1 Release NotesBasic Information

Product Model	NTA NX3-2000E/1000E
Software Version	V4.5R90F00SP01
Upgrade File	update_nta_V4.5R90F00SP01.180104build25612.bin MD5: 9B64379FC70A5F1A179DC3C3B1BDD3AB
Release Date	2018-01-05
How to Obtain	Obtain the upgrade file from the upgrade system or contact technical support personnel of NSFOCUS.

2. Version Mapping

Product Model	NTA NX3-2000E/1000E (NSF-2800)
ADS M	V4.5R90F00
ADS	• V4.5.88.15 • V4.5R90F00
Threat Analysis and Traceback System (TAT)	V2.0.0
Client Browser	• Chrome • Firefox • Internet Explorer 10
Documentation	NSFOCUS NTA Installation Guide/User Guide (V4.5R90F00)

3. Satisfied Requirements

No.	Requirement Description
1	Transmission of syslog messages in an encrypted manner
2	Fix of some bugs

4. Upgrade Procedure

The source version for the upgrade must be V4.5R90F00.

The upgrade procedure is as follows:

Step 1 Log in to the web-based manager of NTA and choose **Administration** > **System Upgrade**.

Step 2 Browse to the upgrade file **update_nta_V4.5R90F00SP01.180104build25612.bin**, and click **Upload**.

Step 3 Read upgrade notes and click **Confirm Upgrade** to continue the upgrade.

Step 4 Wait 5 minutes for the installation to complete before refreshing the current page.

Step 5 Click **About** in the upper-right corner of the web-based manager to check the current system version.

If **Product Version** is **V4.5R90F00SP01**, the upgrade succeeded; if not, the upgrade failed and you need to contact technical support personnel of NSFOCUS.

----End

It is normal that the following situations arise during upgrade:

1. The SSH client is disconnected.
2. The web-based manager displays an error message "502 Bad Gateway" or directly denies your access request.
3. All engines stop working.

Note	• The installation takes about 5 minutes. Later, you need to manually refresh the page. • The system will automatically restart after the installation is complete.

5. Function Changes

5.1 Transmission of Syslog Messages in an Encrypted Manner

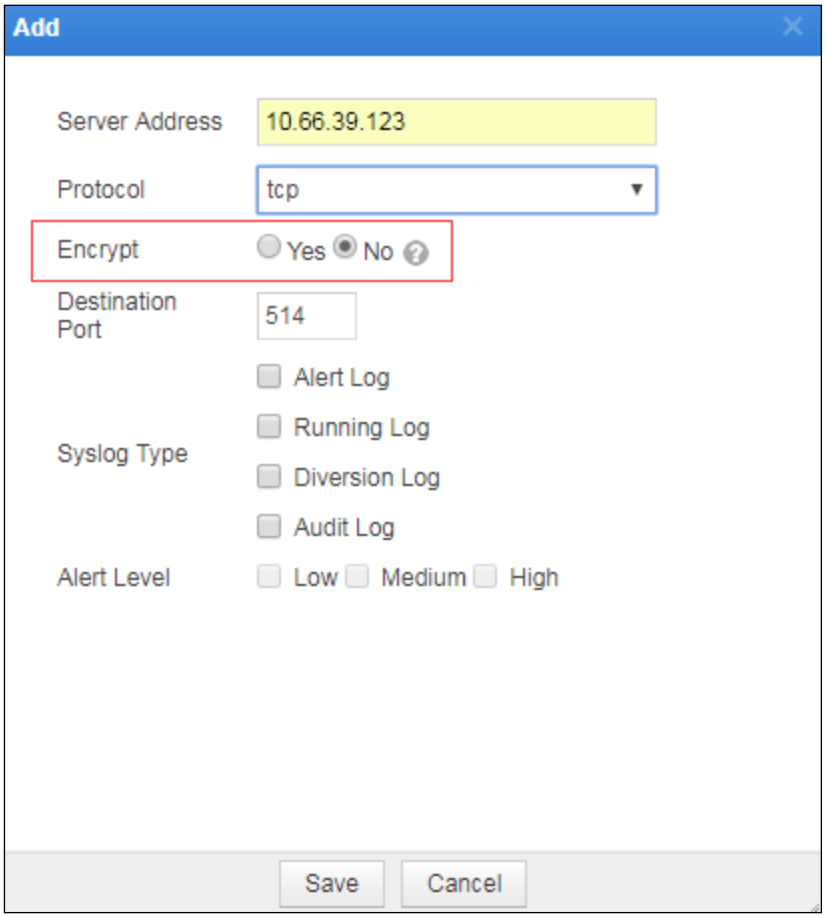
Scenario

Transmission of syslog messages from a client to a server may take place in an intranet or an extranet.

