Release Notes

Basic Information

Product Model	NTA NX3-2000E/1000E
Software Version	V4.5R89F03SP01
Upgrade File	update_nta_V4.5R89F03SP01.170811build24724.bin MD5: 6871C530BD154438840D36DC66EB1EEB
Release Date	2017-08-15
How to Obtain	Obtain the upgrade file from the upgrade system or contact technical support personnel of NSFOCUS.

Version Mapping

Product Model	NTA NX3-2000E/1000E (NSF-2800)
ADS M	ADS M V4.5R89F03SP01
ADS	ADS V4.5.88.15/V4.5R89F03SP01
Threat Analysis and Traceback System (TAT)	TAT V2.0.0
Client Browser	• Chrome • Firefox • IE 10
Documentation	NSFOCUS NTA Installation Guide/User Guide (V4.5R89F03)

Satisfied Requirements

No.	Requirement Description
1	The HA function supports configuration of both IPv4 and IPv6 addresses for the same interface and inclusion of the two types of IP addresses in two different VRRP groups.

No.	Requirement Description
2	The source and destination port can be set to 0 in custom alert configuration.
3	DNS parsing is optimized for cloud-side authentication.
4	For top 5 DDoS alerts, destination IP addresses and router interfaces are added.
5	A vulnerability related to the Linux kernel is fixed.
6	Some bugs are fixed.

Upgrade Procedure

The source version for the upgrade must be V4.5R89F03.

Perform the following steps to upgrade the software:

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_V4.5R89F03SP01.170811build24724.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 **V4.5R89F03SP01**, 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:

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

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.

Function Changes

(1) HA Function Supporting Configuration of Both IPv4 and IPv6 Addresses for the Same Interface and Inclusion of the Two Types of IP Addresses in Two Different VRRP Groups

Scenario

A typical scenario is that both IPv4 and IPv6 addresses are configured for the management interface and included in two different VRRP groups to implement the HA function.

Configuration and Use

Under **Administration > Hot Standby**, configure an IPv4 address and an IPv6 address for the same interface and then add them to two different VRRP groups.

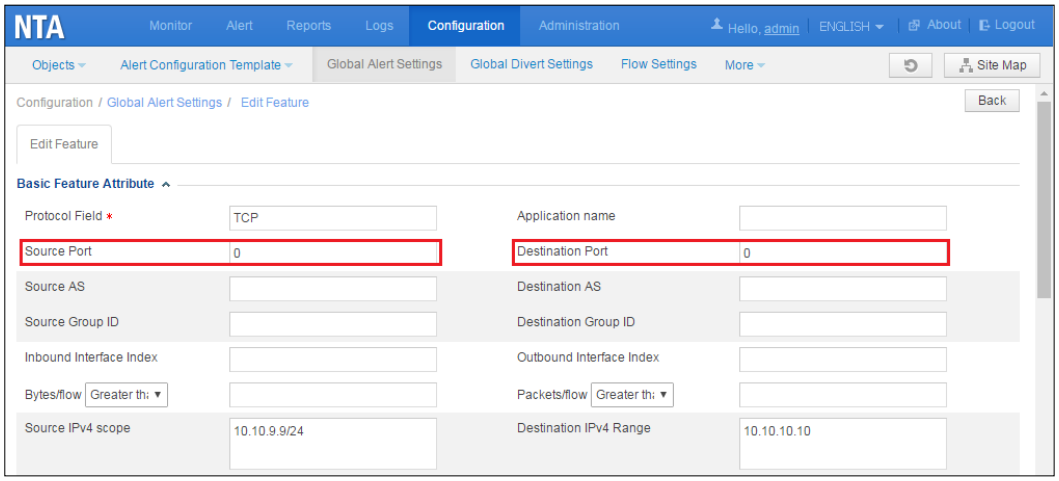
(2) Source/Destination Port Allowed to Be 0 in Custom Alert Configuration

Scenario

Detection of fragment attacks requires the source and destination ports to be able to be set to 0.

Configuration and Use

When configuring custom attack alerts under **Configuration > Global Alert Settings > Alert Plug-in Management**, users can set the source port and destination port to 0 so that NTA can detect fragment attacks.



