1 Basic Information

Product Model	NTA NX3-2000E/1000E
Software Version	V4.5R90F00
Upgrade File	update_nta_V4.5R90F00.171206build25517.bin (MD5: 775C567710250AA31219352757EE15B4)
Release Date	2017-12-29
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

Requirements Based on V4.5R89F03

No.	Requirement Description
1	Batch operations should be allowed on regions and IP groups.
2	A template should be applied to multiple regions or IP groups simultaneously.
3	Each diversion policy should be configured with a separate diversion hold time.
4	Different statistical modes need should be available for selection when the statistical interval for flows is 60 seconds.
5	For collaboration with a third-party cloud platform, file types to be sent should be selected, global DDoS alert data should be sent, and top 100 source IP addresses should be included in DDoS alerts.
6	Verification codes should be displayed on the login page for user authentication.
7	Traffic of regions and IP groups should be sent to ADS M.
8	The performance of the traffic statistics collection engine should be optimized.
9	The database performance should be optimized.
10	The performance of collaborating with BSA should be optimized.
11	Version validation should be performed during system updating.
12	The interface for uploading files to a cloud platform should be changed to A interface.
13	vNTA should display no page when the license fails the check.
14	API-related documentation should be downloaded from the web-based manager.
15	Traffic units (both pps and bps) should be added to alerts logs sent by email.

4 Upgrade Procedure

The source version for the upgrade must be V4.5R89F03 or V4.5R89F03SP.

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_V4.5R90F00.171206build25517.bin and click Upload.

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

The upgrade takes about 5 minutes. 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 **V4.5R90F00**, the upgrade succeeded; if not, the upgrade failed and you need to contact technical support personnel of NSFOCUS.

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" for or directly denies your access request.
3. All engines stop working.
4. The upgrade 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 Description of New Functions

5.1 Batch Operations on Regions and IP Groups

Requirement Description

Regions or IP groups should be able to be created or deleted in batches.

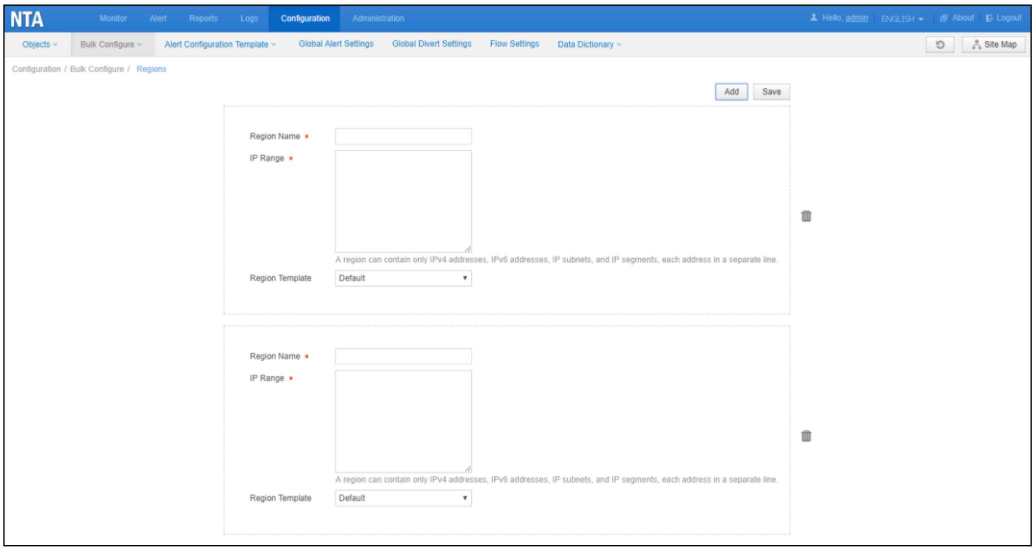
Scenario

- Addition: Users want to create multiple regions or IP groups with the same alert thresholds, but different IP address ranges. In this case, these regions or IP groups need to be created in batches with the same template.
- Deletion: Users want to delete multiple regions or IP groups in a rapid way.

Configuration and Use

Here, the bulk creation of two regions is used as an example.

Choose **Configuration > Bulk Configure**, click **Add**, type region names and IP address ranges for two regions, select a region template, and click **Save**.



