Release Notes

1. Basic Information

Device Model	NTA NX3-2000E/1000E
Software Version	V4.5R90F01SP02
Upgrade File	update_nta_V4.5R90F01SP02.190225build30068.bin md5: 8cbc60ffbc339b47dedf38602fa71722
Release Date	2019-02-25
How to Obtain	Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support.

2. Version Mapping

Product Model	NTA NX3-2000E/1000E (NSF-2800)
ADS	• V4.5.88.15 • V4.5R90F01 • V4.5R90F01SP01 • V4.5R90F01SP02 • V4.5R90F01SP03
ADS M	V4.5R90F01SP03
NTA-ATM	V4.5R89F03
Threat Analysis and Traceback System (TAT)	V2.0.0
Client Browser	• Chrome • Firefox • IE 10
Documentation	NSFOCUS NTA Installation Guide/User Guide (V4.5R90F01)

3. Satisfied Requirements

No.	Requirement Description
1	New support for sending of SNMP notification-type data
2	Inclusion of custom alerts when displaying top 5 DDoS attack alerts
3	Inclusion of custom alerts when displaying ongoing alerts
4	New support for sending of real-time data to ATM
5	Addition of three options (20k, 40k, and 50k flows/s) in vNTA licenses
6	New support for access control
7	Support by the license for the display of IPv6 authorization
8	Secondary encryption for upgrade packages of vNTA
9	Support for automatic FlowSpec diversion
10	Display of the cloud platform connection status
11	Change of the retention period of traffic trend data in alert details to six months

4. New Functions

4.1 New Support for Sending of SNMP notification-type Data

The SNMP notification type is a data type newly added in SNMPv2. For details, see RFC 2576. The SNMP notification type contains a number of object types and data of those types can be combined arbitrarily. Arguably, this data type is equivalent to a view.

This upgrade package supports the sending of data of the SNMP notification type.

4.2 Inclusion of Custom Alerts When Displaying Top 5 DDoS Attack Alerts

On the **Overview** page under **Monitor**, custom alerts are also included in statistics for top 5 DDoS alerts.

4.3 Inclusion of Custom Alerts When Displaying Ongoing Alerts

On the **Regions** page under **Monitor**, you can click a specific region to open its details page on which custom alerts are included in statistics of ongoing alerts.

4.4 New Support for Sending of Real-Time Data to ATM

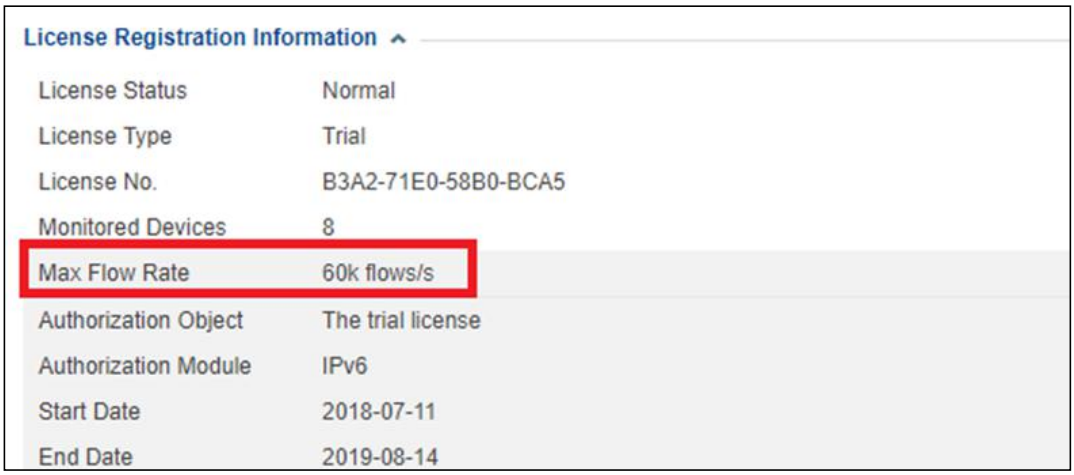
NTA can send real-time alert data to ATM which must be V4.5R89F03 or later.

