NSFOCUS NTA Release Notes

1. Basic Information

Product Model	• NTA NX3-HD2100/HD2200/HD3000 • NTA VM
Software Version	V4.5R90F06
Upgrade File	update_nta_x86_V4.5R90F06.241220build50693.bin Hash: 8d345b70f5bfbf1db453ad596a960edd
Release Date	2024-12-30
How to Obtain	Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support.

2. Version Mapping

ADS	V4.5R90F06
ADS M	V4.5R90F06
ADBOS	V4.5R90F06
NTA-ATM	V4.5R89F05
Threat Analysis and Traceback System (TAT)	V2.0.0
MF	• V4.5R90F01SP08 • V4.5R90F01SP09 • V4.5R90F01SP10
Client Browser	• Chrome • Firefox
Documentation	NSFOCUS NTA V4.5R90F06 User Guide

3. New Requirements

No.	Requirement Description
1	Network segment-based DDoS detection for regions, IP groups, and the global scope
2	Support for netmask/prefix length customization for network segment-specific diversion
3	Power status information sent via SNMP
4	Addition of "NSFOCUS" before the product name on the login page
5	Adaptation of third-party interfaces
6	NPAI interface upgrade
7	Bugs should be fixed.

4. Function Changes

4.1 Network Segment-based DDoS Detection Function for Regions, IP Groups, and the Global Scope

Overview

Traditional DDoS attacks target single IP addresses, and so can usually be detected by comparing the actual traffic destined for an IP address with the threshold (predefined or auto-learned). However, carpet bombing attacks often target an entire network segment, with attack traffic to a single IP address being too small to be detected by conventional detection solutions. Nowadays, in addition to IDCs and ISPs, which are typical targets of carpet bombing attacks, financial institutions are vulnerable to this type of attack due to business expansion (increasing number of IP addresses). As carpet bombing attacks often target session tables of a firewall or WAF, both IP address-specific and total attack traffic are too small to be detected, let alone triggering traffic cleaning.

Previous versions of NTA have provided behavior-based protection against carpet bombing attacks initiated from real IP addresses. The new version should complete the detection function by providing detection of and protection against network segment-specific attacks initiated from forged IP addresses. NTA can now detect carpet bombing attacks through the network segment-based DDoS detection function.

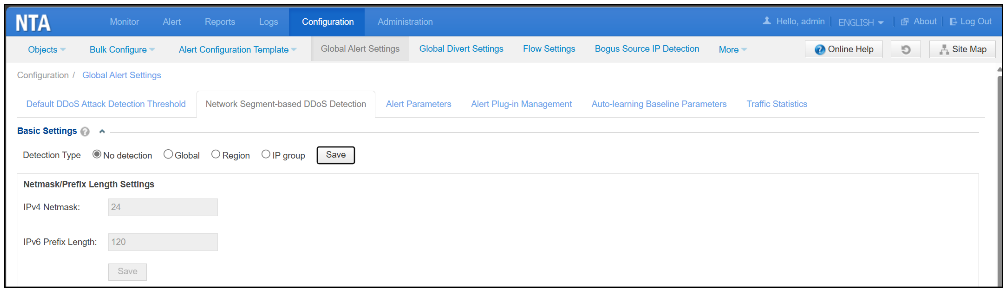
Configuration and Use

First, note the following when configuring and using the network segment-based DDoS detection function:

1. Unlike single IP address-triggered DDoS alerts, the destination IP address in network segment-specific DDoS alerts is in the format of "IP/netmask" like 1.1.1.0/24.
2. Network segment-specific DDoS alerts do not support query of alert details (not covered in traffic statistics). In other words, clicking the alert ID of a network segment-specific alert in the alert list under **Alert > Overview** would not return any more information about the alert.
3. Network segment-specific DDoS attack alerts can be sent via email/SNMP/syslog/SFTP, and to a cloud cleaning platform and management platform configured under **Administration > Third-Party Interface**.

You can configure different types of network segment-based DDoS detection under **Configuration > Global Alert Settings > Network Segment-based DDoS Detection** to suit different scenarios.

- **No detection**: global switch for turning on or off the function of detecting network segment-specific DDoS attacks. If this is selected, the function does not work even when it is enabled for a region or IP group.