Region Name *

IP Range *

A region can contain only IPv4 addresses, IPv6 addresses, IP subnets, and IP segments, each address in a separate line.

Region Template: Default

Region Name *

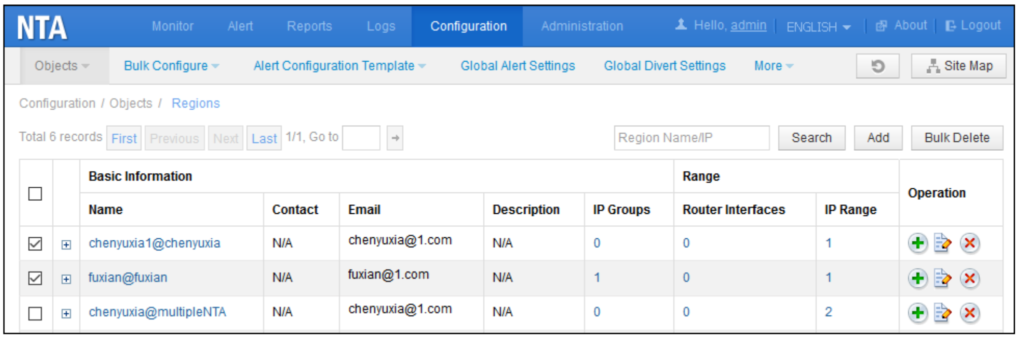
IP Range *

A region can contain only IPv4 addresses, IPv6 addresses, IP subnets, and IP segments, each address in a separate line.

Region Template: Default

Here, the deletion of two regions is used as an example.

Choose **Configuration > Objects > Regions**, select two regions, and click **Bulk Delete**.



□		Basic Information					Range		Operation
		Name	Contact	Email	Description	IP Groups	Router Interfaces	IP Range	
☑	⊞	chenyuxia1@chenyuxia	N/A	chenyuxia@1.com	N/A	0	0	1	
☑	⊞	fuxian@fuxian	N/A	fuxian@1.com	N/A	1	0	1	
□	⊞	chenyuxia@multipleNTA	N/A	chenyuxia@1.com	N/A	0	0	2	

5.2 Batch Application of an Alert Template to Multiple Regions or IP Groups

Requirement Description

An alert template should be able to be applied to more than one region or IP group simultaneously.

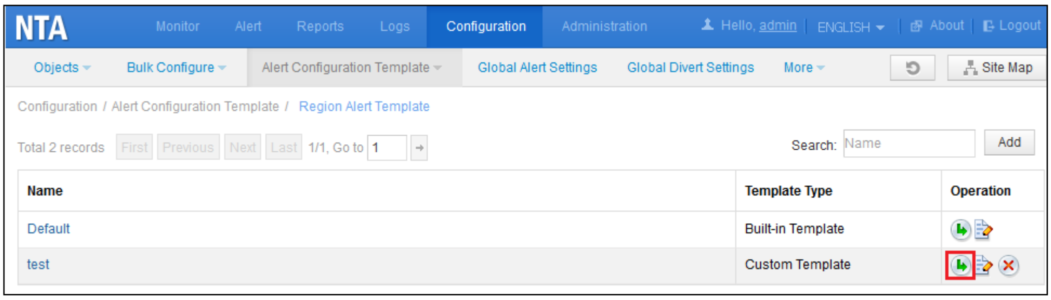
Scenario

A user creates regions with the same alert template. After a period of time, the user finds that certain thresholds included in the alert template are inappropriately configured or needs to turn off certain detections. In this case, the user can modify the alert template and re-apply it to these regions or IP groups.

