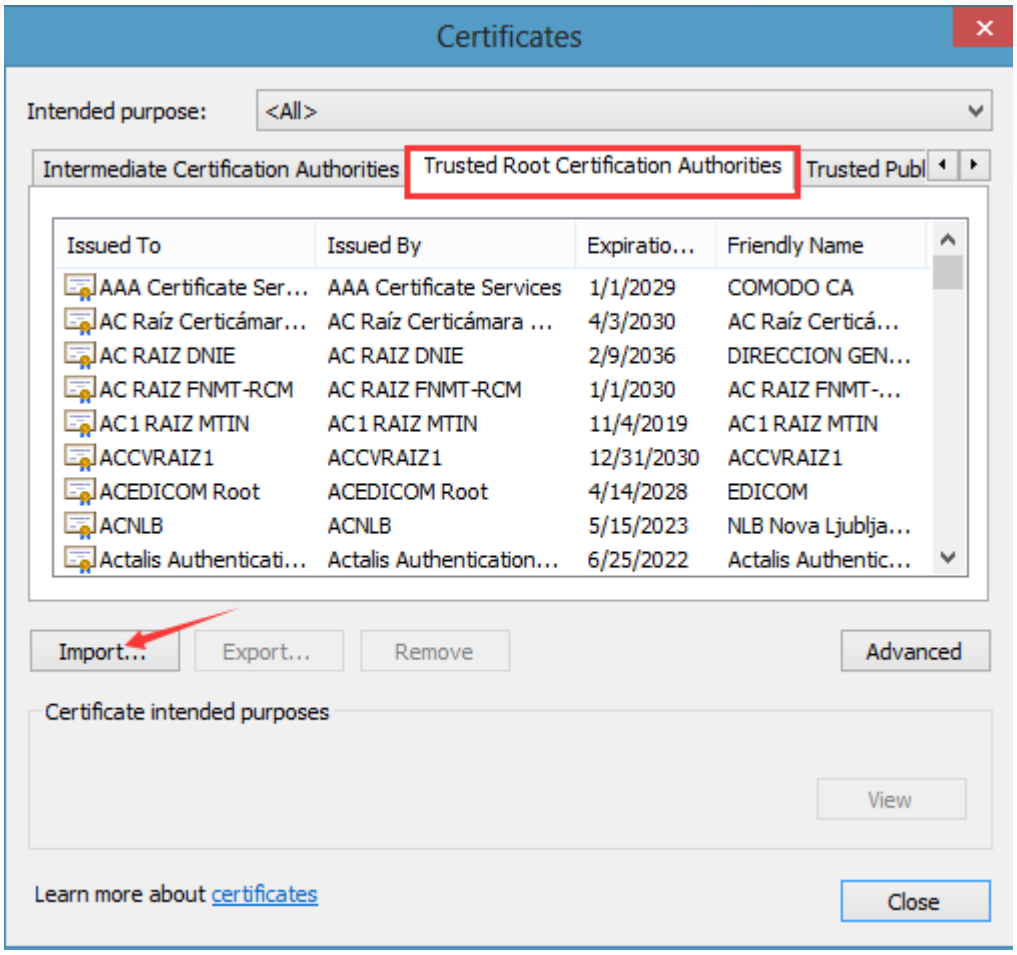
（2） Bind this SSL-proxy profile in policy