Choose **Administration > Third-Party Interface > NTA-ATM**, select **Real-time** for **Synchronization Mode**, and configure ATM-related parameters: Set **NTA-ATM Address 1**, **2**, or **3** to the IP address of ATM, **File Port** to **80**, **Log Port** to **1111**, and **translocalhost** to **127.0.0.1** for an NAT environment or to the IP address of ATM for a non-NAT environment.

With this function, NTA can read alerts and traffic information from the real-time database and send them to ATM through the A interface. Alerts are transmitted every 20 seconds and traffic information is sent every 30 seconds.

4.5 Addition of Three Options (20k, 40k, and 50k flows/s) in vNTA Licenses

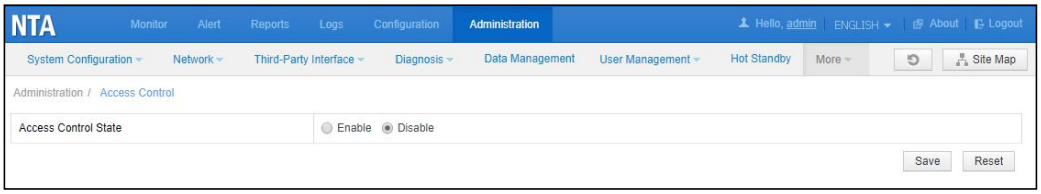
You can view the flow upperlimit supported by the license on the **License** page under **Administration**.



If the actual number of flows exceeds the specified upperlimit, excessive ones will be dropped.

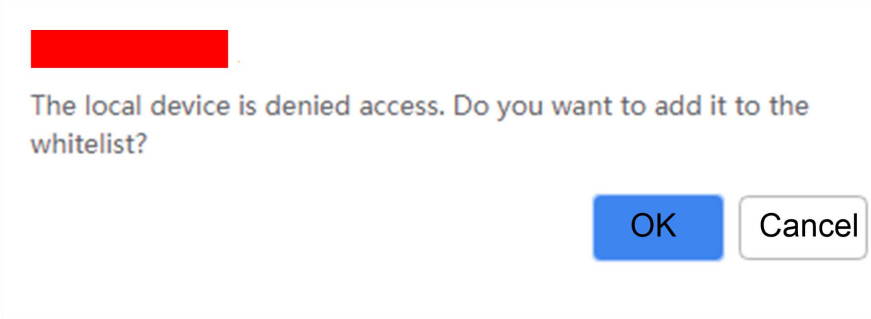
4.6 New Support for Access Control

The access control function can be configured on the **Access Control** page under **Administration**. This function is implemented with iptables and disabled by default. A maximum of 10 access control rules can be specified.

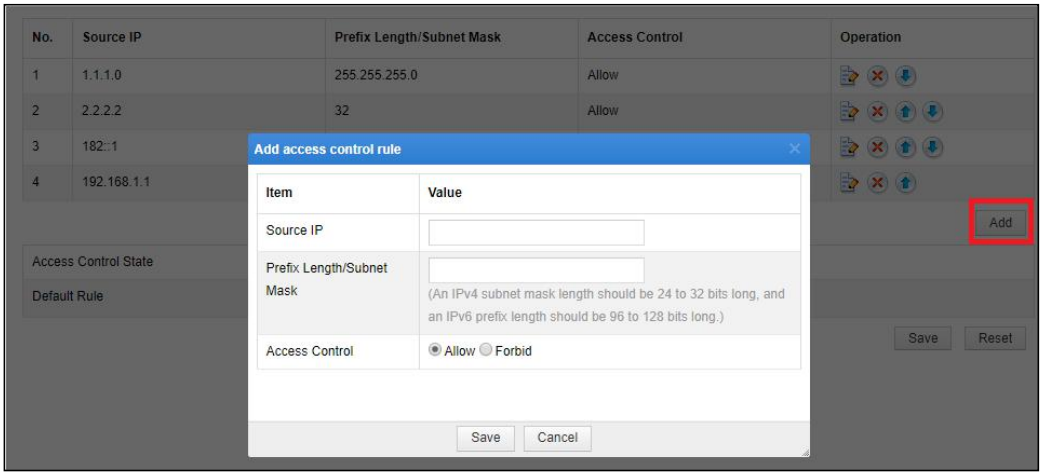


You can select **Enable** for **Access Control State** to enable the access control function.

