Release Notes

1. Basic Information

Product Model	NTA NX3-2000E/1000E/HD2100/HD2200 NTA VM
Software Version	V4.5R90F02SP02
Upgrade File	update_nta_V4.5R90F02SP02.200806build39743.bin 046dfa890360dc0b968729be5710c083
Release Date	2020-08-07
How to Obtain	Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support.

2. Version Mapping

Hardware Model	NTA NX3-2000E/1000E (NSF-2800) NTA NX3-HD2100/HD2200 (C236)
ADS	V4.5R90F02 V4.5R90F02SP01 V4.5R90F02SP02
ADSM	V4.5R90F02SP02
NTA-ATM	V4.5R89F03
Threat Analysis Traceback (TAT)	V2.0.0
Client Browser	Chrome Firefox
Documentation	None

3. New Requirements

No.	Requirement Description
1	The number of auto-learned IP groups should be increased to 500.
2	BGP diversion should be available for abnormal inbound or outbound traffic of a region or IP group.
3	The format of data sent via SFTP needs to be optimized.
4	Manual traffic diversion should resume upon an engine/device recovery from an exception.
5	Manual traffic diversion should resume upon a high availability (HA) switchover.

4. New Functions

4.1 The Number of Auto-learned IP Groups Increased to 500

Description

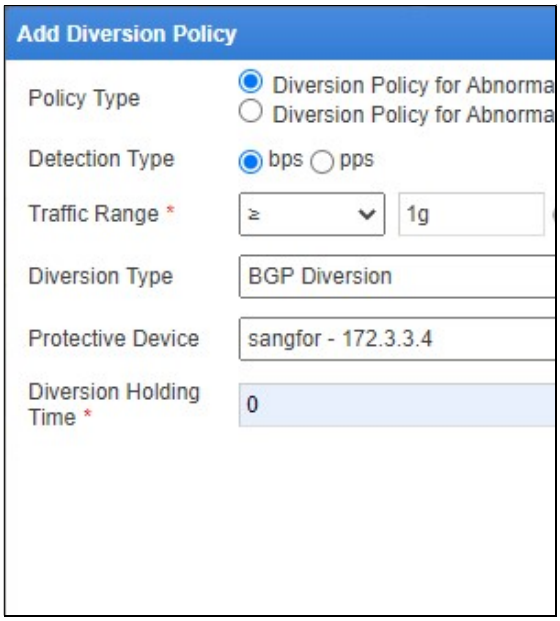
In earlier versions, the auto-learning engine, due to limited performance, can only support a maximum of 150 "Learning" and "Applied" IP groups. The V4.5R90F02SP02 version optimizes the auto-learning engine, increasing such figure to 500 (when the time granularity is 60 minutes).

4.2 BGP Diversion Available for Abnormal Inbound or Outbound Traffic of a Region or IP Group

Description

As for traffic diversion, in V4.5R90F02SP01 and earlier versions, only null route diversion is available for abnormal inbound or outbound traffic of a region or IP group. V4.5R90F02SP02 adds BGP diversion, allowing abnormal inbound or outbound traffic to be diverted to a cloud cleaning center or a third-party device.

Configuration and Use



4.3 Optimization of the Format of Data Sent via SFTP

Description

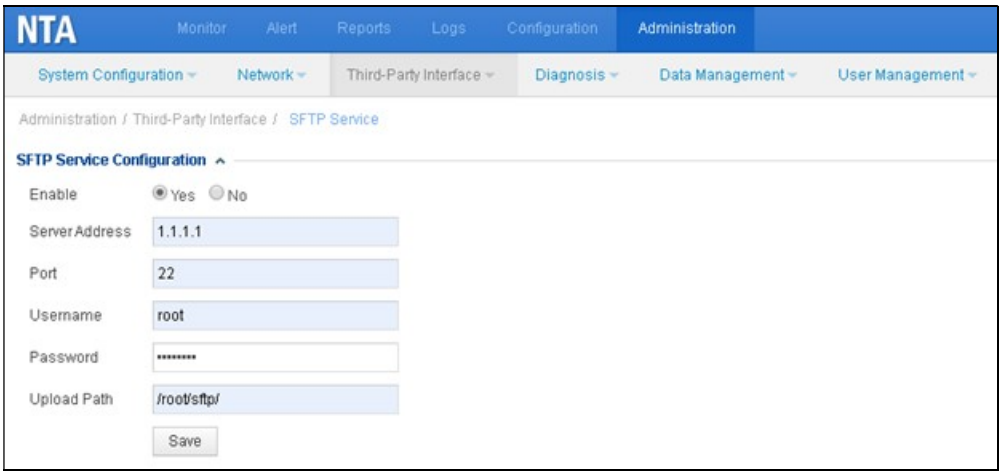
V4.5R90F02SP02 modifies the fields of data sent via SFTP:

- The sending of state_bgp data is canceled.
- The val is changed from <2000> to <9999> when the NTA license is invalid.
- state_traffic is modified to verify whether there is traffic over ports that are up. When there is traffic over each port that is up, val is <0> and msg is <Traffic on ports: normal>. When a port that is up (for example port M) has no traffic, val is <1> and msg is <No traffic on port M>.
- state_port is changed to define the port state according to the port state change within 1 minute (for example, port M turns to DOWN from UP). A port is deemed normal if its state remains unchanged in such period. Otherwise, its state is abnormal. Normal: val is <0> and msg is <Status of all ports remains unchanged>. Abnormal: val is <1> and msg is <Port M turns DOWN from UP>.
- state_proces is added to monitor the states of NTA's key processes (nginx, ttserver, postgres, memcached, and webservice) and record abnormal processes. When all processes are normal, val is <0> and msg is <Process normal>. When some processes (for instance

nginx and webservice) are abnormal, val is <1> and msg is <nginx abnormal, webservice abnormal>. Note: When database postgres is abnormal, state_proces val is <1> and state_port and log_alert that are derived from the database are not sent. When database postgres is normal but connections exceed 100, state_proces val is <0> and state_port and log_alert that are derived from the database are not sent.

Configuration and Use

Choose **Administration > Third-Party Interface > SFTP Service**.



4.4 Resumption of Manual Traffic Diversion upon an Engine/Device Recovery from an Exception

Description

Users under attacks might divert and clean traffic of a specific IP address via manual traffic diversion. When the abnormal diversion engine or device is restarted, manual traffic diversion cannot resume automatically, failing to produce the intended diversion effect.

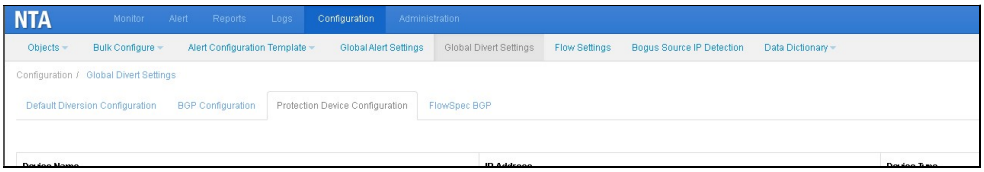
- Manual traffic diversion resumes upon an engine/device recovery from an exception.
- Manual FlowSpec diversion can resume upon an engine/device recovery from an exception.

Configuration and Use

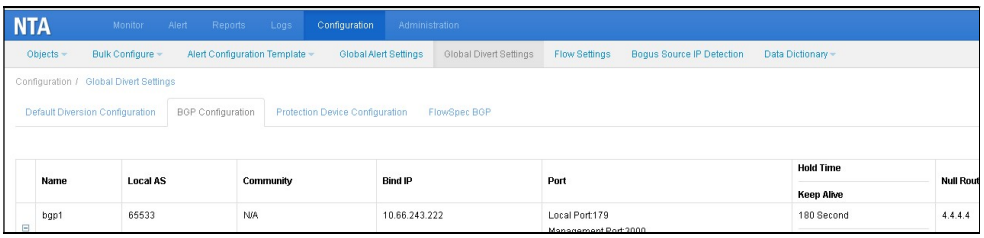
Manual Traffic Diversion

Manual traffic diversion includes ADS diversion, BGP diversion, and null route diversion. BGP diversion configurations include BGP configuration and manual diversion configuration. Null route diversion configurations includes protection device configuration, BGP configuration, and manual diversion configuration. ADS diversion configurations include protection device configuration and manual diversion configuration.

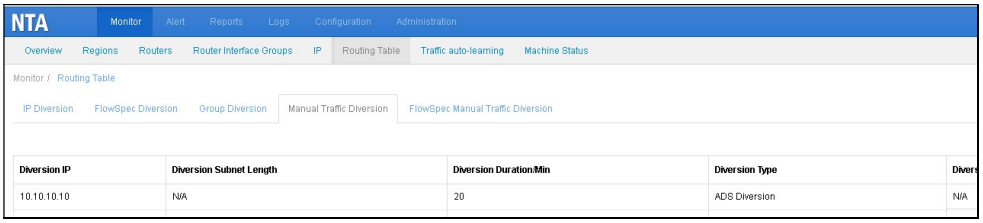
- Protection device configuration: **Choose Configuration > Global Divert Settings > Protection Device Configuration**.



- BGP configuration: Choose **Configuration > Global Divert Settings > BGP Configuration**.



- Manual diversion configuration: Choose **Monitor > Routing Table > Manual Traffic Diversion**.



- Click  in the **Operation** column to dispatch manual diversion. You can view THE diversion status by choosing **Monitor > Routing Table > IP Diversion**.

