Release Notes

1. Basic Information

Product Model	NTA NX3-2000E/1000E
Software Version	V4.5R90F00SP03
Upgrade File	update_nta_V4.5R90F00SP03.180428build26719.bin MD5: 9EB610D0309DE32602F52991A9224698
Release Date	2018-05-02
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	V4.5R90F00SP02
ADS	• V4.5.88.15 • V4.5R90F00SP02
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	The data dictionary of autonomous systems (ASs) should be updated.

No.	Requirement Description
2	The alert start time should be consistent.
3	The maximum number of source IP addresses allowed in alert details should be improved.
4	Some bugs should be fixed.

4. Upgrade Procedure

The source version for the upgrade must be V4.5R90F00, V4.5R90F00SP01, or V4.5R90F00SP02.

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 **update_nta_V4.5R90F00SP03.180428build26719.bin** file and then click **Upload**.

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

Step 4 Wait about 5 minutes and then refresh 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 **V4.5R90F00SP03**, the upgrade succeeded. If not, the upgrade failed and you need to contact NSFOCUS technical support.

----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.
4. The installation takes about 5 minutes. Later, you need to manually refresh the page.

Note that the system will automatically restart after the installation is complete.

5. Function Changes

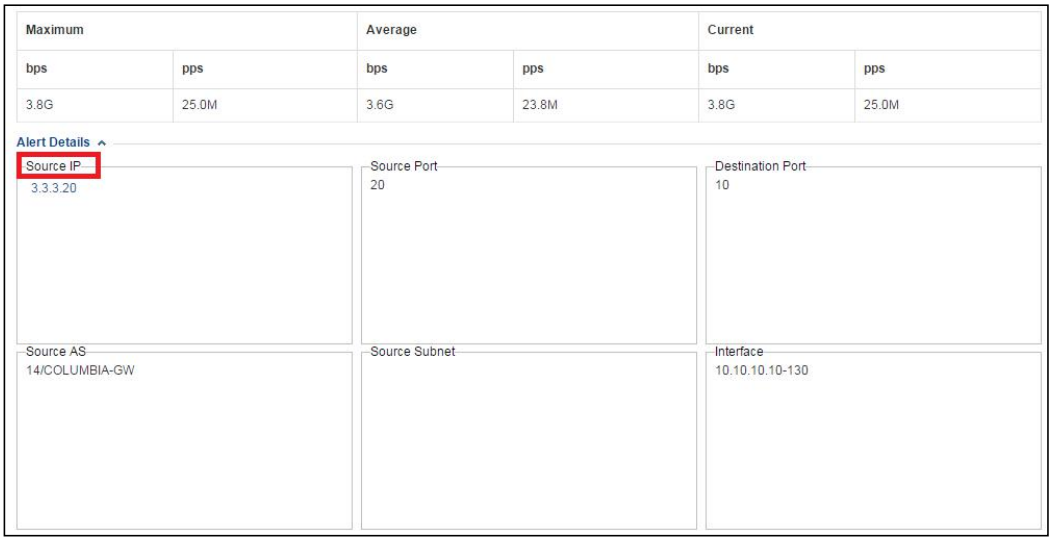
5.1 Making the Alert Start Time Consistent

On the alert list, the start time indicates the point of time when an alert is generated upon completion of the latency period. However, the traffic graph provided in alert details displays traffic from when the latency period starts. This leads to inconsistency between the two times.

To ensure consistency, the start time on the alert list is changed to the time when the latency period starts.

5.2 Improving the Maximum Number of Source IP Addresses Allowed in Alert Details

The maximum number of source IP addresses allowed in alert details is improved from 200 to 500.



6. Fixed Bugs

Bug ID	Bug Description
136091	Source and destination ports provided in icmp_sflow statistics are incorrect.
135760	The same alert is generated again in the diversion holding period, resulting in redundant diversion logs.
135706	The device crashes after loading the SP01 package.
135387	An error message is displayed for statistics query based on IP segments.
135006	During cloud-side authentication, after device information is sent, two dev_status_proc.py processes are launched.
134755	A message prompting failure to connect to the configuration manager is displayed in response to requests for canceling auto-learning.
133667	Some alerts cannot be successfully retrieved if routers are selected as one of the filtering conditions.
133994	Filtering conditions for abnormal region/IP group-specific traffic alerts are improperly displayed.
132613	After a region is deleted upon generation of an alert, the region name is incorrectly displayed in the DDoS attack report.
132534	After a region is deleted, information related to this region is displayed in HTML format on the web-based manager.
124253	After the auto-learning engine is restarted, the adjustment multiple set under the time policy cannot take effect until the next cycle (specified with **Time Granularity** in **Advanced Settings**) starts.

Bug ID	Bug Description
137210	After regions are deleted in batches and then added again, they cannot be identified according to the auto-learning baseline parameters.
135186	If a region has more than one IP group, after a user modifies its settings and attempts to commit the changes, he or she has to wait a longer time than usual and ends up with a message prompting failure to connect to the configuration manager.

7. Compatibility

- Browser: Chrome, Firefox, and Internet Explorer 10, with the former two recommended
- ADS: V4.5R90F00SP02 and V4.5.88.15
- ADS M: V4.5R90F00SP02
- TAT: V2.0.0