For **Default Rule**, For **Default Rule**, if **Allow external access** is selected, any IP address can access NTA by default. In this case, access control rules configured by users function as blacklists. If **Deny external access** is selected, all IP addresses are denied access to NTA by default. At this time, access control rules configured by users function as blacklists. After the configuration is completed, click **Save** to enable the access control function. **It is important to note that if Default Rule is set to Deny external access, the system will ask you whether to add the IP address of the local host to the whitelist and you need to click OK in the dialog box, or the local host cannot access NTA**.



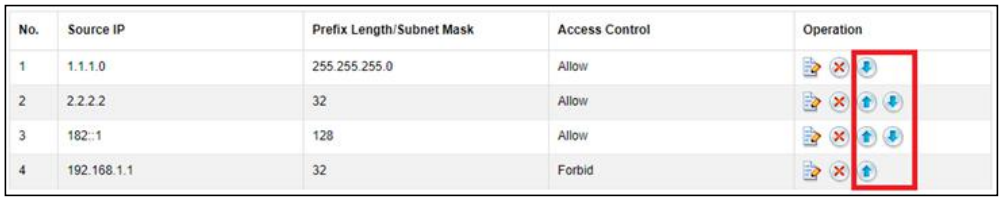
Click **Add** to create an access control rule.



Source IP supports both IPv4 and IPv6 addresses. For an IPv4 address, **Prefix Length/Subnet Mask** can be set to either the subnet mask (such as 255.255.255.0) or mask length (such as 24); for an IPv6 address, **Prefix Length/Subnet Mask** can only be set to a number representing the prefix length.

Access control rules are listed in the chronological order and **the system checks packets against them in a top-down manner**. You can click or in the **Operation** column to move a rule up or down.

No.	Source IP	Prefix Length/Subnet Mask	Access Control	Operation
1	1.1.1.0	255.255.255.0	Allow	
2	2.2.2.2	32	Allow	
3	182::1	128	Allow	
4	192.168.1.1	32	Forbid	



Also, you can click  or  in the **Operation** column to edit or delete a rule.

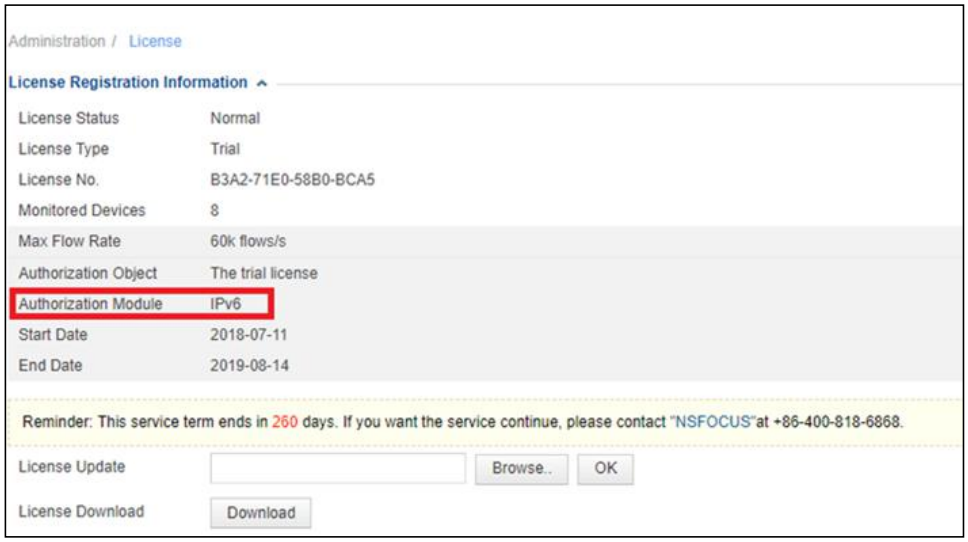
In the command-line window, you can run the **iptables show** command to view the current access control list:

```
NTA# iptables show
ACCEPT     all  --  1.1.1.0/24          0.0.0.0/0
ACCEPT     all  --  2.2.2.2             0.0.0.0/0
DROP       all  --  192.168.1.1         0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0           0.0.0.0/0
ACCEPT     all      182::1              ::/0
ACCEPT     all      ::/0                ::/0
```