Configuration and Use

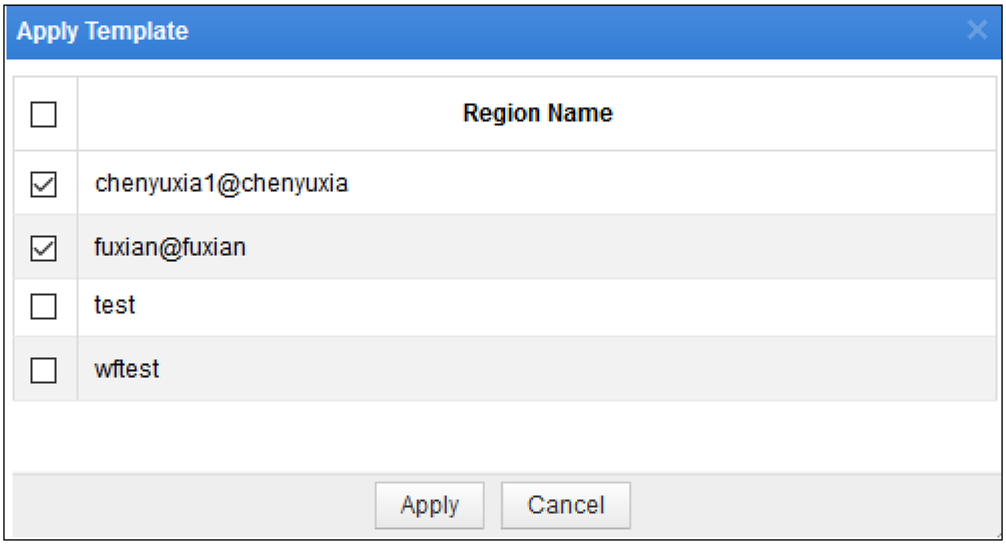
Here, the application of a region template is used as an example.

Choose **Configure > Alert Configuration Template > Region Alert Template** and click ➥ in the **Operation** column of a region template.



Name	Template Type	Operation
Default	Built-in Template	
test	Custom Template	

Select regions to which the template applies and click **Apply**.



Apply Template

☐	Region Name
☑	chenyuxia1@chenyuxia
☑	fuxian@fuxian
☐	test
☐	wftest

5.3 Separate Diversion Holding Time for Each Diversion Policy

Requirement Description

The global hold time for null route/BGP diversion should be removed, and each diversion policy should be configured with a separate diversion holding time instead. This setting should be included in both the global diversion configuration and region/IP group diversion configuration.

Scenario

Different sizes of alert traffic need to be diverted in different ways. For example, 1 GB traffic is diverted to ADS through BGP, while 10 Gbps traffic is diverted to a null route. In particular, the null-route diversion may be conducted by an upstream device. In order to prevent route flapping, the holding time of the null-route diversion is generally longer than that of BGP diversion or ADS diversion.

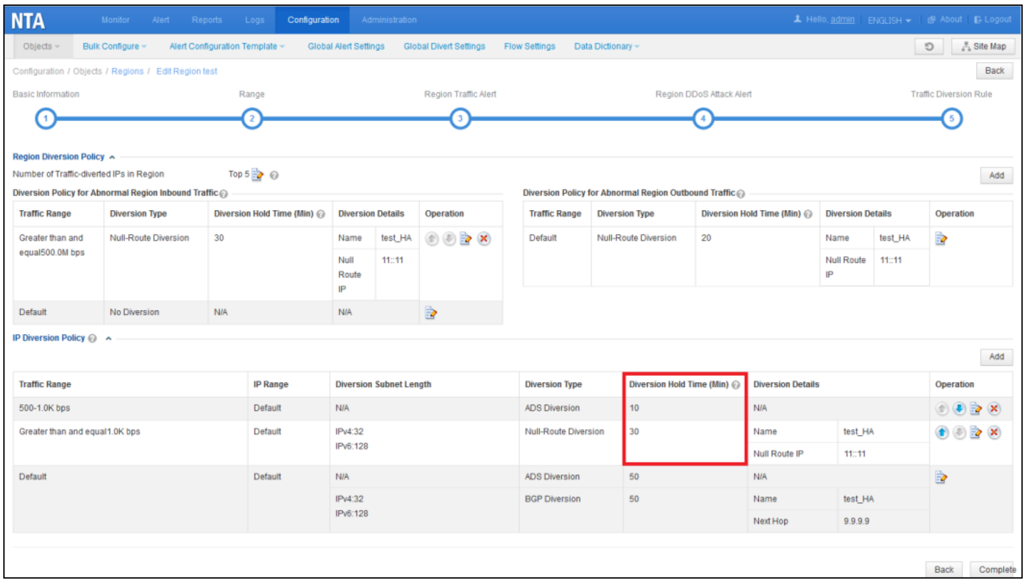
In a word, different diversion policies should be configured with different diversion holding time.

Configuration and Use

Here, the region configuration is taken as an example.

Choose **Configuration > Objects > Regions** and create a region. Then configure different diversion holding time for different diversion policies.

