7.4 Decryption

Decryption is used for the decryption scenarios of encrypted emails and HTTPS data for LAN users who access the internet through the device and the scenario where the LAN has an encrypted server and the NGAF device decrypts the traffic accessing the server to protect the server. You must enable multi-functional authorization to enable this function.

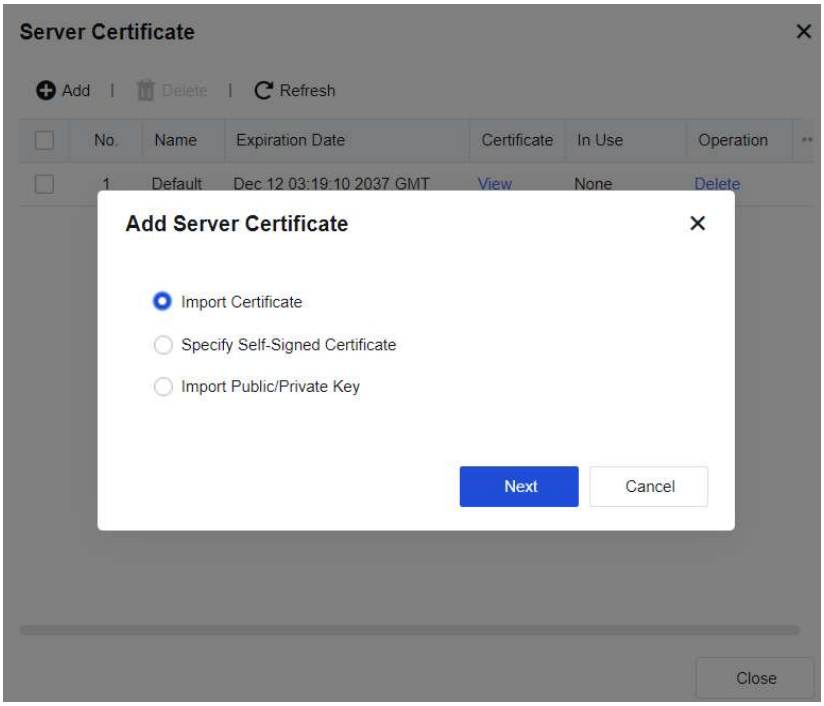
7.4.1 Decrypt Data to Internal Server

The service released by the decryption intranet server applies to the encryption server in LAN. The NGAF device detects the server's traffic by decrypting the traffic accessing the server to protect the server from attacks. See the figure below.

7.4.1.1Configuration Steps

A web application server is released on the intranet of an enterprise to provide internal and external services. The web application server is transmitted via HTTPS protocols. To prevent the webserver from being attacked, HTTPS traffic must be detected to ensure the security of the server.

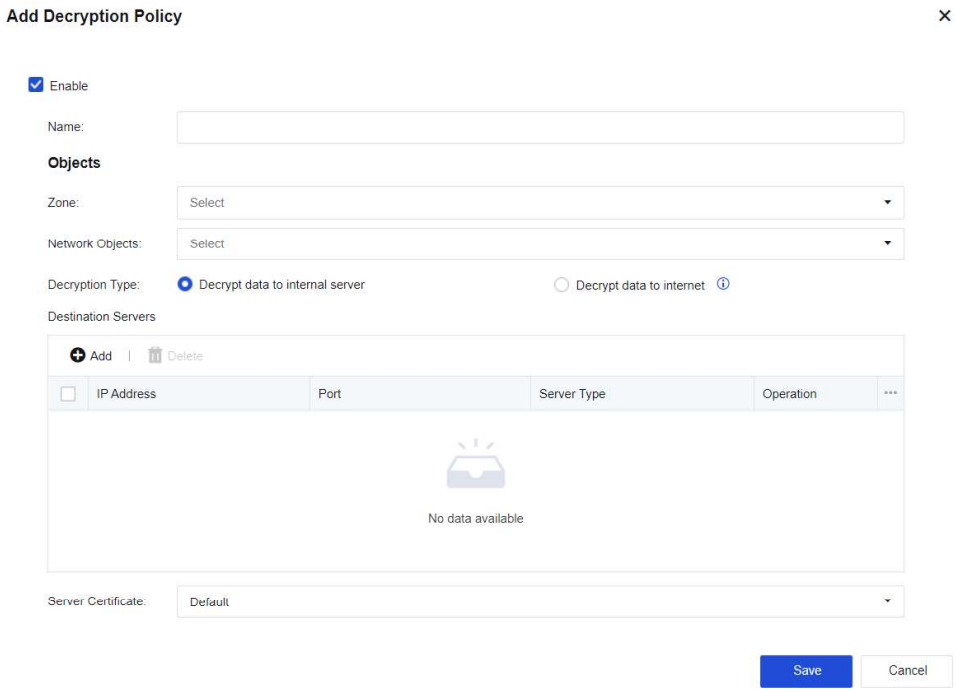
Step 1. Import the HTTPS server certificate. Click **Server Certificate**. Then, the **Server Certificate** dialog box appears. Click **Add** to create a server certificate, as shown in the following figure.