In addition, you can run the **iptables on** or **iptables off** command to enable or disable the access control function.

4.7 Support by the License for the Display of IPv6 Authorization

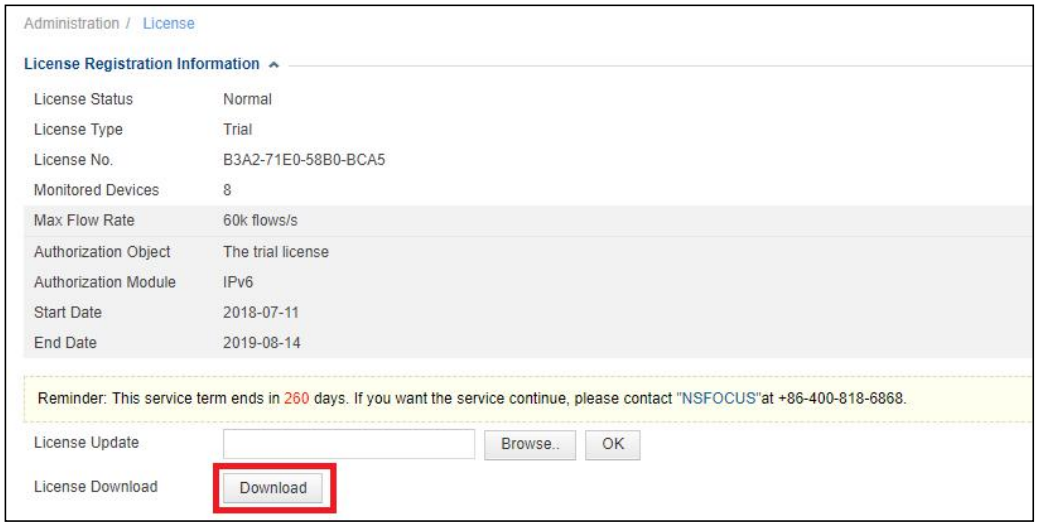
On the **License** page under **Administration**, you can see that the IPv6 authorization module is added to the license.



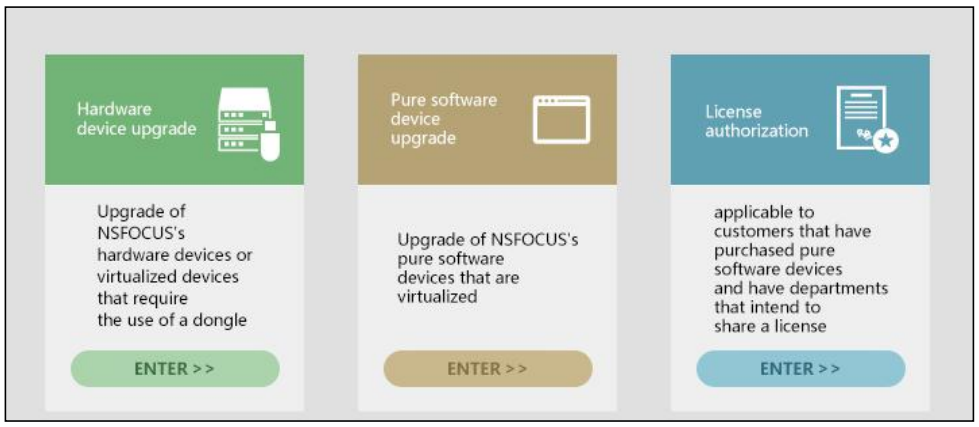
4.8 Secondary Encryption for Upgrade Packages of vNTA

This function is available only to vNTA. vNTA V4.5R90F01SP01 and later can be upgraded only by installing an upgrade package with secondary encryption.