The value range of the diversion holding time is 0–1440 minutes. The value **0** indicates that the diversion stops immediately after the alert ends.



Region Diversion Policy

Number of Traffic-diverted IPs in Region Top 5

Diversion Policy for Abnormal Region Inbound Traffic

Traffic Range	Diversion Type	Diversion Hold Time (Min)	Diversion Details		Operation
Greater than and equal500.0M bps	Null-Route Diversion	30	Name Null Route IP	test_HA 11::11	
Default	No Diversion	N/A	N/A		

Diversion Policy for Abnormal Region Outbound Traffic

Traffic Range	Diversion Type	Diversion Hold Time (Min)	Diversion Details		Operation
Default	Null-Route Diversion	20	Name Null Route IP	test_HA 11::11	

IP Diversion Policy

Traffic Range	IP Range	Diversion Subnet Length	Diversion Type	Diversion Hold Time (Min)	Diversion Details		Operation
500-1.0K bps	Default	N/A	ADS Diversion	10	N/A		
Greater than and equal1.0K bps	Default	IPv4:32 IPv6:128	Null-Route Diversion	30	Name Null Route IP	test_HA 11::11	
Default	Default	N/A	ADS Diversion	50	N/A		
		IPv4:32 IPv6:128	BGP Diversion	50	Name Next Hop	test_HA 9.9.9.9	

5.4 Different Statistical Modes Being Added in the Case of Flow Statistical Interval of 60 Seconds

Requirement Description

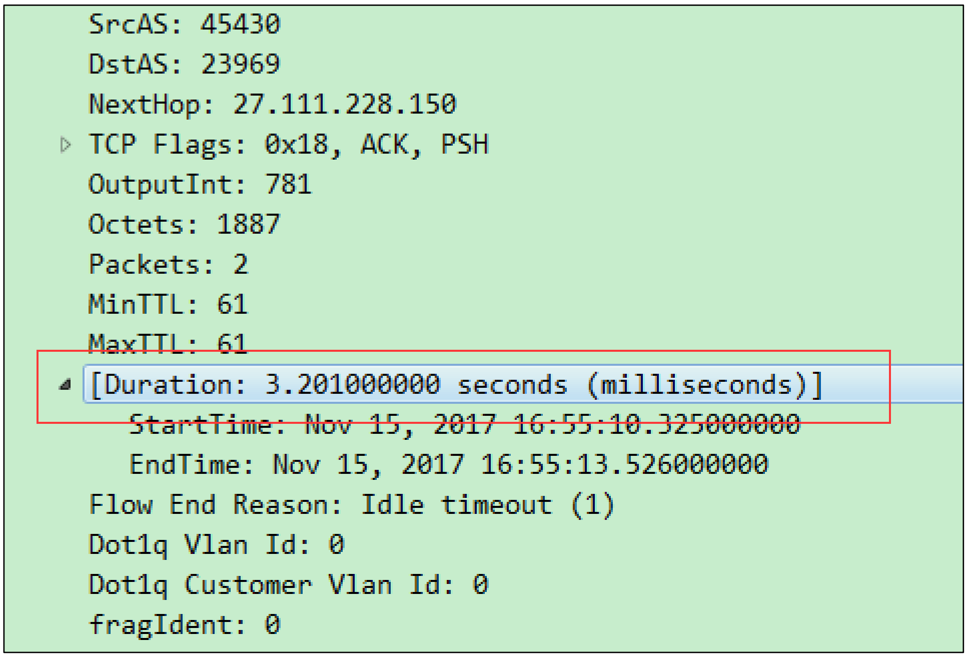
When the statistical interval for flows is 60 seconds, different statistical modes (partial statistics and all statistics) should be provided for selection.

Scenario

Switches or routers adopt the following flow output mechanism: The switch or router collects flow information and stores it in the cache. The two parameters, active timeout and inactive timeout, specify the timeout period of active flows and inactive flows respectively. If the timeout period expires, the device assembles the cached flow information into flows and sends to NTA.

If the timeout period is too long, for example 10 minutes, the switch or router collects flow information that is cached for 10 minutes, assembles the information into flows, and sends them to NTA. This will cause a too long attack detection delay on NTA, leading to inaccurate statistics (because NTA's statistical engine collects statistics periodically).

