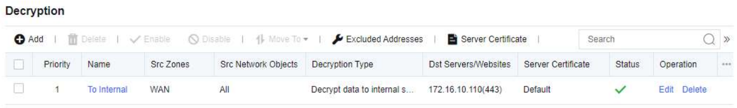
7.4 Decryption

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 Network Secure 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 Network Secure device detects the server's traffic by decrypting the traffic accessing the server to protect the server from attacks. See the figure below.



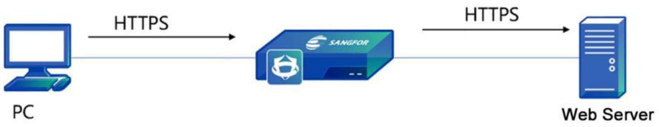
Decryption

Add | Delete | Enable Disable | Move To | Excluded Addresses | Server Certificate |
Search

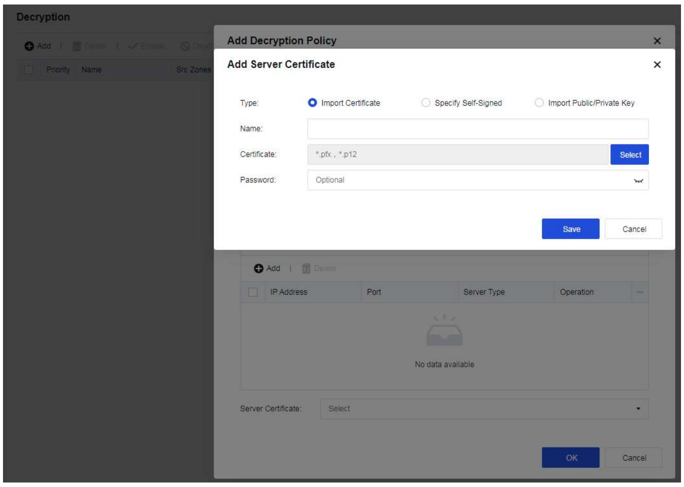
□	Priority	Name	Src Zones	Src Network Objects	Decryption Type	Dst Servers/Websites	Server Certificate	Status	Operation
□	1	To Internal	WAN	All	Decrypt data to internal s...	172.16.10.110(443)	Default	✓	Edit Delete

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.**



Type: ● Import Certificate ○ Specify Self-Signed ○ Import Public/Private Key

Name:

Certificate: *.pfx , *.p12

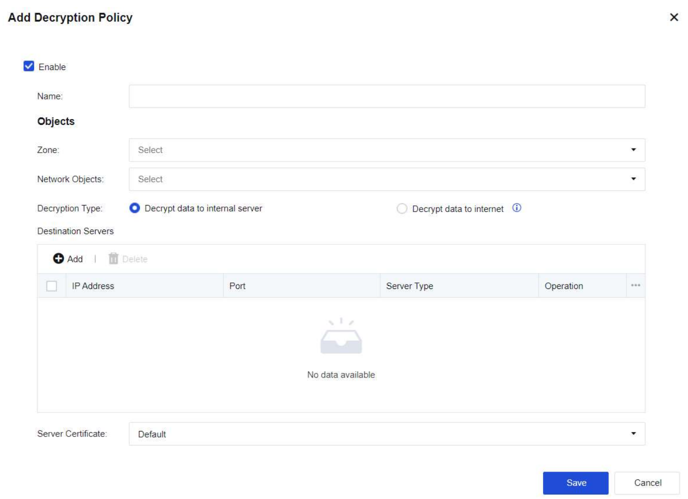
Password: Optional

Server Certificate: Select

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.



Add Decryption Policy

☑ Enable

Name:

Objects

Zone: Select

Network Objects: Select

Decryption Type: ● Decrypt data to internal server ○ Decrypt data to internet

Destination Servers

☐	IP Address	Port	Server Type	Operation

No data available

Server Certificate: Default

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 Network Secure. The **Decrypt data to internet** option applies to the decryption of emails and HTTPS data when LAN users access the internet.