Choose **Administration > License** and click **Download** to download the license to a local disk drive.



Then visit http://update.nsfocus.com/ and select **Pure software device upgrade** and click **ENTER**.



Browse to the license downloaded just now and click **Upload**. On the page that appears, click **NTA**, select the appropriate version to download the upgrade package with secondary encryption. Such upgrade package can only be used for the upgrade of vNTA.

Upgrade packages with secondary encryption downloaded using the same license can only be used for upgrade for the device which the license matches.

Physical devices are upgraded in the same way as previous versions.

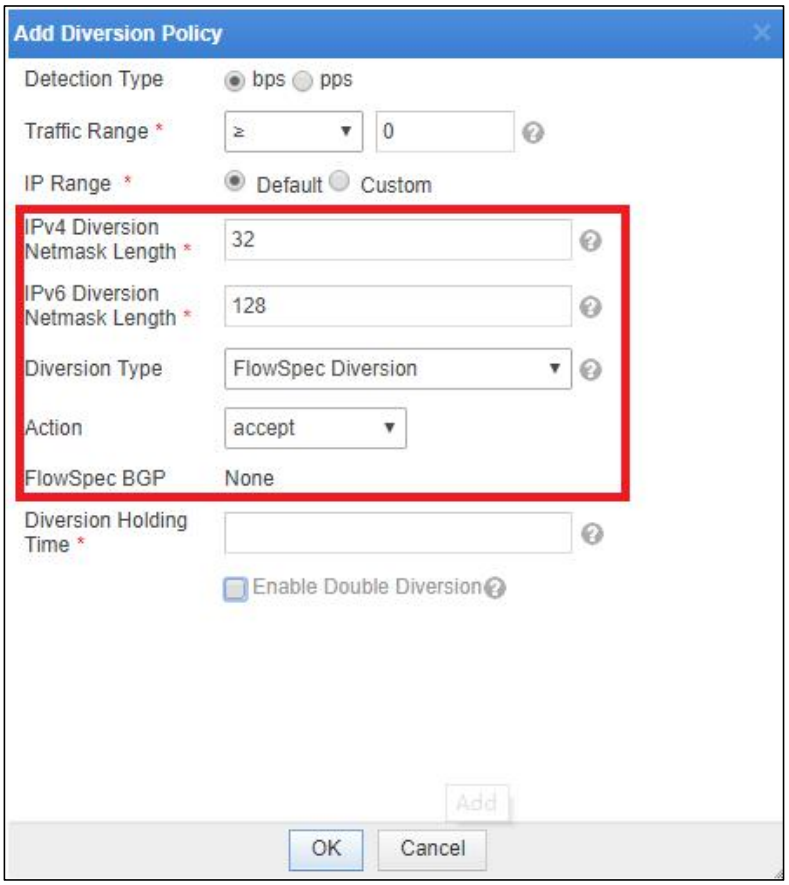
The following table lists the mapping between physical and virtual devices and upgrade package types.

Upgrade Package Type	Device Type	Update Result
Common upgrade package	Physical	Normal upgrade
	Virtual	An error occurs. An upgrade package with secondary encryption must be applied.
Upgrade package with secondary encryption	Physical	An error occurs. A common upgrade package must be applied.
	Virtual	Normal upgrade

4.9 Support for Automatic FlowSpec Diversion

FlowSpec diversion can now be performed automatically, but related rules can be configured only by specifying destination IP addresses and subnet masks. Besides, such diversion works only for DDoS alerts and does not respond to abnormal region traffic alerts.

Automatic FlowSpec diversion can be configured in the following dialog box under **Configuration > Global Divert Settings > IP Diversion Policy**, **Regions >** *Region* **> Traffic Diversion Rule > IP Diversion Policy**, and **Regions >** *Region* **>** *IP Group* **> Traffic Diversion Rule > IP Diversion Policy**.