The following figure shows the NetFlow capture data, where **Duration** indicates how long flows are cached before being sent to NTA.



```
    SrcAS: 45430
    DstAS: 23969
    NextHop: 27.111.228.150
  ▷ TCP Flags: 0x18, ACK, PSH
    OutputInt: 781
    Octets: 1887
    Packets: 2
    MinTTL: 61
    MaxTTL: 61
  ◢ [Duration: 3.201000000 seconds (milliseconds)]
      StartTime: Nov 15, 2017 16:55:10.325000000
      EndTime: Nov 15, 2017 16:55:13.526000000
    Flow End Reason: Idle timeout (1)
    Dot1q Vlan Id: 0
    Dot1q Customer Vlan Id: 0
    fragIdent: 0
```

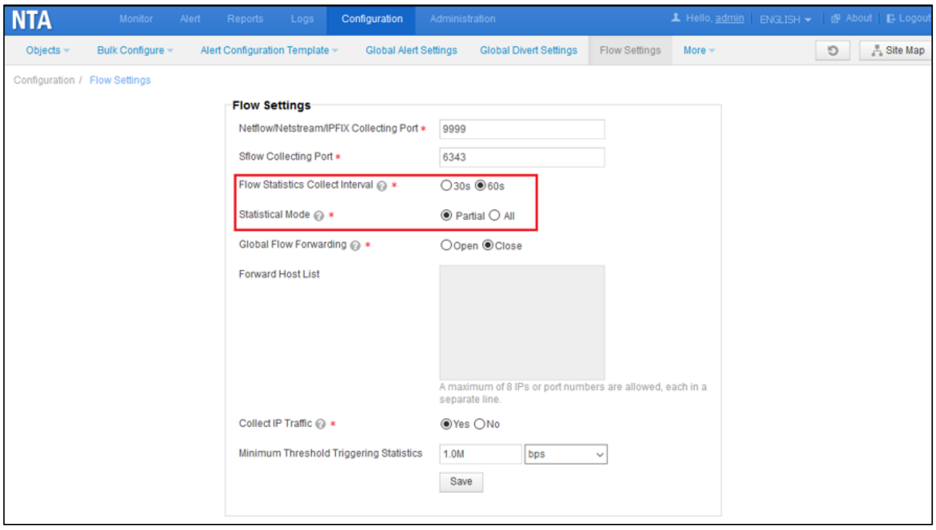
NTA of this version provides three flow statistics modes:

- **30 seconds:** This mode is recommended. In this mode, to ensure timely attack detection, users are advised to set the active timeout period and inactive timeout period to less than 30 seconds on the switch or router.
- **Collection of all flows every 60 seconds**: For most switches or routers, the flow timeout periods can be set to 60 seconds, if they cannot be set to 30 seconds. If flow timeout periods are set to 60 seconds on a switch or route, NTA collects statistics all flows from the switch or router every 60 seconds.
- **Collection of partial flows every 60 seconds**: For some reasons such as the user's switch or router is old, the flow timeout periods may be more than 30 or even 60 seconds. In this case, it is recommended that NTA collect partial statistics every 60 seconds. That is to say, NTA only collects flows that are cached for 60 seconds. The consequence of this mode is that the flow rate calculated by NTA is slightly lower than the actual rate. This mode applies when flows are cached for a long time. This is because only a part of flows are collected in such a case. If NTA is configured to collect all flows every 60 seconds at this time, the flow rate calculated by NTA may be multiple times the actual rate.

Here is an example: A flow is cached for 120 seconds, reaching 300 bytes in total. The rate of this flow is 2.5 (300/120) bytes per second. In this collection mode, NTA collects flow data of 150 bytes ((60s/120) x 300) every 60 seconds. The flow rate calculated by NTA is 2.5 (150/60) bytes per second. You can see that the two flow rates are consistent in this statistical mode.

Configuration and Use

Choose **Configuration > Flow Settings** and configure **Flow Statistics Collect Interval** and **Statistical Mode**.



Configuration / Flow Settings

Flow Settings

Netflow/Netstream/IPFIX Collecting Port * 9999

Sflow Collecting Port * 6343

Flow Statistics Collect Interval * ○30s ●60s

Statistical Mode * ● Partial ○ All

Global Flow Forwarding * ○Open ●Close

Forward Host List

A maximum of 8 IPs or port numbers are allowed, each in a separate line.

