

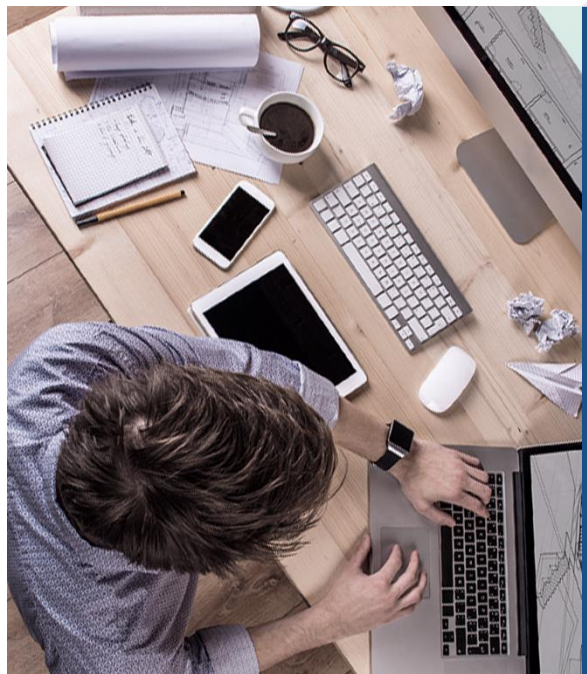


**SANGFOR**

# SANGFOR\_NGAF\_V8.0.47\_Professional

Decryption





- 1 Introduction
- 2 Decrypt data to internal server
- 3 Decrypt data to internet from LAN
- 4 HSTS

# 1. Introduction

---



# Background

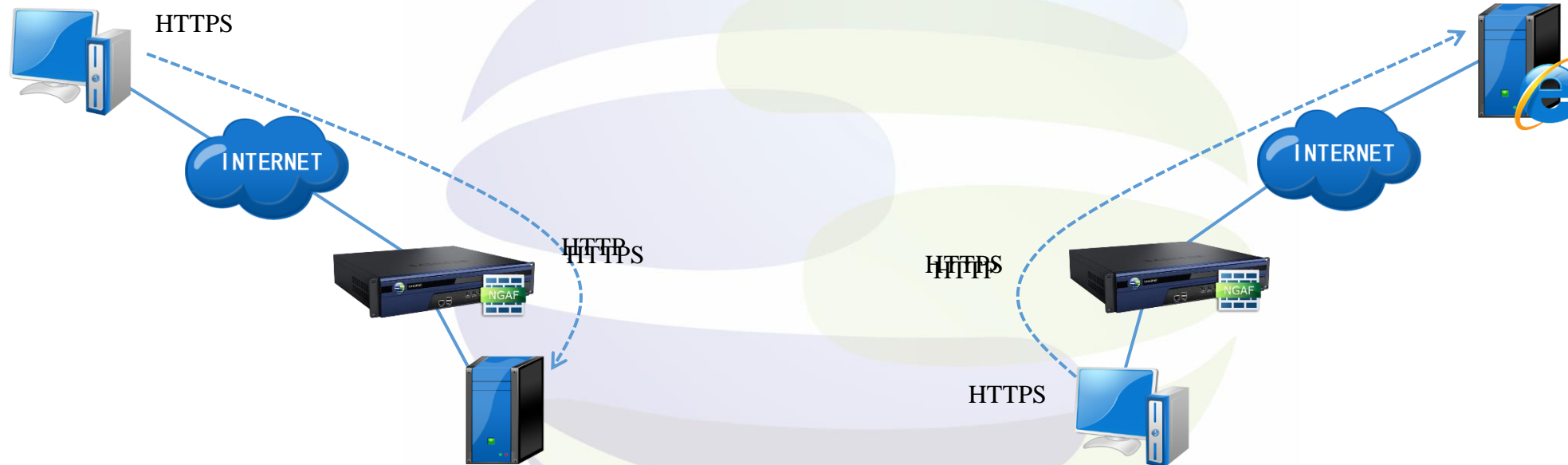
The information you send on the Internet is passed from computer to computer to get to the destination server. Any computer in between you and the server can see your personal details, and other sensitive information if it is not encrypted with an SSL certificate. When an SSL certificate is used, the information becomes unreadable to everyone except for the server you are sending the information to. This protects it from hackers and identity thieves.

As a consequence, the growing adoption of SSL protocols to encrypt Internet communication is providing cyber criminals with more means to evade detection. Sangfor NGAF can inspect HTTPS traffic by acting as a man in the middle.

# Scenario

There are two scenarios of SSL decryption.

1. Decrypt data to internal server from the Internet.
2. Decrypt data to the Internet from the LAN



Client access the inside HTTPS server with decryption inspection to protect the inside server.

Client access the external HTTPS server with decryption inspection to protect the internal host.