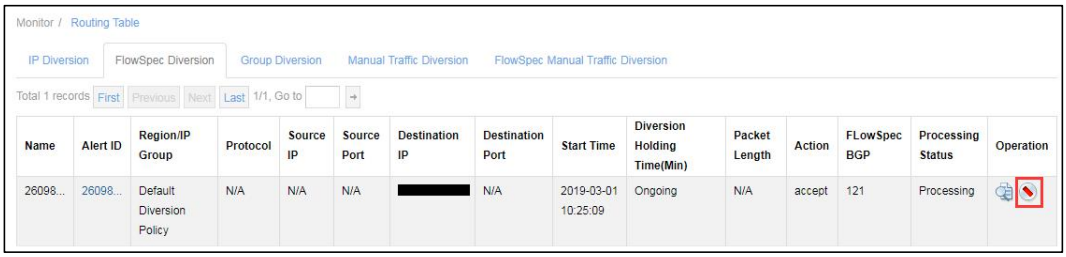
- **IPv4 Diversion Netmask Length**: specifies the subnet mask length for IPv4 addresses. This parameter controls the routes to be sent by NTA. For example, the value **32** indicates that NTA sends only one host route for diversion; the value **24** indicates that NTA sends a /24 IP address for diversion. The recommended value is **32**.
- **IPv6 Diversion Netmask Length**: specifies the subnet mask length for IPv6 addresses. The recommended value is **128**.
- **Action**: specifies one of the following actions to be taken by the router.

Action	Description	Value Description
rate_limit	Limits the traffic rate.	Traffic rate in bps
redirect	Redirects traffic.	VRF or IP address
mark	Marks traffic.	Value range: 0–63
accept	Allows traffic to pass.	None
discard	Drops traffic.	None

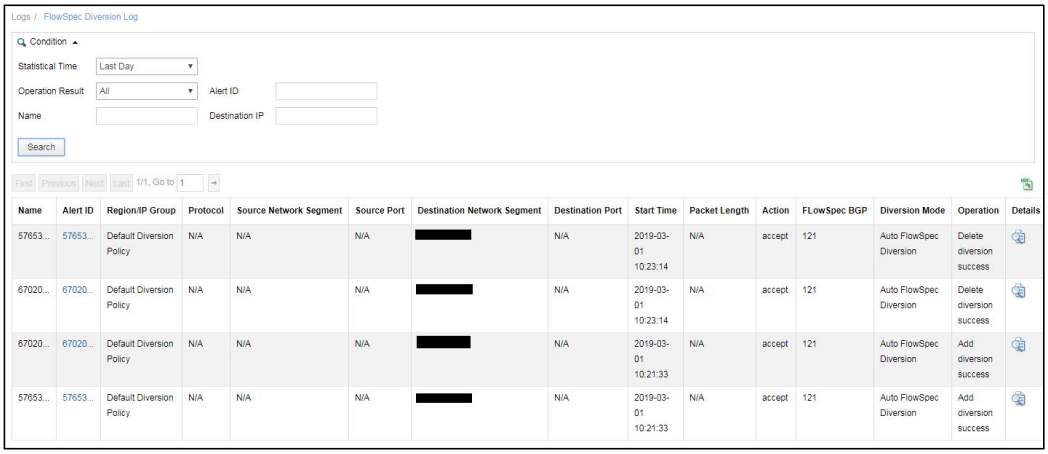
FlowSpec BGP: selects a BGP session from the drop-down list. BGP sessions can be configured under **Configuration > Global Divert Settings > FlowSpec BGP**.

Double diversion is supported. In this case, different BGP sessions must be specified.

A FlowSpec diversion rule, after being committed, is listed under **Monitor > Routing Table > FlowSpec Diversion** and can be revoked.



To view FlowSpec diversion logs, choose **Logs > FlowSpec Diversion Log**.



4.10 Display of the Cloud Platform Connection Status

After the address of NSFOCUS Cloud is configured under **Administration > Third-Party Interface > Cloud Platform**, NTA will test whether the address is reachable in the background and then display the status with an indicator on the right of the related text box.