Collect IP Traffic * ●Yes ○No

Minimum Threshold Triggering Statistics 1.0M bps

5.5 Support for Selection of File Types to Be Sent, Sending of Global DDoS Alert Data, and Inclusion of Top 100 Source IP Addresses in DDoS Alerts During Collaboration with a Third-Party Cloud Platform

Requirement Description

When collaborating with a third-party platform, NTA should allow users to select the types of files to be sent and send global DDoS alert data.

Scenario

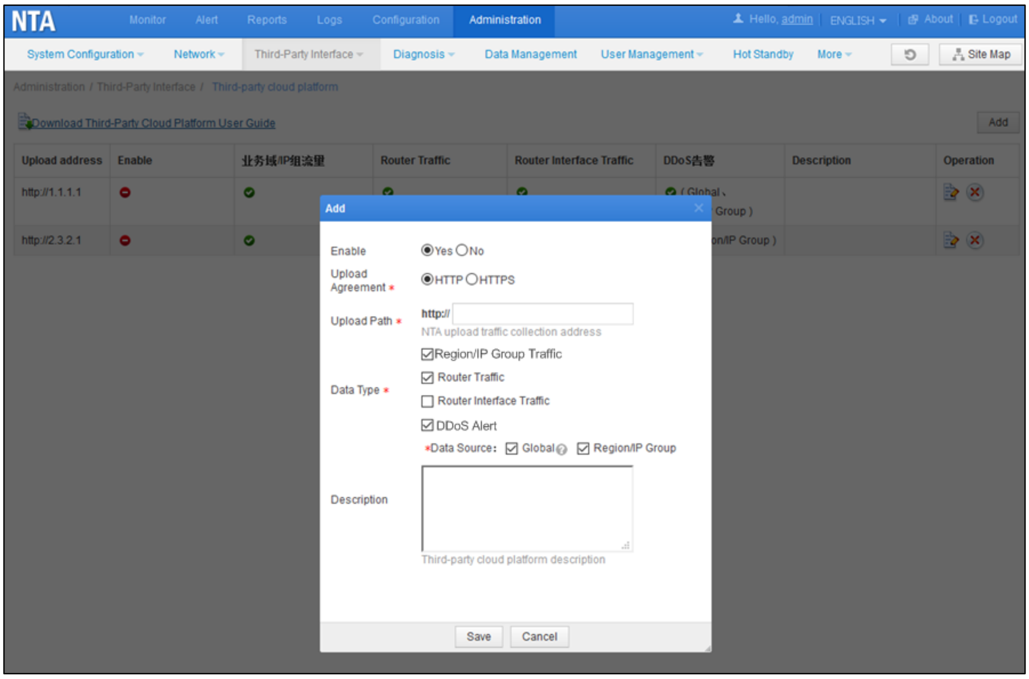
NTA can send DDoS alert traffic, region/IP group traffic, router traffic, and router interface traffic to a third-party cloud platform. However, some third-party cloud platforms may only need certain types of traffic data, rather than all data. In such a case, NTA should support the selection the types of data to be sent to those third-party cloud platforms. This helps save the customer's bandwidth, avoiding unnecessary pressure on the server.

For DDoS alert traffic, NTA of the previous version can only send IP alerts specific to regions/IP groups. However, some users also care about global alerts.

As DDoS alert data relating to source IP addresses is also a major concern of users, statistics of top 10 source IP addresses in previous versions are not adequate, and therefore data of top 100 source IP addresses is added in this version.

Configuration and Use

Choose **Administration** > **Third-Party Interface** > **Third-Party Cloud Platform** and configure the types of files to be sent and DDoS alert objects



Upload address	Enable	业务域/IP组流量	Router Traffic	Router Interface Traffic	DDoS告警	Description	Operation
http://1.1.1.1	●	✓	✓	✓	✓ (Global、 Group)		
http://2.3.2.1	●	✓			on/IP Group)		

Add

Enable ● Yes ○ No

Upload Agreement * ● HTTP ○ HTTPS

Upload Path * http://
NTA upload traffic collection address

Data Type *
☑ Region/IP Group Traffic
☑ Router Traffic
□ Router Interface Traffic
☑ DDoS Alert
*Data Source: ☑ Global ☑ Region/IP Group

Description
Third-party cloud platform description

5.6 Verification Codes for User Authentication

Requirement Description

Verification codes should be used to authenticate users.