## 2. Decrypt data to internal server

---



**SANGFOR**  
深信服科技

# Decrypt data to internal server from the Internet



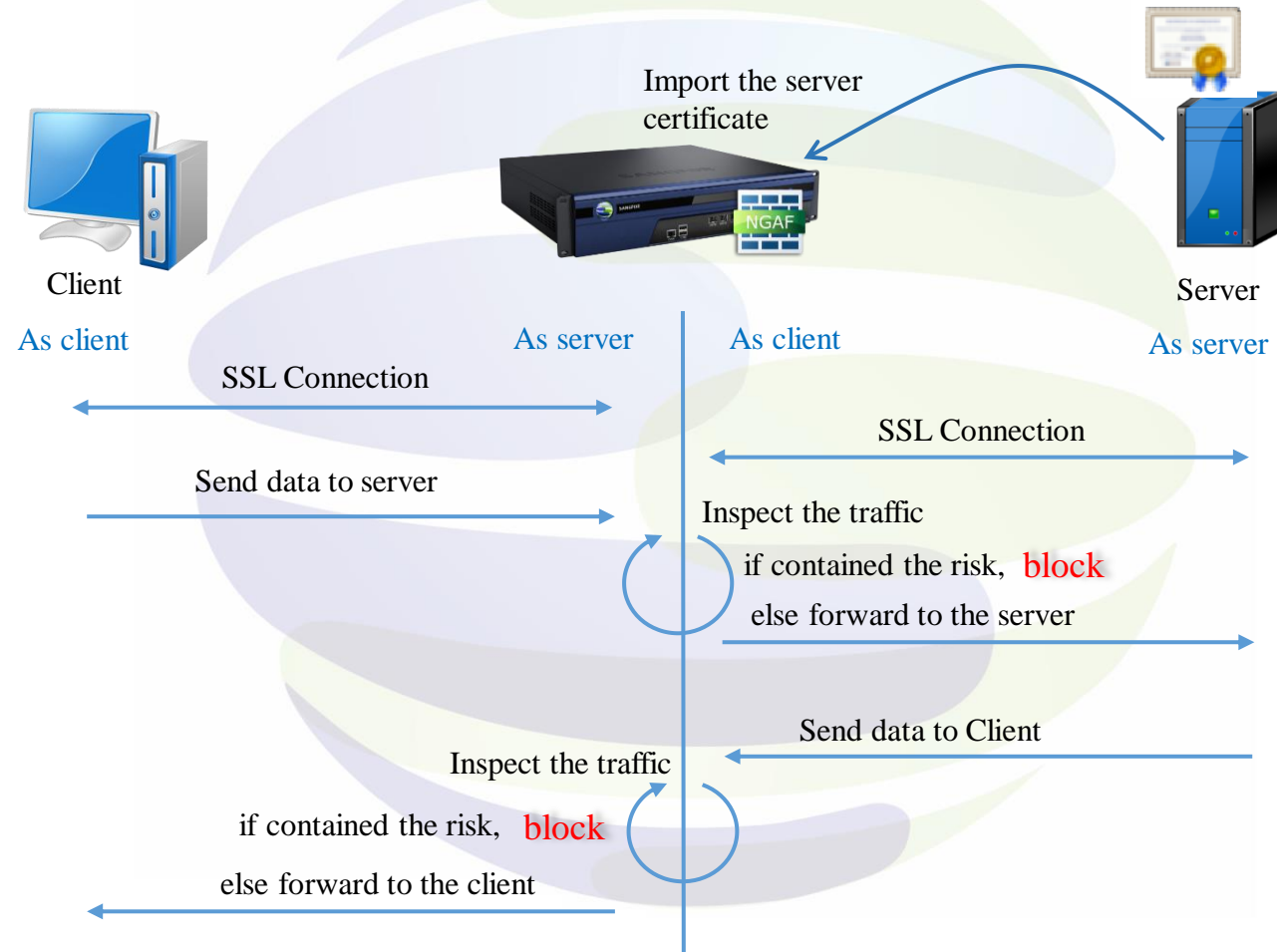
## Theory

The client hand shake with NGAF at first, after the handshake is successful, NGAF initiates the SSL connection with the real server (NGAF is the client). When the handshake succeeded, NGAF accepts and decrypts the data client sent, the decrypted data will be sent to the WAF and other functions for inspection. If found attack, them block, otherwise forward the data to server. It's the same way to handle the data replied from server.

But NGAF certificate is not in the browser **Trusted Root Certification Authorizes** list, we should import the server certificate to NGAF.

# Decrypt data to internal server from the Internet

## Theory





# Decrypt data to internal server

Server scenario need to fill in the source zone, source IP group, server IP and port, as well as to add the server's certificate, the default with the **Default** certificate.

(NGAF certificate is not in the browser **Trusted Root Certification Authorizes** list, browser will pop up an alert webpage. It needs to import the server certificate to NGAF.)

Setting server protection scenarios require customer to provide public key and private key, and if there is a password, it is also need to be provided provide a password (the specific format will be described below)

**Add Decryption Policy**

Enable

Name:

**Objects**

Zones:

Network Objects:

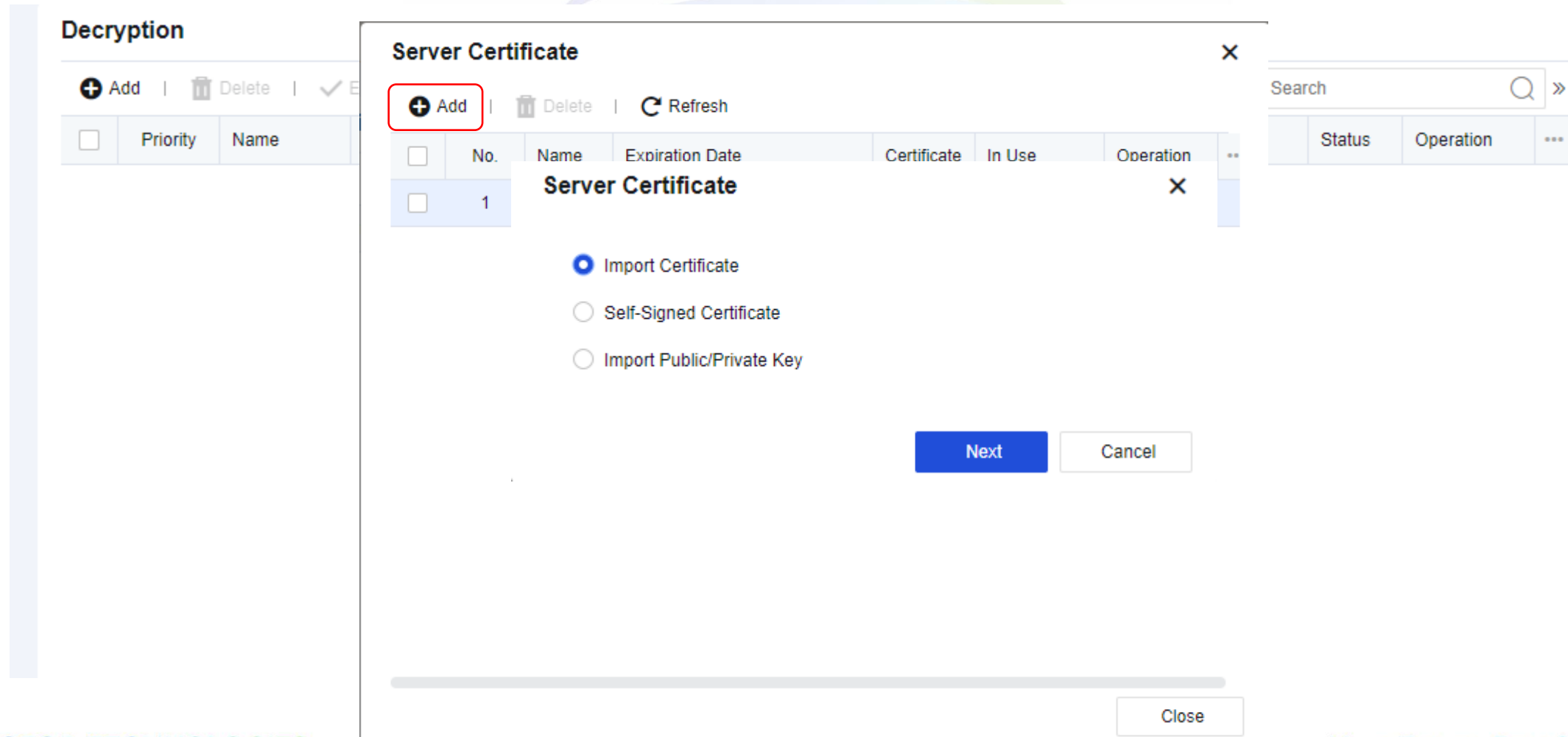
Service:  Decrypt data to internal server from the internet  Decrypt data to the internet from the LAN ⓘ