（3） Export CA certificate from FW and import to browser

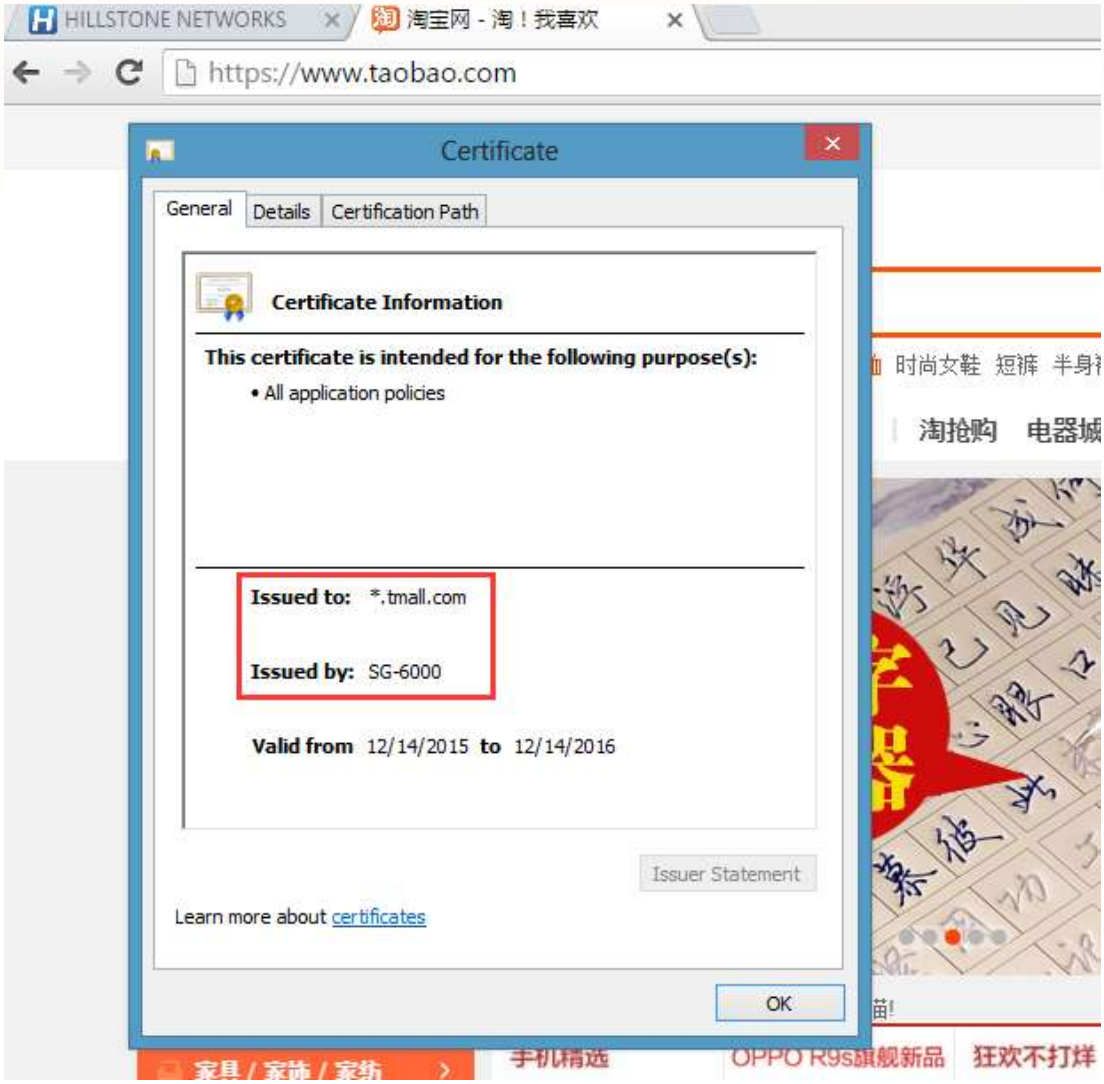