Each verification code is a combination of four English letters (case-insensitive) and digits.

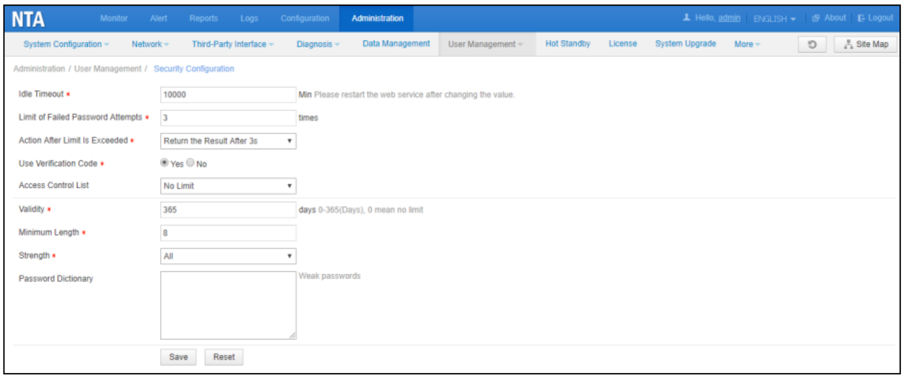
Verification codes are randomly generated upon each login. You can click the verification code displayed or press F5 to refresh verification code.

Scenario

Verification codes are added on the web login page to prevent brute-force cracking attacks against the web-based manager or to satisfy compliance requirements.

Configuration and Use

Choose **Administration > User Management > Security Configuration** and select **Yes** for **Use Verification Code**.



Administration / User Management / Security Configuration

Idle Timeout * 10000 Min Please restart the web service after changing the value.

Limit of Failed Password Attempts * 3 times

Action After Limit Is Exceeded * Return the Result After 3s ▾

Use Verification Code * ● Yes ○ No

Access Control List No Limit ▾

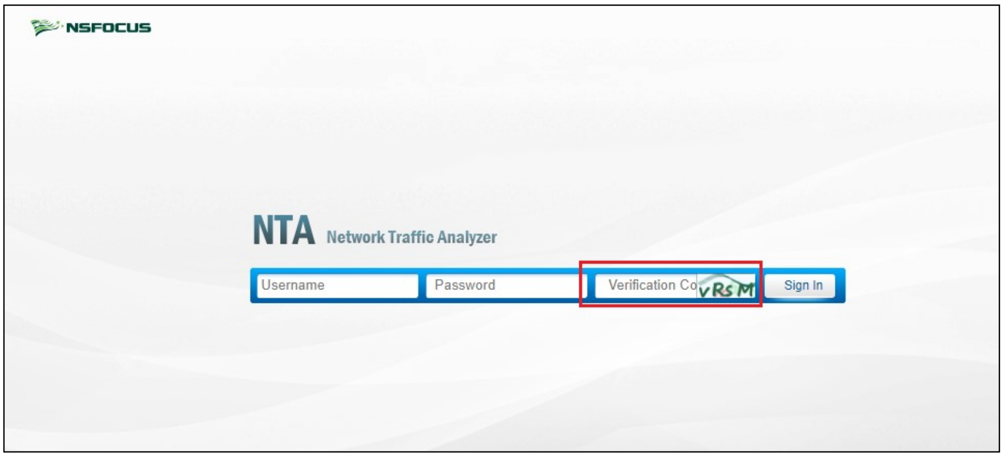
Validity * 365 days 0-365(Days), 0 mean no limit