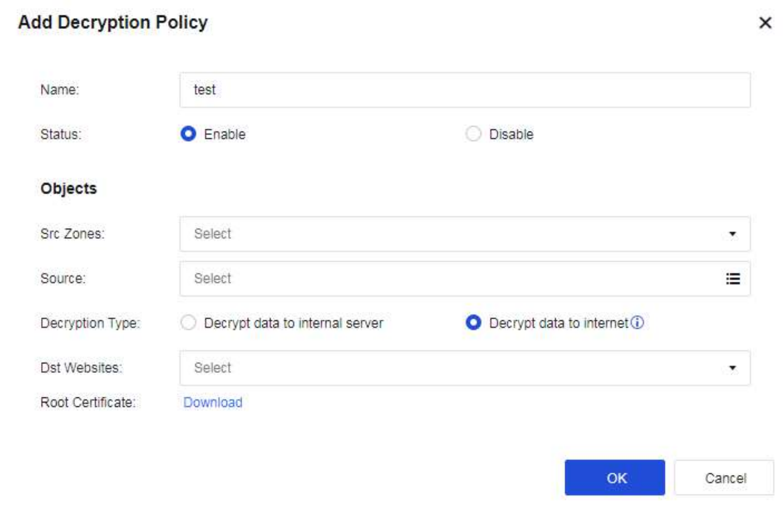
Destination Servers: Add the IP address and port of the server to be decrypted. Web server, mail server, FTP server, and other servers are available.

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.



Add Decryption Policy

Name: test

Status: ● Enable ○ Disable

Objects

Src Zones: Select

Source: Select

Decryption Type: ○ Decrypt data to internal server ● Decrypt data to internet

Dst Websites: Select

Root Certificate: Download

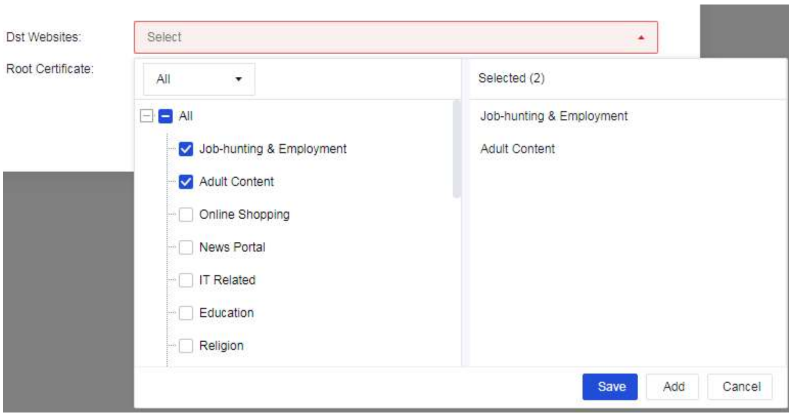
Name: Enter a policy name easy to identify.

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.



Dst Websites: Select

Root Certificate:

All

☐ All
☑ Job-hunting & Employment
☑ Adult Content
☐ Online Shopping
☐ News Portal
☐ IT Related
☐ Education
☐ Religion

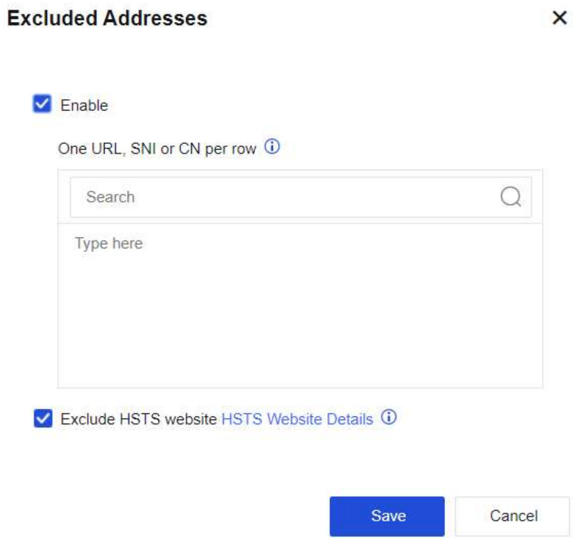
Selected (2)

Job-hunting & Employment
Adult Content

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.

7.4.3 Excluded Addresses

The excluded-address function is to exclude the specified URLs, SNIs, and CNs from the decryption, as shown in the following figure.



Excluded Addresses

☑ Enable

One URL, SNI or CN per row

Search

Type here

☑ Exclude HSTS website HSTS Website Details

NOTE

1. To enable the decryption function, multi-functional authorization must be enabled.

2. This function may impose some pressure on the device's performance. Do not enable it arbitrarily.

3. By default, the encrypted emails of LAN users accessing the WAN are decrypted. You only need to enable a policy for decrypting data accessing sites. The rest of the operations only need to be set in the content security policy.

4. Security of encrypted emails, HTTPS antivirus, HTTPS webpage filtration, and the filtration of HTTPS uploads and downloads rely on the decryption of data accessing sites.

7.5 Bandwidth Management

Bandwidth management is to control the traffic sizes of various web applications by building bandwidth management channels.

The bandwidth management system provides the functions of bandwidth guarantee and limitation. The former ensures the access bandwidths of important applications, whereas the latter restricts the total inbound and outbound bandwidths of user groups/users and those of various applications.