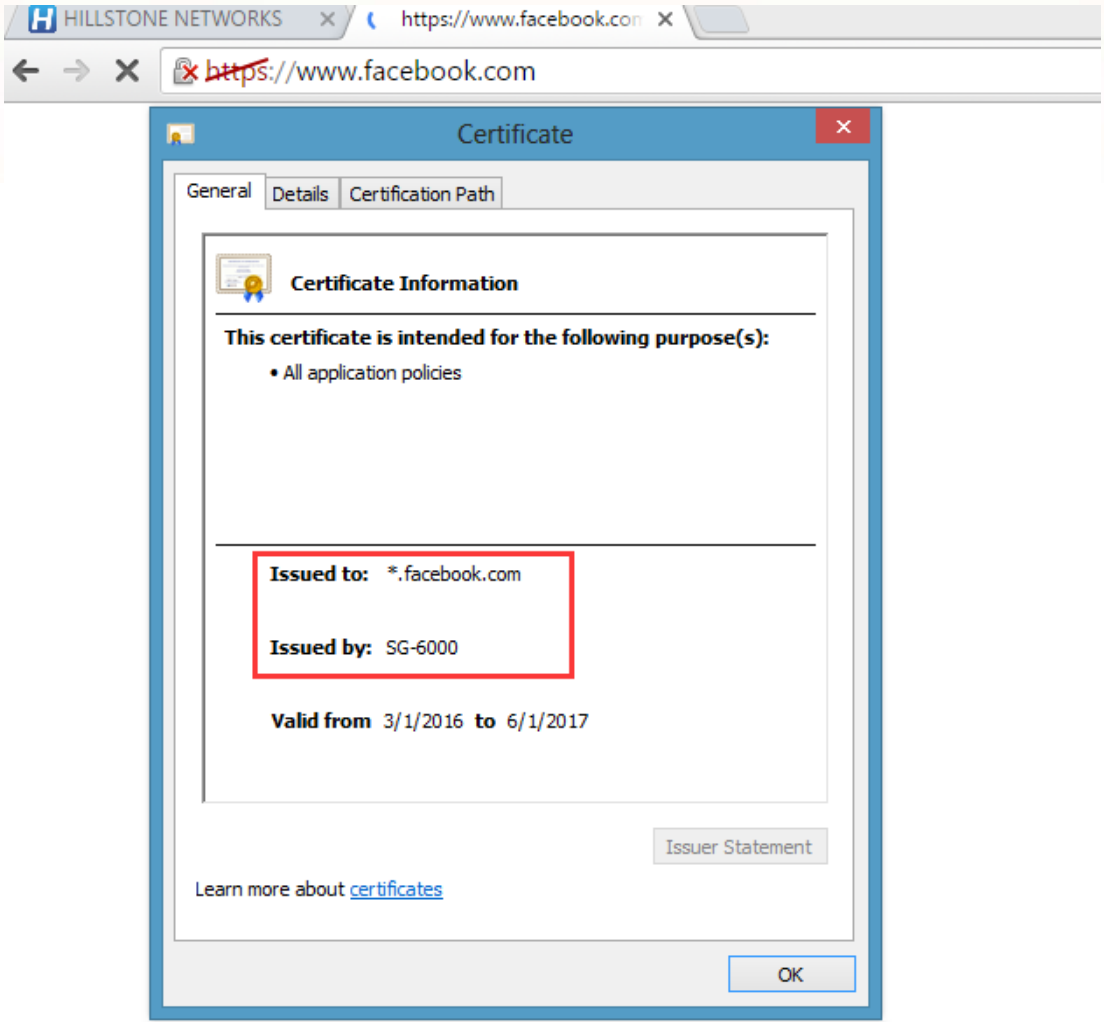
Import the root certificate to the “Trusted Root Certification Authorities” of client browser