Minimum Length * 8

Strength * All ▾

Password Dictionary Weak passwords

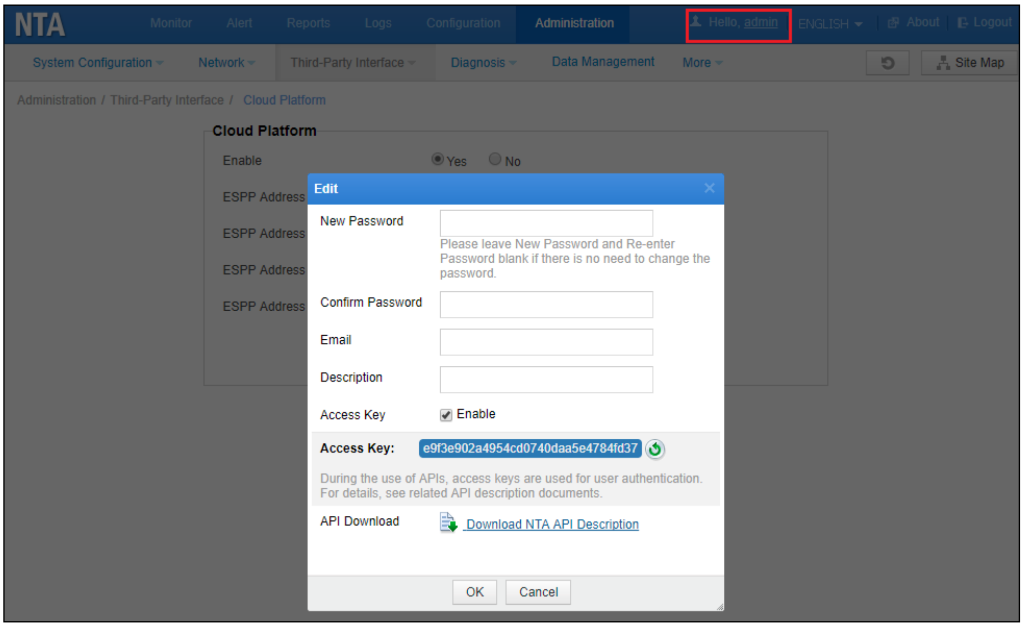
After the setting, a verification code is displayed upon a login:



5.7 Other Functions

1. Traffic of regions and IP groups can be sent to ADS M.
2. Traffic of regions and IP groups can be sent to ADS M so that the trend of such traffic on NTA can be shown on ADS M.
3. The performance of the traffic statistics collection engine is optimized.
4. The database performance is optimized.
5. The performance of collaborating with BSA is optimized.
6. The issue of overhigh CPU usage and memory usage during collaboration with BSA is resolved.
7. Version validation is performed during system upgrade.
8. V4.5R90F00 can be upgraded only from V4.5R89F03, V4.5R89F03SP01, and V4.5R89F03SP02.
9. The interface for uploading files to a cloud platform is changed to A interface.
10. vNTA displays no page when the license fails the check.
11. API-related documentation can be downloaded from the web-based manager.

    Click the user name in the quick access bar and then click the API documentation link to download the document in the **Edit** dialog box.



Cloud Platform

Enable ● Yes ○ No

ESPP Address

ESPP Address

ESPP Address

ESPP Address

Edit

New Password

Please leave New Password and Re-enter Password blank if there is no need to change the password.

Confirm Password

Email

Description

Access Key ☑ Enable

Access Key: e9f3e902a4954cd0740daa5e4784fd37

During the use of APIs, access keys are used for user authentication. For details, see related API description documents.

API Download Download NTA API Description

5.1.8 Fixed Bugs

1. 120170-[Other-BGP] NTA with a virtual IPv6 address fails form a neighbor relationship with a router.
2. 120286-[SNMP interface traffic] The maximum traffic on the SNMP interface is incorrectly displayed as 595056254 Gbps.
3. 124836-[Other] If a router is removed when an alerted condition persists for one of its interfaces, the router interface name is displayed as HTML tags in this alert.
4. 124903-[Diversion controller] If the alert holding period is unusually long, the triggered diversion is revoked before the period expires.
5. 124926-[HA] After HA is enabled, NTA fails to collaborate with ADS M in another network segment.
6. 125564-[Other] Under **Administration** > **User Management** > **Security Configuration**, only the first of allowed IP addresses typed in the **Access Control List** box takes effect.
7. 124149-[Traffic display on cloud service] Inaccurate traffic data is uploaded from NTA to NSFOCUS Collapsar Cloud-based Scrubbing Service (CCSS).
8. 127315-[Traffic analysis] Statistics on top ASs do not cover 32-bit AS numbers.

6 Compatibility

- Browser: Chrome, Firefox, and Internet Explorer 10, with the former two recommended.
- ADS: V4.5.88.15 and V4.5R90F00
- ADS M: V4.5R90F00
- TAT: V2.0.0