Server IP Address/Port

IP	Port	Server Type	Operation	...
<input type="checkbox"/> 192.168.1.1	443	Web server	Delete	

# Decrypt data to internal server

How to import the server certificate?



The screenshot displays the 'Decryption' interface with a 'Server Certificate' dialog box open. The dialog box has a title bar with a close button (X) and a toolbar with '+ Add', 'Delete', and 'Refresh' icons. The 'Add' icon is highlighted with a red box. Below the toolbar is a table with columns: No., Name, Expiration Date, Certificate, In Use, and Operation. The first row is selected and contains the value '1' in the 'No.' column and 'Server Certificate' in the 'Name' column. Below the table are three radio button options: 'Import Certificate' (selected), 'Self-Signed Certificate', and 'Import Public/Private Key'. At the bottom of the dialog are 'Next' and 'Cancel' buttons. A 'Close' button is located at the bottom right of the dialog box.

**Decryption**

+ Add | Delete | ✓ E

Priority	Name

**Server Certificate** X

+ Add | Delete | Refresh

No.	Name	Expiration Date	Certificate	In Use	Operation
1	Server Certificate				X

Import Certificate

Self-Signed Certificate

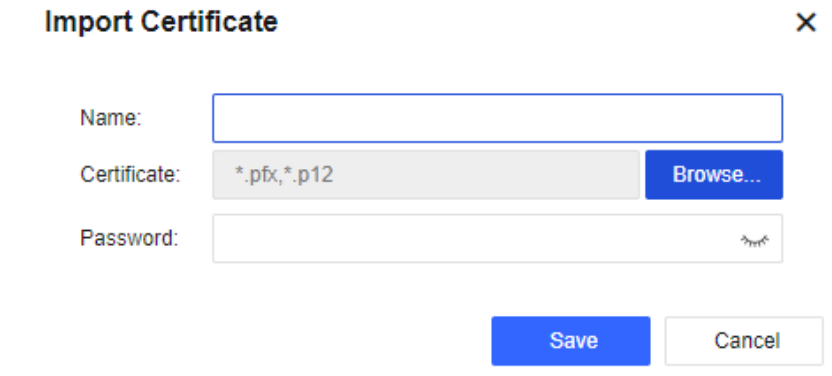
Import Public/Private Key

Next Cancel

Close

# Decrypt data to internal server


## 1. Import Certificate



Import Certificate

Name:

Certificate: \*.pfx, \*.p12

Password:  

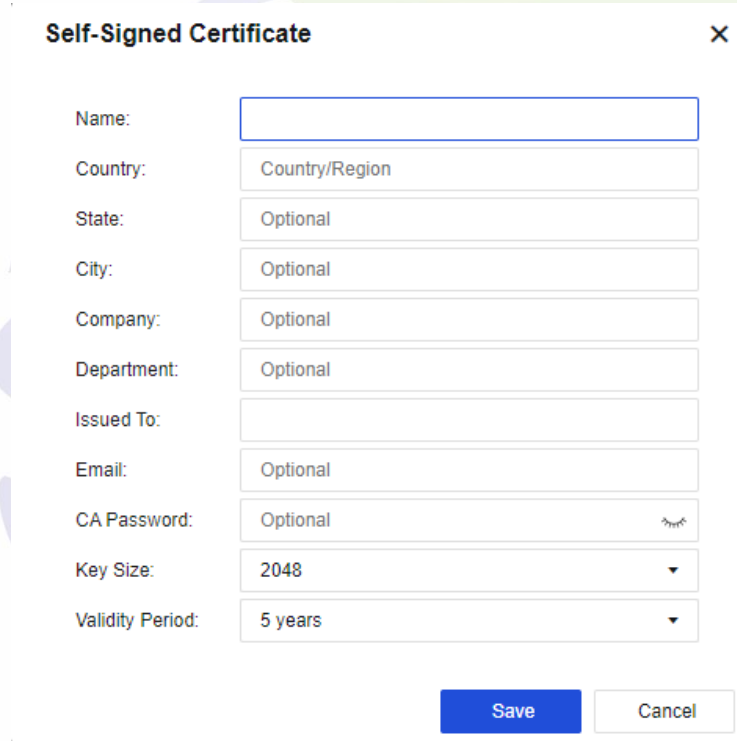
.pfx, .p12, these two certificates are a combination of public key and private key (It only can be decrypted by importing public key and private key )

You can export the certificate from the server as below:

```
openssl pkcs12 -export -in server.crt -inkey server.key -out server.pfx
```

# Decrypt data to internal server

## 2. Self-signed Certificate



Self-Signed Certificate

Name:

Country:

State:

City:

Company:

Department:

Issued To:

Email:

CA Password:

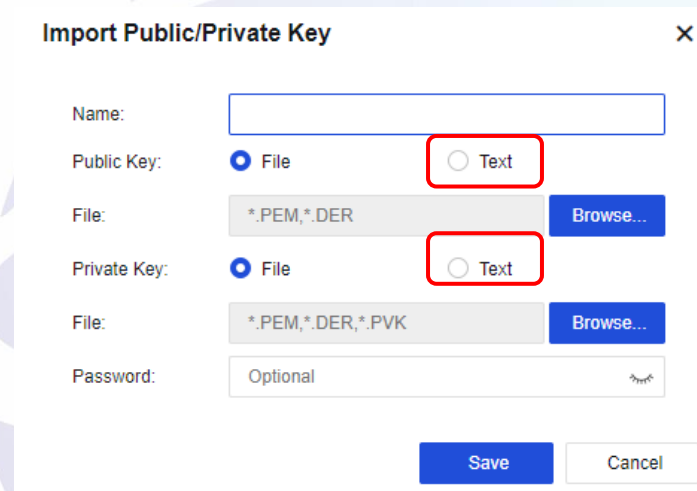
Key Size:

Validity Period:

Self-signed certificate is certificate generated by ourselves acting as a CA(This certificate is not in the browser **Trusted Root Certification Authorities** list, so it is illegal). Browser will pop up a alert webpage if match the policy used this certificate, so generally we do not use it.

# Decrypt data to internal server

## 3. Import Public/Private Key



Import Public/Private Key

Name:

Public Key:  File  Text

File: \*.PEM,\*.DER

Private Key:  File  Text

File: \*.PEM,\*.DER,\*.PVK

Password: Optional

It can be imported by a pair of Public Key and Private Key.

The format of Public Key can be pem, der, crt;

The format of Private Key can be pem, der, cakey;

Crt and cakey can not be imported directly, could copy the text and paste the text at **Text**.

# 3. Decrypt data to internet from LAN

---



**SANGFOR**  
深信服科技

# Decrypt data to the Internet from the LAN

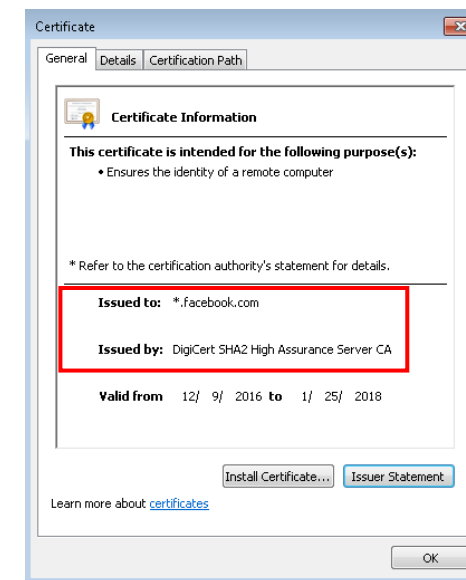
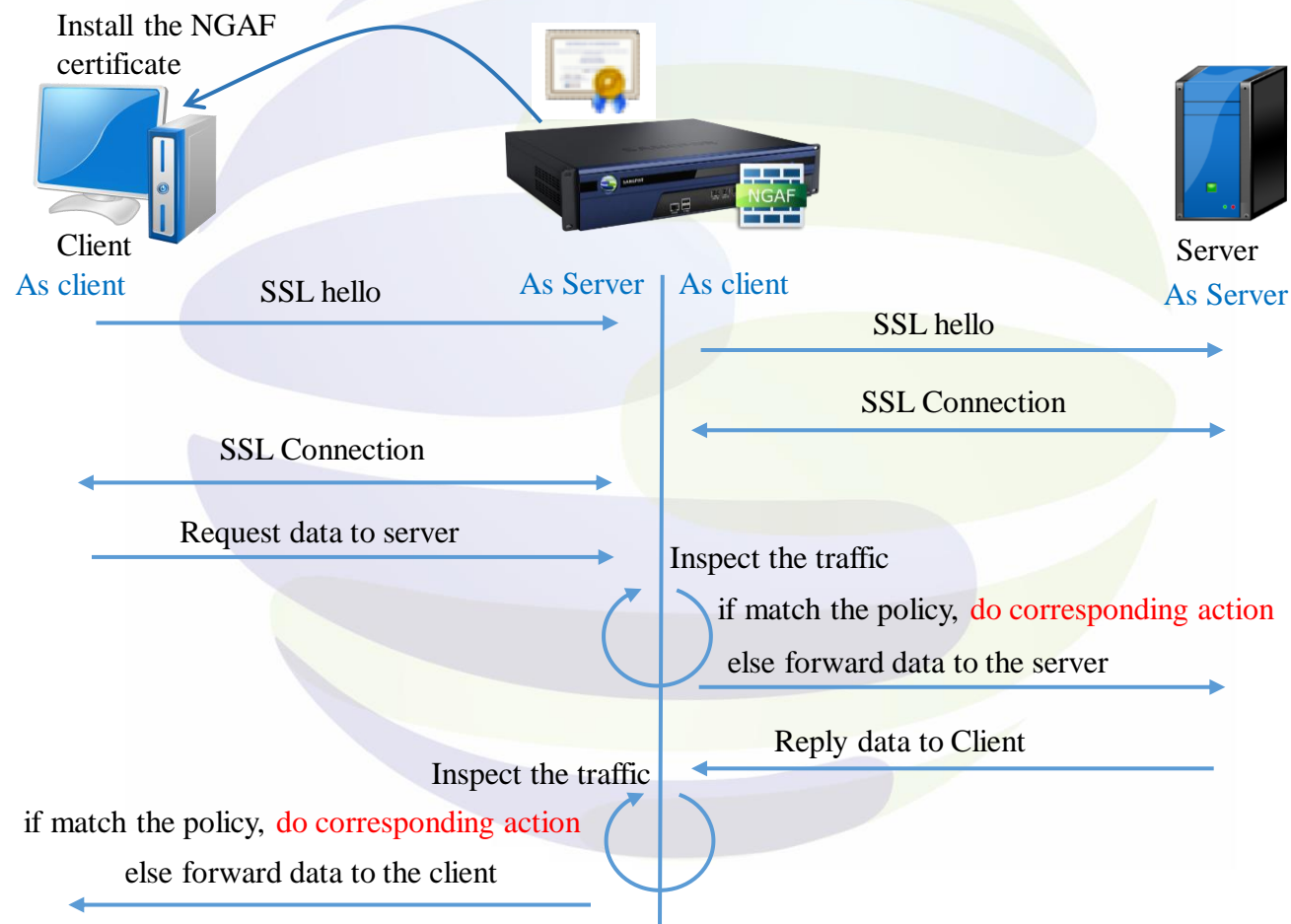
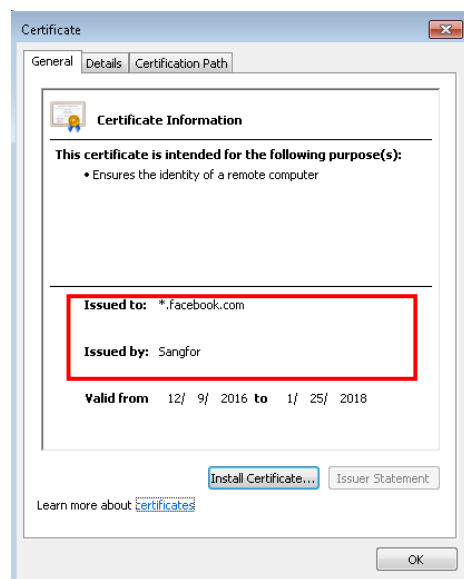
## Theory