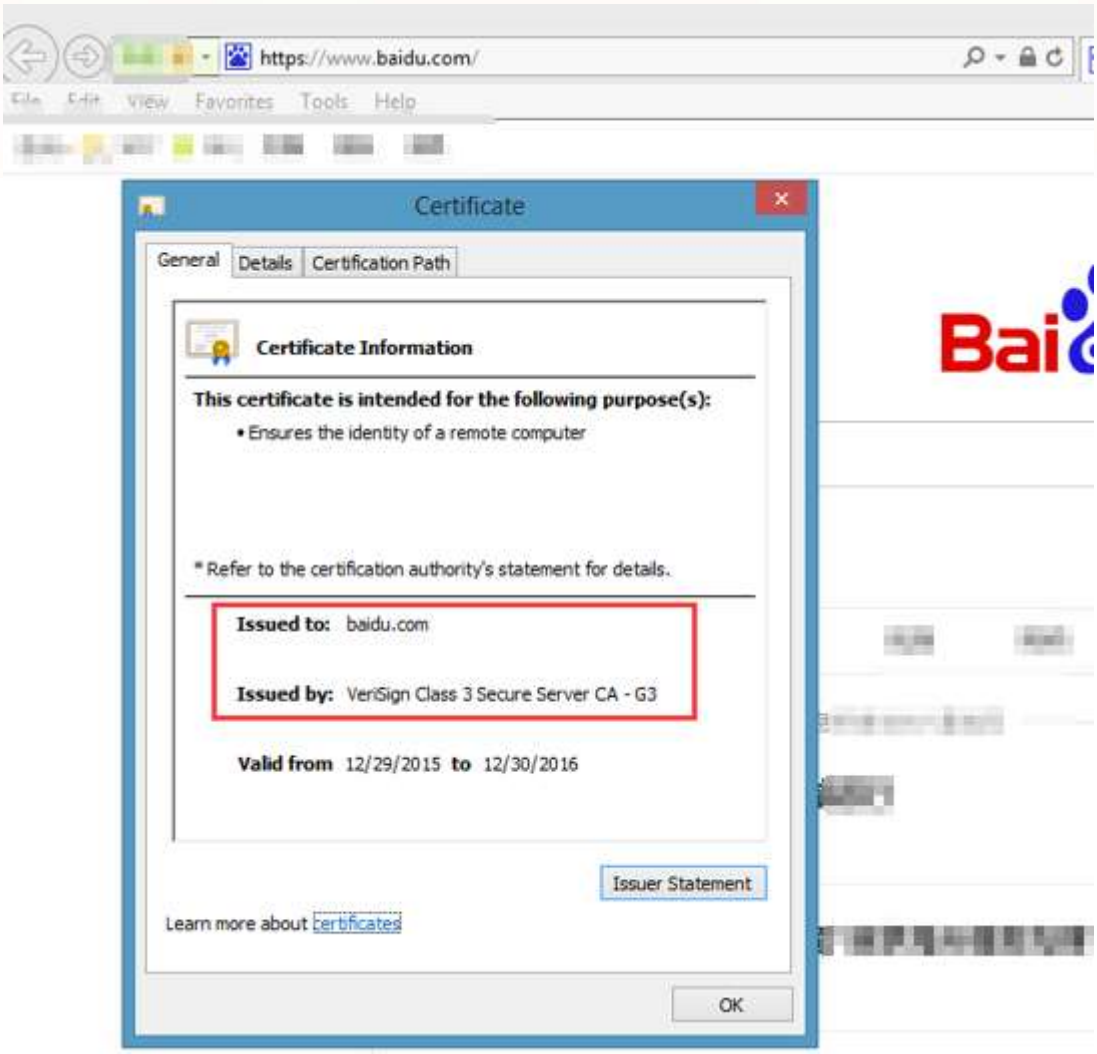
(4) Verify the result

A. The proxy site:


HILLSTONE NETWORKS
淘宝网 - 淘！我喜欢
https://www.taobao.com
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All application policies
Issued to: *.tmall.com
Issued by: SG-6000
Valid from 12/14/2015 to 12/14/2016
Issuer Statement
Learn more about certificates
OK
时尚女鞋 短裤
淘抢购 电器城
家具 / 家饰 / 家纺
手机精选
OPPO R9s旗舰新品
狂欢不打烊