Form of certificate	Note
Import Certificate	Imports a certificate file suffixed with .pfx or .p12. The file contains the public key, private key, and password. Enter the password to decrypt the file.
Specify Self-Signed Certificate	Indicates the custom certificate. You need to manually enter the name, country, issue, key length, and validity period. The rest parameters are optional. A self-signed certificate can be generated after the preceding parameters are set.
Import Public/Private Key	Imports a public or private key certificate. The public key certificate supports a file suffixed with .pem or .der, and the private key certificate supports a file suffixed with .pem, .der, or .pvk. Click Save after the certificate is imported.

Table 15: Description of Actions

Step 2. Click **Add** to create a decryption policy and enter the corresponding information, as shown in the following figure.



Name: Enter a policy name easy to identify.

Zone: Select the source zone for accessing the server.

Network object: Enter the network objects that will access the server.

Decryption Type: If you select **Decrypt data to internal server**, the encryption server is deployed in the LAN zone of NGAF. The **Decrypt data to internet** option applies to the decryption of emails and HTTPS data when LAN users access the internet.

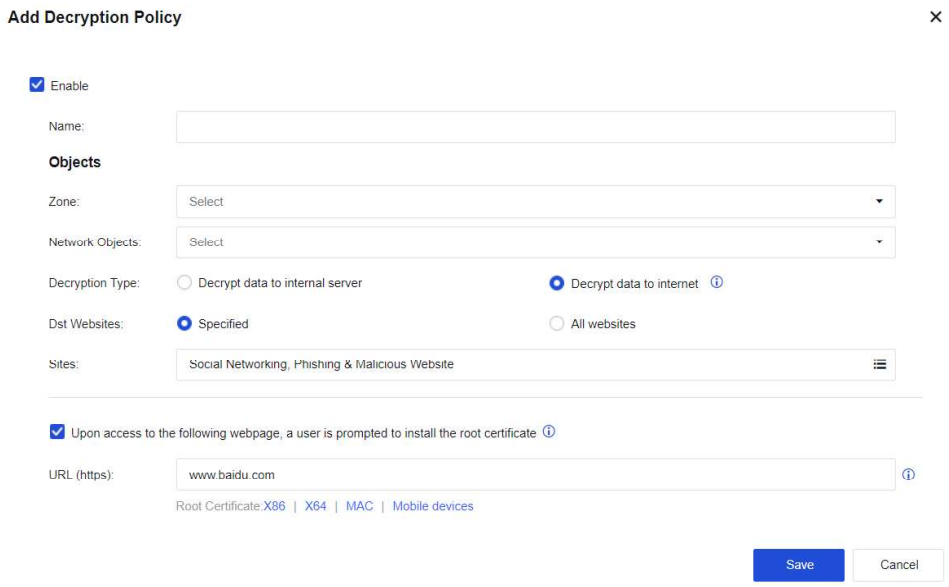
Destination Servers: Add the IP address and port of the server to be decrypted. Web server, mail server, FTP server, and other servers are available.