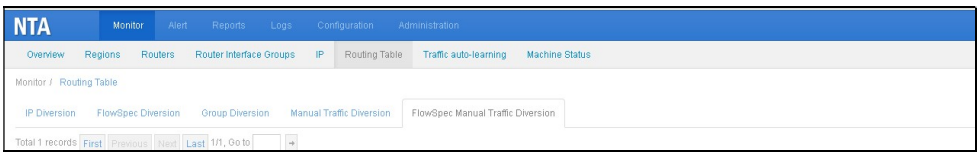
Manual FlowSpec Diversion

- Configure FlowSpec BGP

  Add FlowSpec BGP by choosing **Configuration > Global Divert Settings > FlowSpec BGP**.

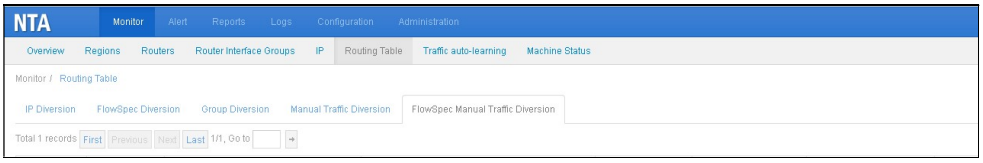
- Configure a rule for manual FlowSpec diversion

  Add a rule for manual FlowSpec diversion by choosing **Monitor > Routing Table > FlowSpec Manual Traffic Diversion**.

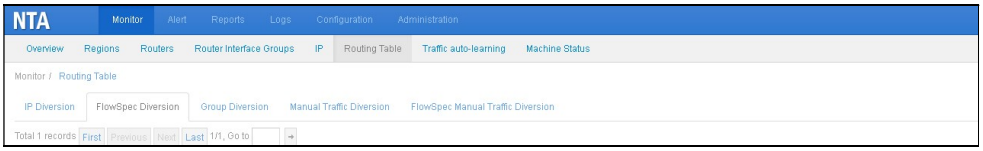


- Dispatch manual FlowSpec diversion

Click in the **Operation** column to dispatch manual FlowSpec diversion.



- View the status of manual FlowSpec diversion by choosing **Monitor > Routing Table > FlowSpec Diversion**.



4.5 Resumption of Manual Traffic Diversion Upon a HA Switchover

Description

Users under attacks might divert and clean traffic of a specific IP address via manual traffic diversion. When the abnormal device triggers a HA switchover, the backup device should resume diversion so as to ensure that the attack traffic is diverted and cleaned.

- Manual traffic diversion that is disrupted by the HA switchover can be resumed.
- Manual FlowSpec diversion that is disrupted by the HA switchover can be resumed.

Configuration and Use

First configure an HA environment by choosing **Administration > Hot Standby**, and then configure manual diversion on the host (see section 4.4). When an HA switchover occurs, you can view the diversion status on the new host (see section 4.4).

5. Fixed Bugs

- Bug 176412: [NTA generality - router] The CPU usage and memory usage of the device cannot be obtained at some points of time.
- Bug 178498: [NTA generality - SFTP] val of the state_traffic field is incorrect.
- Bug 176247: [NTA generality - NTA supports DPI detection — Reports/Monitor] Even if the traffic is stable, a traffic jump is observed in router traffic monitoring statistics, reports, and router interface traffic statistics.
- Bug 176524: [NTA generality - NTA supports DPI detection — Monitor] When Cisco routers are configured, a traffic leap is observed during the switching from SNMPv3 to SNMPv1.
- Bug 177282: [NTA generality - NTA supports DPI detection — Monitor] Sometimes, the error "nginx bad gateway" occurs on the web.
- Bug 180313: [System management] engine-keeper cannot enable webservice which does not operate.

- Bug 180307: [Traffic collector - netflow] After IPv4 addresses are configured on the forwarding list, Netflow flows fail to be sent to IPv6 addresses on the list.
- Bug 170265: [Third-party interface] When ADS M collaborating with NTA gets offline, sendlog-to-adsm.py takes up all CPU resources.
- Bug 176706: Regions cannot be configured.
- Bug 175803: In active/standby mode, both devices are active.
- Bug 181906: [Others] Clearing serial port configurations causes processes concerning flow_spec to fail.
- Bug 179591: [Real-time database – merge] In a stressing environment, data loss is seen in top n alert statistics.
- Bug 179297: [Third-party interface - ADS M collaborating with NTA] Data statistics collected every 60 seconds, when sent to ADS M, might be missing partly.
- Bug 177444: The data transmission from NTA to ADS M is frozen.
- Bug 172488: FlowSpec diversion does not work.
- Bug 175827: No alerts are generated when the alert threshold is reached.

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_V4.5R90F02SP02.200806build39743.bin** and click **Upload**.

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

The upgrade takes about 5 minutes.

Step 4 After the upgrade is complete, refresh 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 **V4.5R90F02SP02.200806build39743**, the upgrade succeeded. If not, the upgrade failed and you need to contact NSFOCUS technical support.

It is normal that the following situations arise during upgrade:

- The web-based manager displays an error message "502 Bad Gateway" for or directly denies your access request.
- All services 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