(3) Optimization of DNS Parsing for Cloud-Side Authentication

Requirement Description

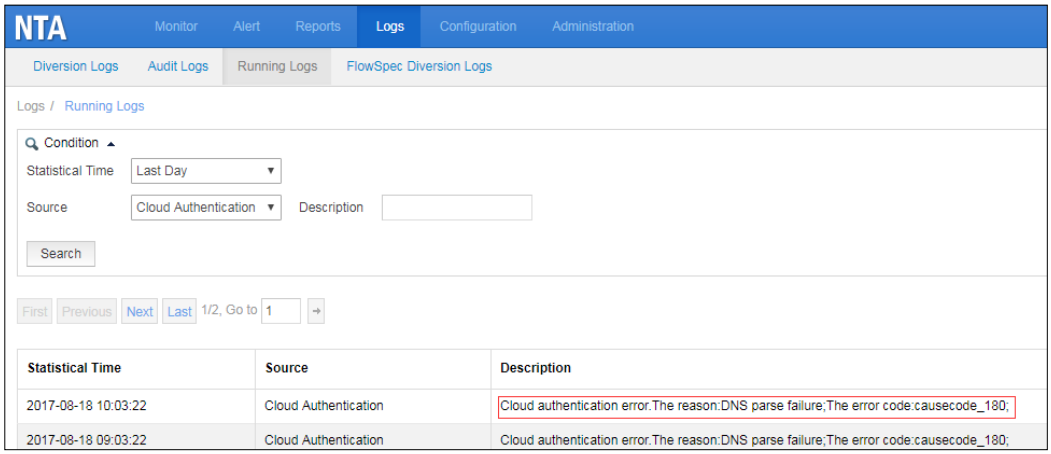
IP addresses of the cloud-side authentication server parsed by DNS are updated in the host file on an hourly basis. If DNS parsing fails, an entry of "DNS parse failure" will be added to the running log, with the source being "Cloud Authentication".

Scenario

DNS parsing failures do not affect the cloud-side authentication process, indicating that the IP address of the authentication server can be successfully obtained from the host file.

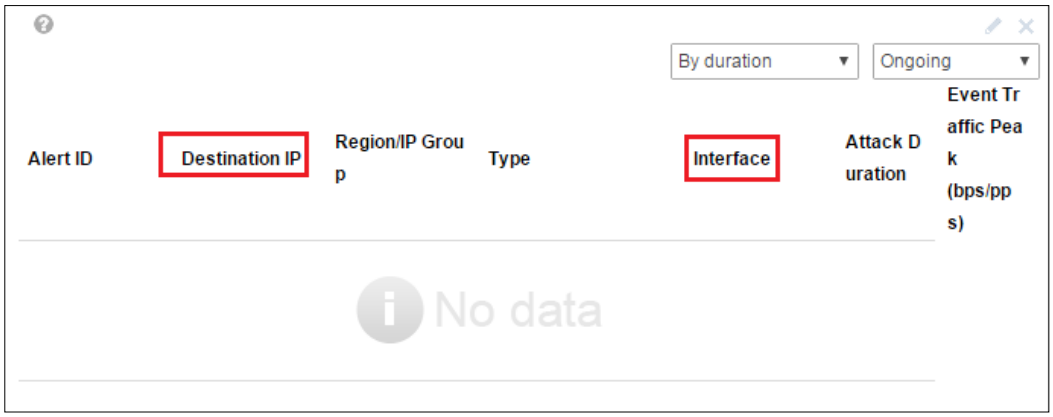
Configuration and Use

If the DNS server specified under **Administration > Network > DNS Server** cannot parse the domain name of the cloud-side authentication server, an entry will be added to the running log, indicating such failure.



(4) Destination IP Addresses and Router Interfaces Added for Top 5 DDoS Alerts

Under **Monitor > Overview**, two columns are added for top 5 DDoS alerts: **Destination IP** and **Interface**. The destination IP address can be either an IPv4 or IPv6 address.



Fixed Bugs

Bug 123045	Incorrect inbound/outbound interfaces of Huawei S7706 are provided in flow information.
Bug 123064	SNMP traffic cannot be obtained from Huawei S5700.
Bug 122636	The traffic value at the first point of time is inaccurate in attack statistics.