When client PC initiate an SSL connection request, NGAF device will act as proxy server and send request to SSL server on behave of client PC, and after connection establish, NGAF will reply to the request of client PC.

NGAF device act as SSL server (for client PC) and as client (for external SSL server). Therefore, client PC and NGAF connection is encrypted using NGAF SSL certificate but the connection between NGAF and external SSL server is using SSL server's certificate to encrypt the data. Thus, client PC will see the certificate is issued by NGAF but not from the original SSL server.

# Decrypt data to the Internet from the LAN

## Theory





# Decrypt data to the Internet from the LAN



User protection scenario need to fill in the source zone, source IP group, websites to be decrypted.

**Edit Decryption Policy** x

Enable

Name: All

**Objects**

Zones: LAN

Network Objects: Private Network Segment

Service:  Decrypt data to internal server from the internet  Decrypt data to the internet from the LAN ⓘ

Website:  Specified  All websites

Sites: IT Related, Science & Technology, Web Application

Upon visit to the following webpage, a user is prompted to install the root certificate ⓘ

URL(https): ⓘ

Root Certificate: X86 | X64 | MAC | Mobile devices

Save Cancel

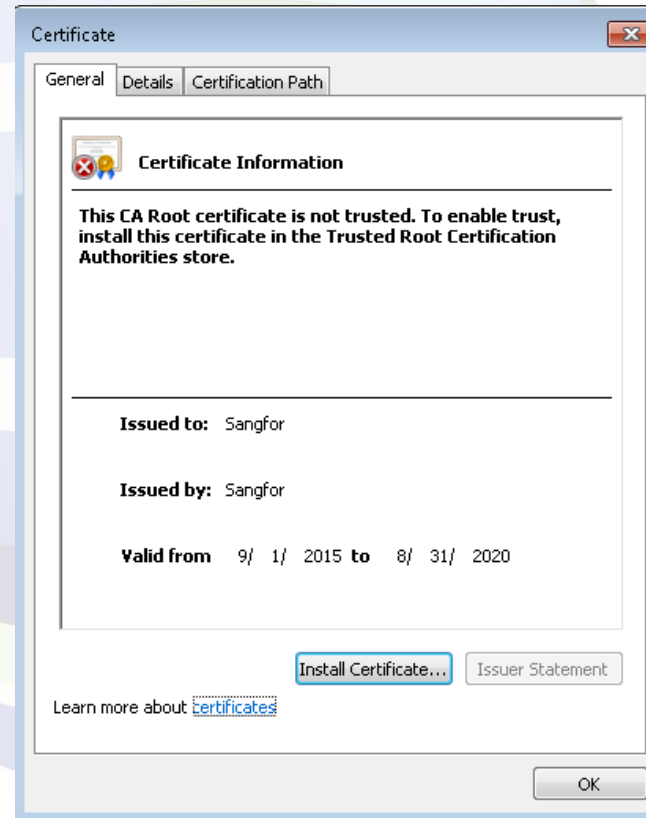
Compared with server protection, there is no certificate could be selected, but clients need to be installed the certificate to eliminate the security alert on browser due to NGAF certificate is not in the browser **Trusted Root Certification Authorizes** list.

# Decrypt data to the Internet from the LAN

There are usually no more than 1 client in the network, How to distribute the certificate to all clients?

There are three ways:

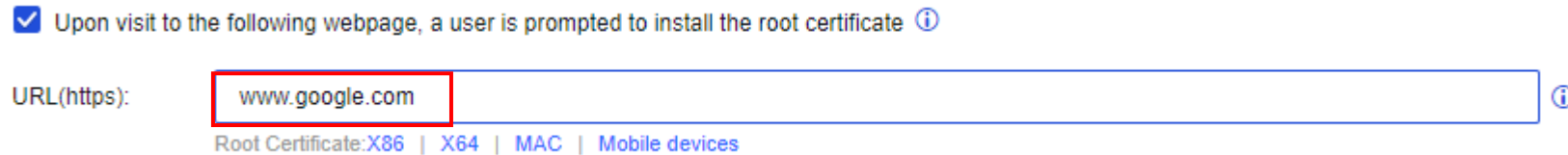
1. Prompt on web browser
2. AD domain
3. User authentication



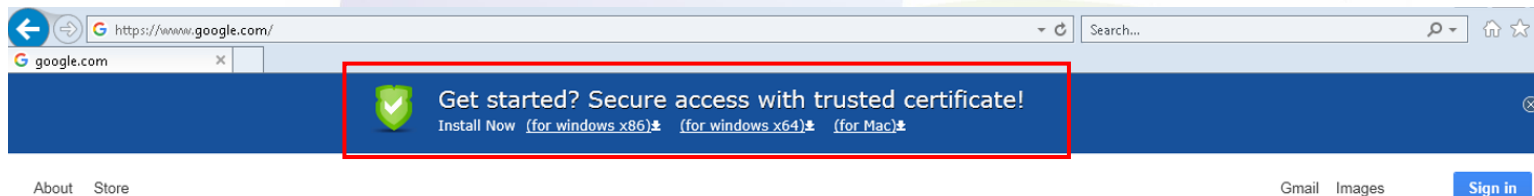
# Decrypt data to the Internet from the LAN

## 1. Prompt on web browser

Set the URL to prompt the certificate



Client can get the download link on the top of website when you visit it.