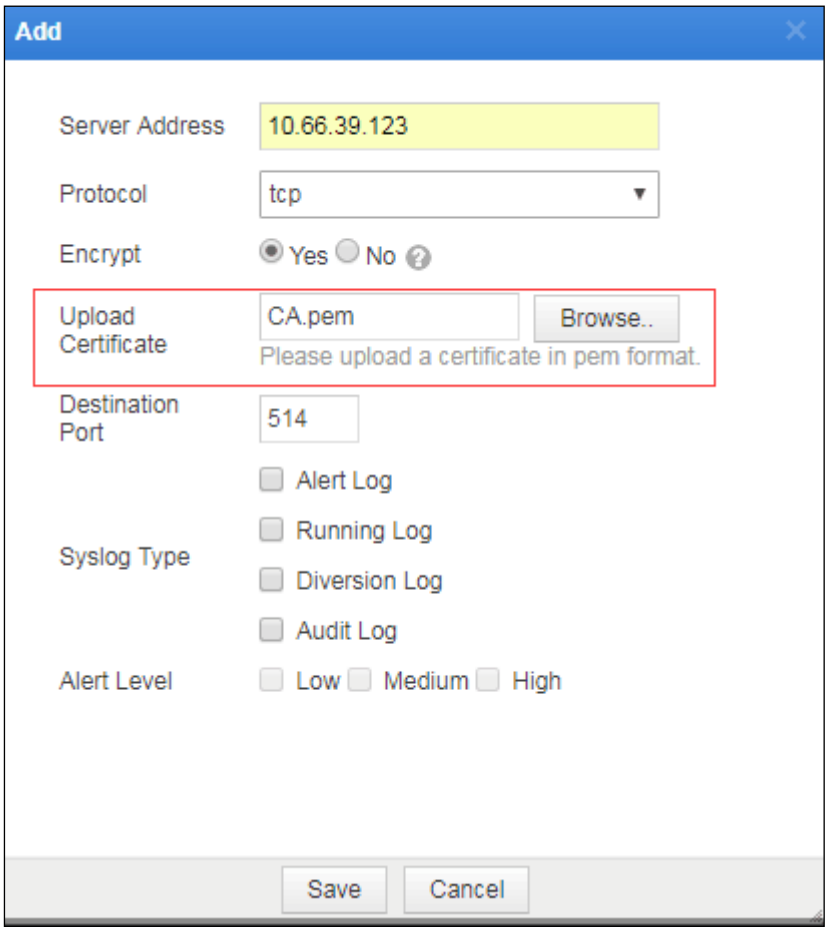
For an extranet, data in transit may be intercepted or tampered with. Therefore, it is necessary to encrypt data so that it can be sent through secure connections. Use of the Transport Layer Security (TLS) protocol can secure authentication and have data encrypted, thus ensuring the integrity of data.

Configuration and Use

Under **Administration > Third-Party Interface > Syslog Service**, in the **Add** dialog box, when **tcp** is selected for **Protocol**, an **Encrypt** field is added for users to choose whether to enable encryption.



After selecting **Yes** for **Encrypt**, users need to further select a server certificate and then import it.



Note that a server certificate can be imported only when it is in .pem format.

After the preceding configuration, NTA will send syslog messages to this server in an encrypted manner to ensure the security of data.

6. Fixed Bugs

Bug ID	Description
131487	The device is found to contain an HTTP Host header attack vulnerability during scanning by WVSS.
131059	When an alert ends 59 seconds after it is generated, no SNMP trap message (indicated with an OID) indicating the end of such alert is sent.
131418	Although configured to generate alerts based on either the number of packets or the number of bytes, NTA generates alerts only when both numbers are exceeded.
131771	In the case of massive traffic, the number of bytes counted in a PDU will exceed 32 bits. This will result in inaccurate traffic calculation.