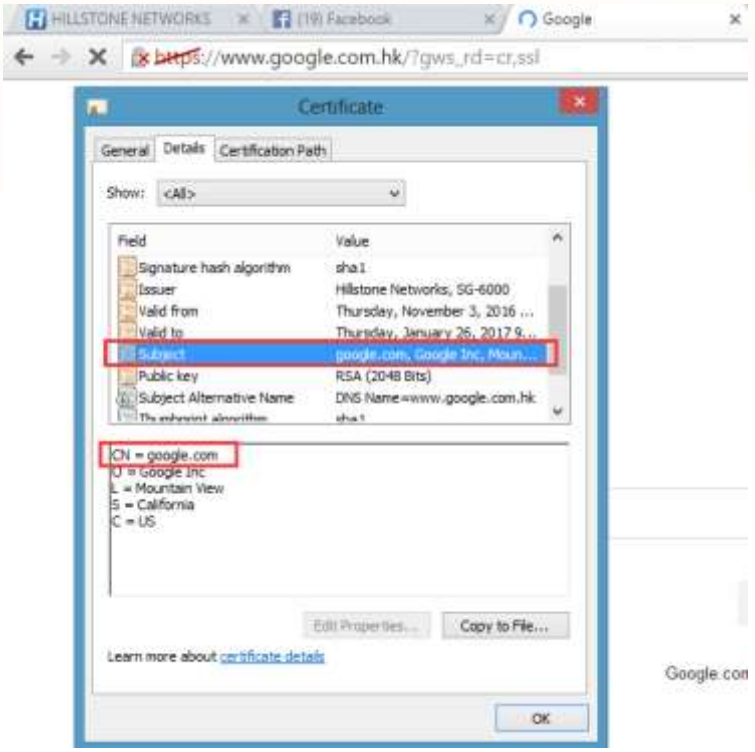


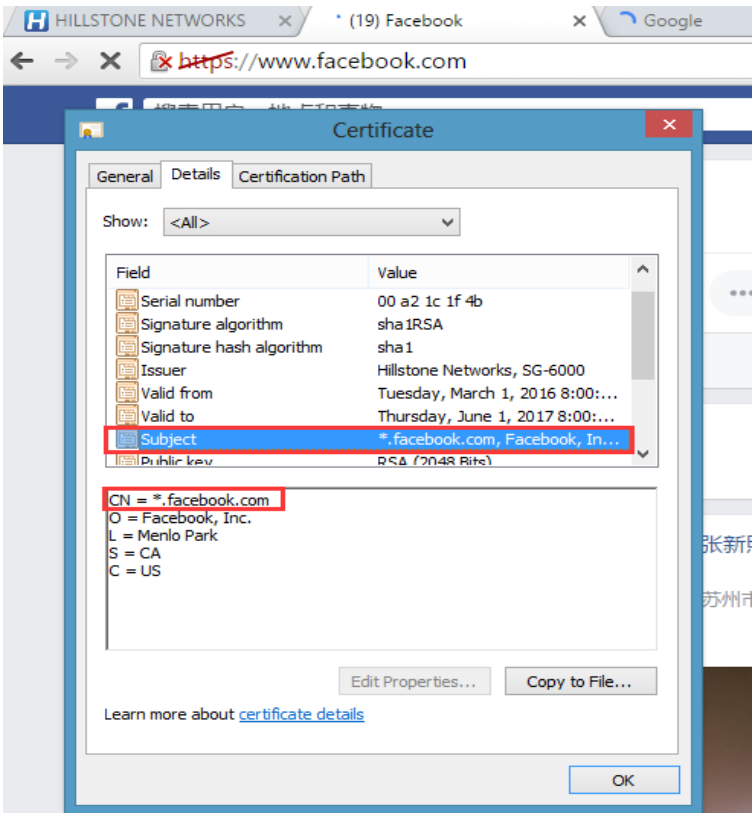
B. Baidu is excepted for proxy



3 Result

（1） ssl-proxy need to check for CA certificate, and use the subject name in certificate which is cn=xxx. Such as google/facebook those different applications need to be identified by decryption





（2） Require mode - the device perform the SSL proxy function on the communication encrypted by the specified website certificate. The communication encrypted by other website certificates will be bypassed.

（3） Exempt mode - the device does not perform the SSL proxy function on the communication encrypted by the specified website certificate. The communication encrypted by other website certificates will be proxied by SSL proxy function.