Google Search

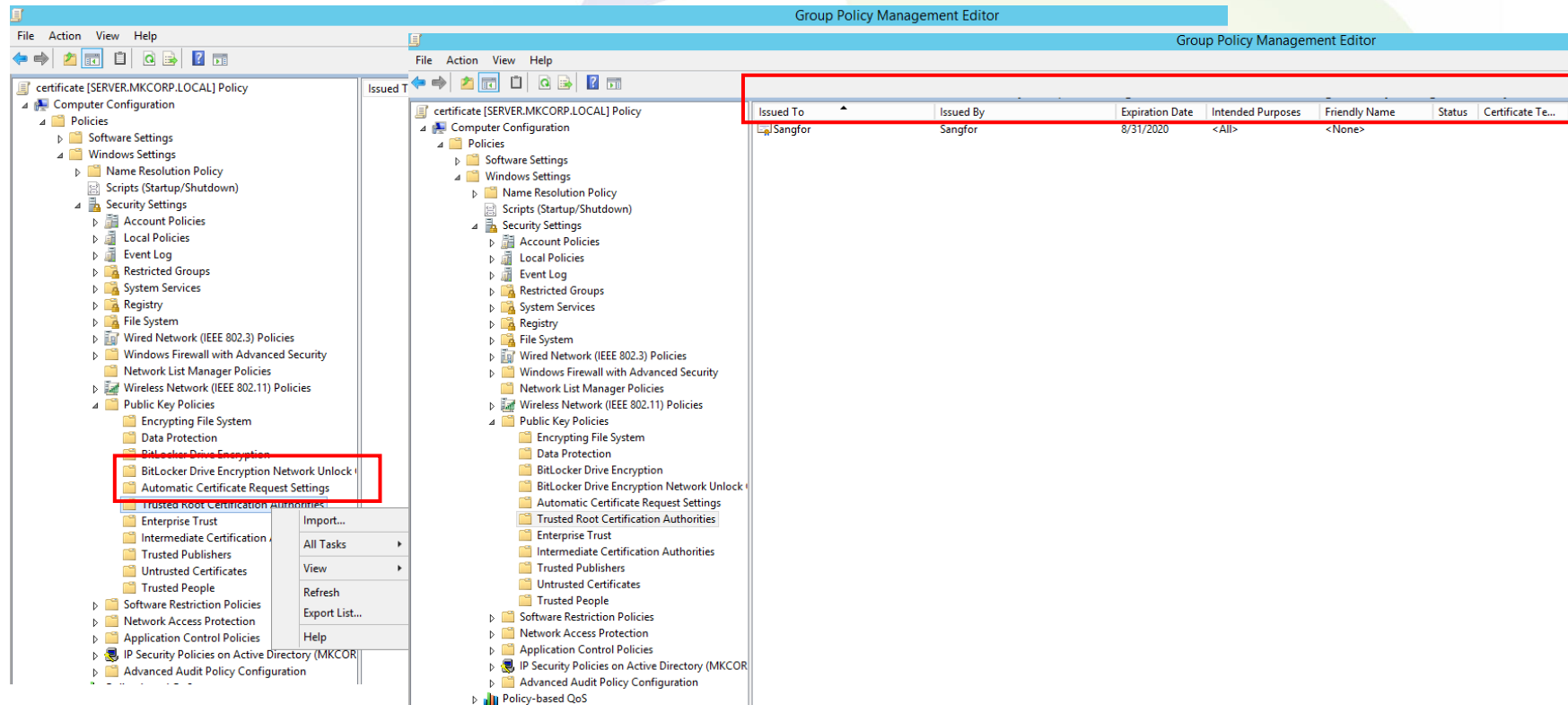
I'm Feeling Lucky

# Decrypt data to the Internet from the LAN

## 2. AD domain

If customer has the domain, it is a good way to distribute the certificate.

Add a **Group Policy** to import the certificate from NGAF to **Trusted Root Certification Authorities**, then update the **Group Policy** to all domain user by ‘gpupdate’.



The screenshot displays the Group Policy Management Editor interface. The left pane shows the tree structure of policies, with 'Public Key Policies' expanded to show 'Trusted Root Certification Authorities'. The right pane shows the details of the selected policy, including a table of issued certificates.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Sangfor	Sangfor	8/31/2020	<All>	<None>		

# Decrypt data to the Internet from the LAN

## 3. User authentication

Installed the certificate is combined with the user authentication by enable the following option, forcing user to install the certificate.

**Authentication Options**

Options	Others
SSO Options	<input checked="" type="checkbox"/> Auto-log out users who are idle for a specified period of time
Auth Page Redirection	Idle Time (mins): <input type="text" value="120"/> ⓘ
Authentication Conflict	<input type="checkbox"/> Submit user credentials over SSL
Obtain MAC By SNMP	<input checked="" type="checkbox"/> DNS service is available before a user passes authentication
<b>Others</b>	<input checked="" type="checkbox"/> Basic services (except HTTP/HTTPS) are available before a user passes authentication
	<input type="checkbox"/> Require authentication again if MAC address is changed
	<input checked="" type="checkbox"/> Lock users if authentication attempts reach the threshold ⓘ
	Max Attempts: <input type="text" value="2"/>
	Lockout Duration (mins): <input type="text" value="1"/> ⓘ
	<input checked="" type="checkbox"/> User can log in only after root certificate is installed