Server Certificate: Select the certificate of the encryption server. You need to import the server certificate on the **Server Certificate** page.

Step 3. Click **Save**. Then, the policy is added.

7.4.2 Decrypt Data to Internet

Decrypting data to the internet applies to the decryption of emails and HTTPS data when LAN users access the internet through the device. See the figure below.



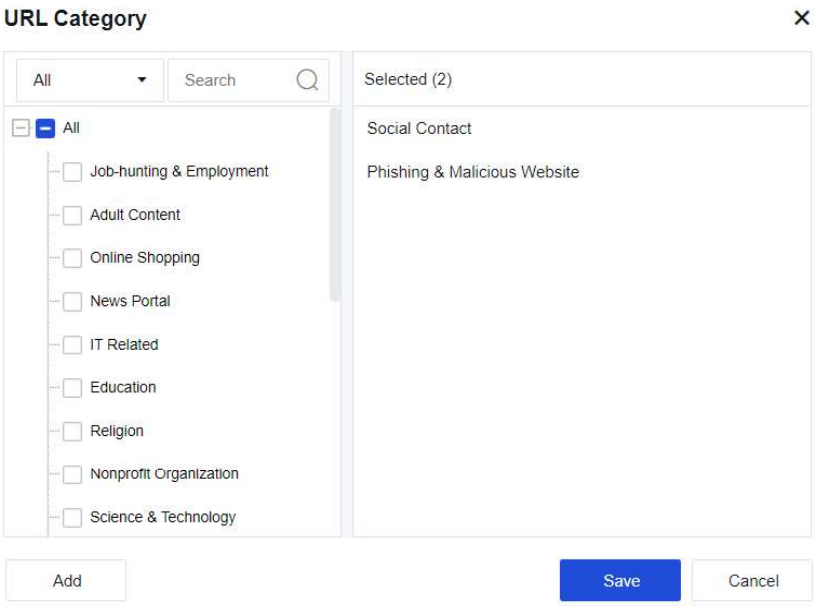
Name: Enter a policy name easy to identify.

Zone: Select the source zone for accessing the internet.

Network object: Enter the network objects that will access the server.

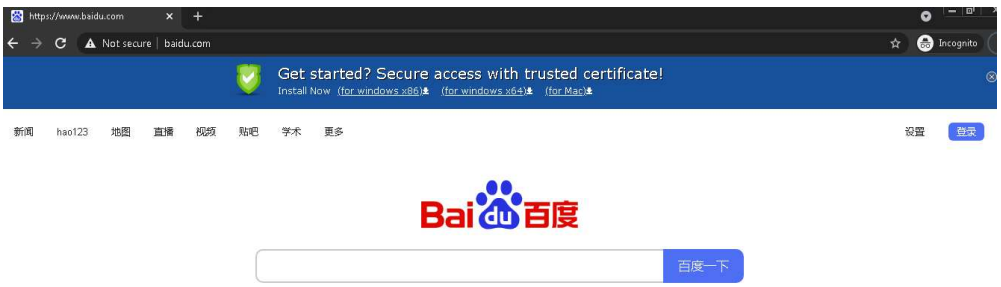
Decryption Type: Select Decrypt data to internet.

Dst Websites: Select **Specified** or **All websites**. If you select **Specified**, select the site category to be decrypted from the URL category database.



Upon access to the following webpage, a user is prompted to install the root certificate: When the decryption function is enabled, a certificate alert message is promoted to a user who accesses the HTTPS website. To avoid this message, select this option and set the URL from which the root certificate is downloaded.

If you set the **URL (HTTPS)** parameter to www.baidu.com, the following page reminding you to install the certificate will be displayed when the LAN user visits https://www.baidu.com.



After the trusted certificate is downloaded and installed, the LAN user will not be prompted to download and install the certificate from Internet Explorer when visiting the HTTPS website.