If NTA can connect to this address, a green indicator appears.

Conversely, if NTA cannot connect to this address, a red indicator appears.

After an address is added and saved, the system immediately starts to test the connectivity and then displays the status. For addresses already configured, their connectivity status is refreshed every 10 seconds.

4.11 Change of the Retention Period of Traffic Trend Data in Alert Details to Six Months

The traffic trend graph on the **Alert Details** page can display traffic data of the past six months. But note that this function interacts with the data management function (**Administration > Data Management**). That is to say, if the data accumulated in less than six months uses more space than allowed under **Administration > Data Management**, the data will be cleared.

5. Fixed Bugs

- Bug 141843: When there are too many source IP addresses, reports fail to be exported.
- Bug 120290: As the system root directory disappears and cannot be mounted, the system reports the "NSF file handle" error.
- Bug 144582: When an NTP server is configured with an IPv6 address, time synchronization fails.
- Bug 145188: A third-party cloud platform with an IPv6 address cannot send data due to the lack of the -g parameter during the invocation of cURL.
- Bug 145194: The login password cannot be changed when users edit personal information.
- Bug 145104: On the Data Management page, partition clearing is described in Chinese.
- Bug 145135: A DNS V6 server, once configured, cannot resolve domain names.
- Bug 145195: The NTI API Description document needs to be modified.
- Bug 144690: When there is traffic on multiple routers at a specific time point, only the traffic on one router is displayed on graphs in the Top Routers area on the Routers page under Monitor.
- Bug 145205: When users keep refreshing the current page on the web-based manager, the system exception error flashes past the page.
- Bug 145216: No attack direction is indicated for custom alerts on the alarm list on the Overview page under Alert.
- Bug 145218: No port is indicated in details of the TCP/UDP fragment alert plug-in on the Global Alert Settings page under Configuration.
- Bug 145401: On the Flow Settings page under Configuration, when Global Flow Forwarding is set to Close, the settings in the Forward Host List box will disappear.
- Bug 149561 [NX3-VM.001] [R90F01] During the license import, the system prompts "Failed to import cloud-side license. Cause: incorrect license format."
- Bug 149089 [Collaboration with ADS] After diversion holding time is configured, diversion notifications issued by NTA to ADS contain incorrect IP addresses.
- Bug 150222 [Reports] Router traffic reports contain incorrect data.
- Bug 149687 [GUI] The visual display of disk partition sizes for data management is inconsistent with values on the x-axis.

- Bug 149685 [GUI] In the case of no traffic details, users are incorrectly prompted.
- Bug 149682 [Traffic detector] Signatures for DNS query flood detection are incorrect.
- Bug 149677 [Other functions] NTA restarts unexpectedly.
- Bug 146633 [Traffic collector] PDUs of MPLS are incorrectly parsed.
- Bug 150726 [Vulnerability test] NTA contains an HttpOnly vulnerability.
- Bug 150817 [Device collaboration] Names of regions or IP groups dispatched by ADS M can be changed on NTA.
- Bug 147594 [NTA R90F00SP03] There is no data about the FlowSpec BGP neighbor status when NTA works in HA mode.
- Bug 132613 [DDoS attack report] If a region, which is involved in an alert, is deleted, its name is incorrectly displayed in the DDoS attack report.

6. Upgrade Procedure

Note: You must upgrade in strict accordance with the upgrade path.

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 update_nta_V4.5R90F01SP02.190225build30068.bin and click Upload.

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

Step 3 Wait 5 minutes for the installation to complete before refreshing the current page. Click **About** in the upper-right corner of the web-based manager to check the current system version. If **Product Version** is **V4.5R90F01SP02.190225build30068**, 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:

- The web-based manager displays an error message "502 Bad Gateway" or directly denies your access request.
- All services will stop running.
- The upgrade takes about 5 minutes. If the page remains unresponsive after 5 minutes, you need to manually refresh the page.

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

7. Upgrade Path