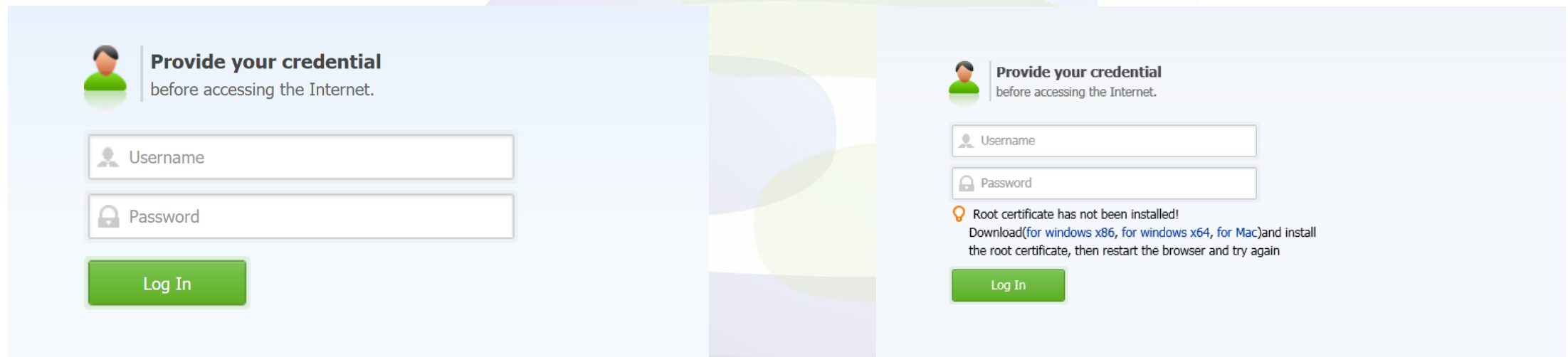
**Save**

# Decrypt data to internal server

Effect of forcing to install the certificate.

Not Enable

Enable



**Provide your credential**  
before accessing the Internet.

Username

Password

Log In

**Provide your credential**  
before accessing the Internet.

Username

Password

Root certificate has not been installed!  
Download(for windows x86, for windows x64, for Mac)and install the root certificate, then restart the browser and try again

Log In

If the certificate has not been installed,  
user can not input the password.

# 4. HSTS

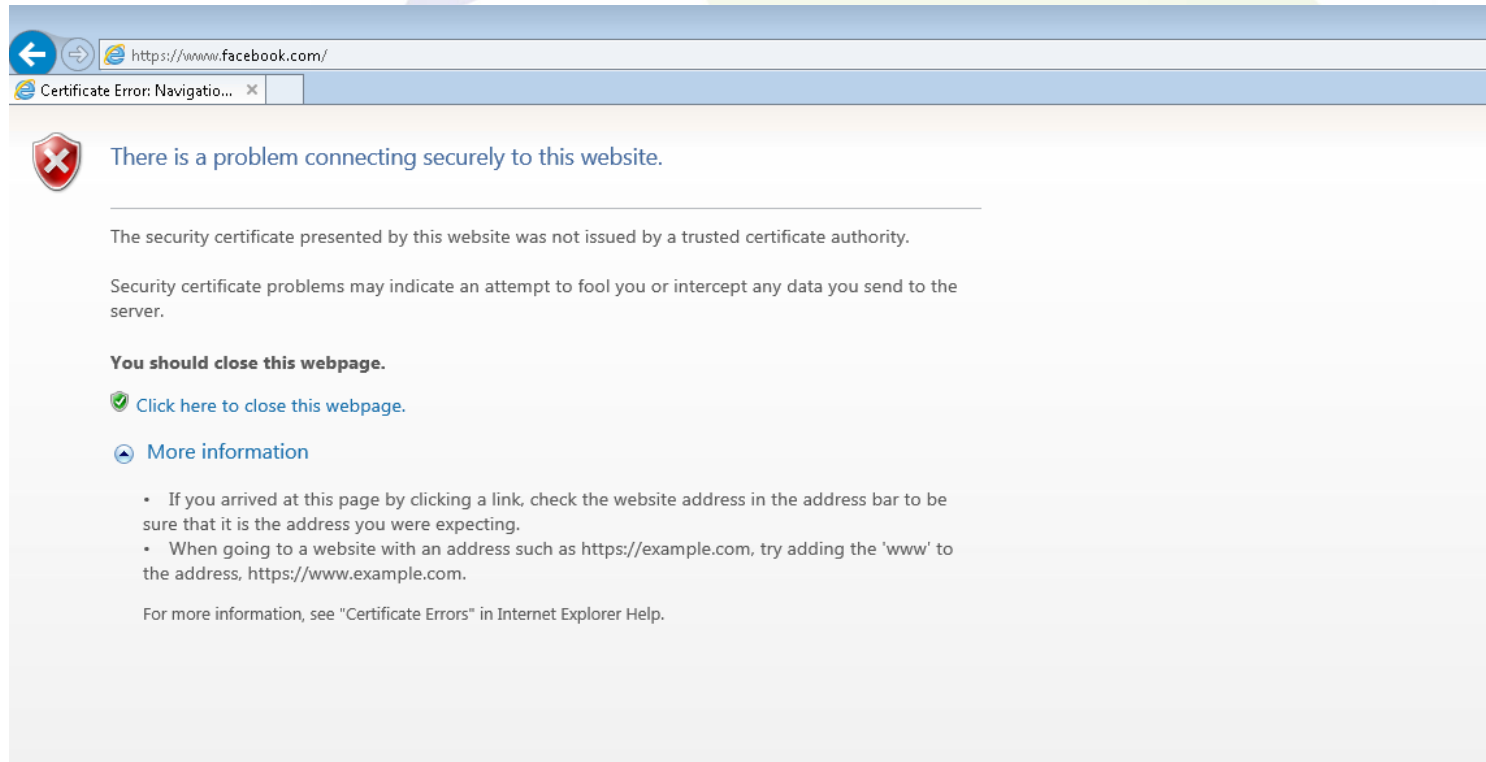
---



**SANGFOR**  
深信服科技

# HSTS

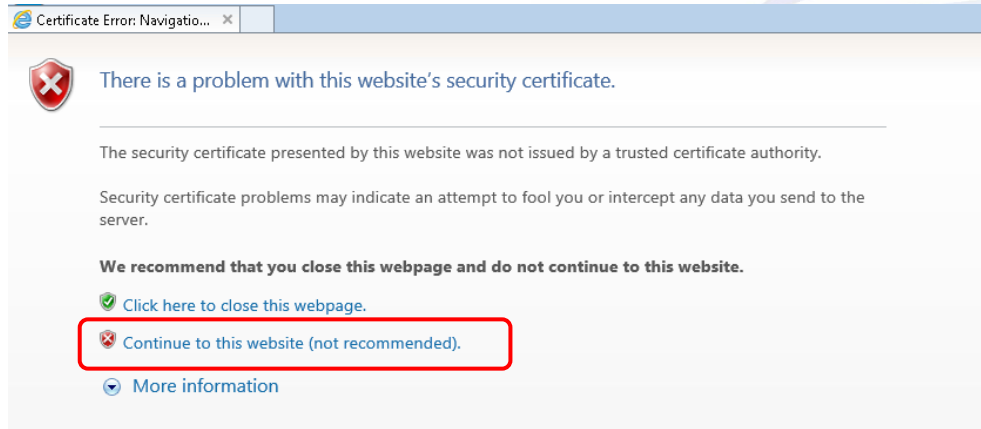
**HSTS (HTTP Strict Transport Security)** is a web security policy mechanism. It can help protect websites against SSL-stripping man-in-the-middle attacks. If the security of the connection cannot be ensured (e.g. the server's TLS certificate is not trusted), show an error message and do not allow the user to access the web application as below.



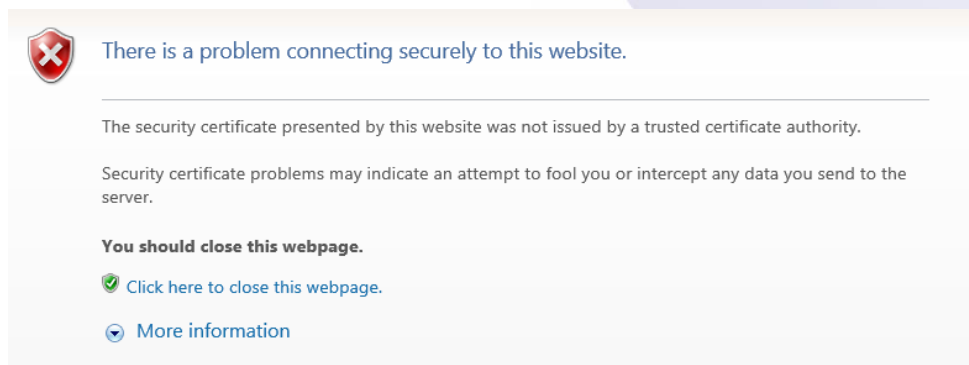


# HSTS

If it is a non-HSTS website and client do not import the NGAF certificate to browser, we can click the ‘Continue to this website(not recommended)’ to browse it

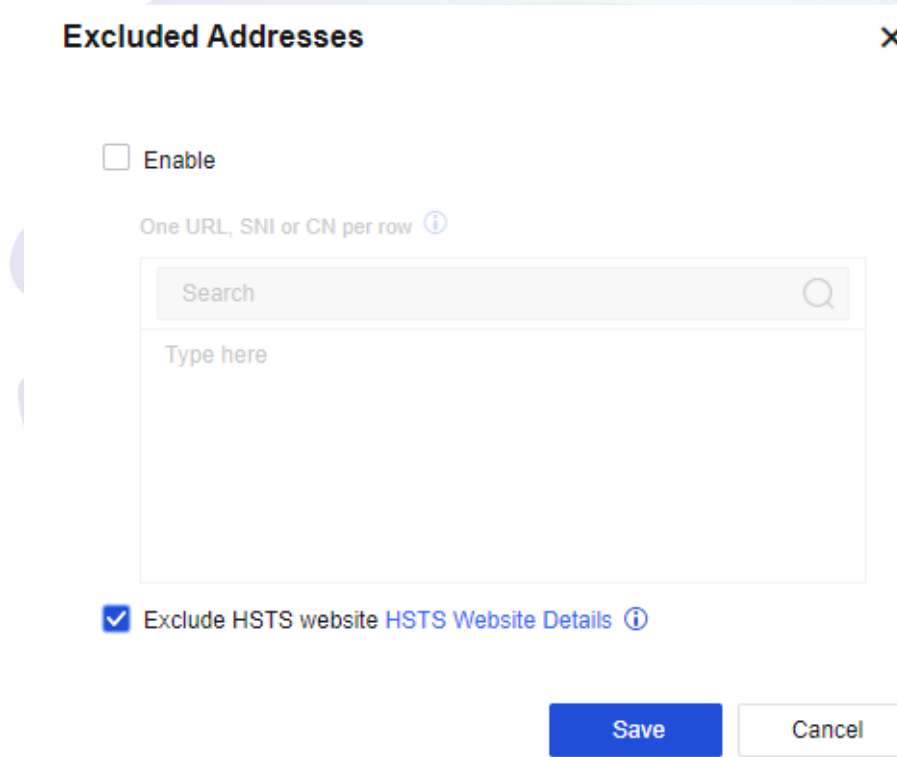


But if client do not install the certificate, there is no option to browse.



# HSTS

There is a built-in HSTS websites list excluded in NGAF to avoid decryption enabled and certificate without installation.



**Excluded Addresses** ×

Enable

One URL, SNI or CN per row ⓘ

Search

Type here

Exclude HSTS website [HSTS Website Details](#) ⓘ

Save Cancel

Notice: If you want to decrypt the HSTS website, the certificate must be installed at first.

# Decryption verified

How to check whether decryption is successful?

## Server Scenario

Test an attack for HTTPS traffic and check whether NGAF can block and log it.

## Internet Access Scenario

Check whether the **'issued by'** of HTTPS website certificate is **Sangfor**.

Test an attack for HTTPS traffic and check whether NGAF can block and log it.

# Thank you !

tech.support@sangfor.com  
community.sangfor.com

## **Sangfor Technologies (Headquarters)**

Block A1, Nanshan iPark, No.1001  
Xueyuan Road, Nanshan District,  
Shenzhen, Guangdong Province,  
P. R. China (518055)