Basic Settings

Detection Type ● No detection ○ Global ○ Region ○ IP group Save

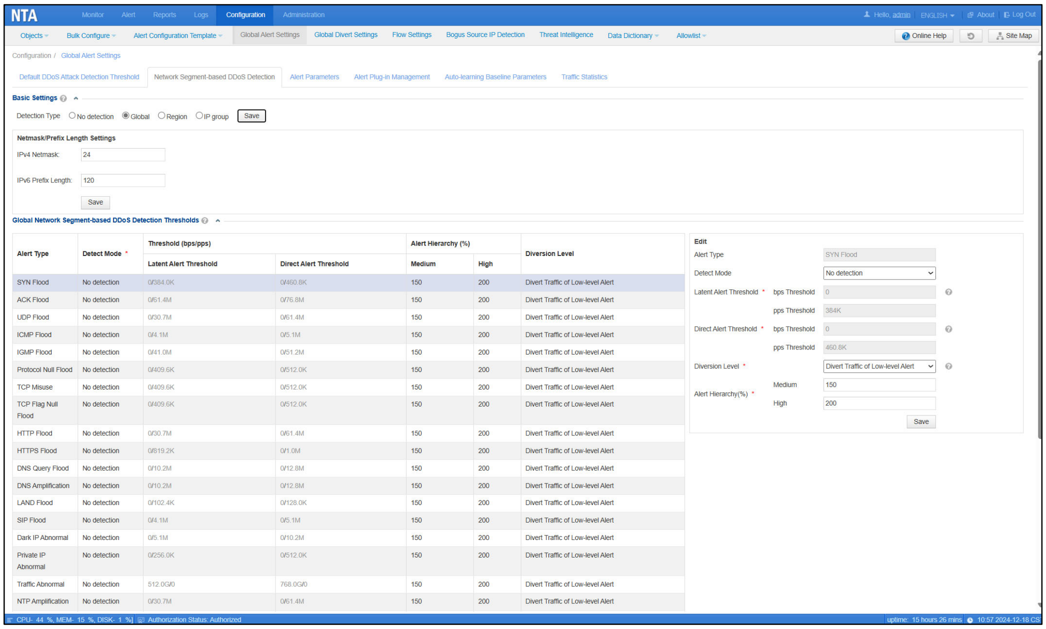
Netmask/Prefix Length Settings

IPv4 Netmask: 24

IPv6 Prefix Length: 120

Save

- **Global**: After this is selected, you should further configure the netmask/prefix length and DDoS detection thresholds under **Configuration > Global Alert Settings > Network Segment-based DDoS Detection**. Then, when network segment-specific alerts are generated, their objects are always "Default DDoS Attack Alert" regardless of whether the matched destination IP address belongs to any region or IP group.



Basic Settings

Detection Type ○ No detection ● Global ○ Region ○ IP group Save

Netmask/Prefix Length Settings

IPv4 Netmask: 24

IPv6 Prefix Length: 120

Save

Global Network Segment-based DDoS Detection Thresholds

Alert Type	Detect Mode *	Threshold (bps/pps)		Alert Hierarchy (%)		Diversion Level
		Latent Alert Threshold	Direct Alert Threshold	Medium	High	
SYN Flood	No detection	0/384.0K	0/460.8K	150	200	Divert Traffic of Low-level Alert
ACK Flood	No detection	0/61.4M	0/76.8M	150	200	Divert Traffic of Low-level Alert
UDP Flood	No detection	0/30.7M	0/61.4M	150	200	Divert Traffic of Low-level Alert
ICMP Flood	No detection	0/4.1M	0/5.1M	150	200	Divert Traffic of Low-level Alert
IGMP Flood	No detection	0/41.0M	0/51.2M	150	200	Divert Traffic of Low-level Alert
Protocol Null Flood	No detection	0/409.6K	0/512.0K	150	200	Divert Traffic of Low-level Alert
TCP Misuse	No detection	0/409.6K	0/512.0K	150	200	Divert Traffic of Low-level Alert
TCP Flag Null Flood	No detection	0/409.6K	0/512.0K	150	200	Divert Traffic of Low-level Alert
HTTP Flood	No detection	0/30.7M	0/61.4M	150	200	Divert Traffic of Low-level Alert
HTTPS Flood	No detection	0/819.2K	0/1.0M	150	200	Divert Traffic of Low-level Alert
DNS Query Flood	No detection	0/10.2M	0/12.8M	150	200	Divert Traffic of Low-level Alert
DNS Amplification	No detection	0/10.2M	0/12.8M	150	200	Divert Traffic of Low-level Alert
LAND Flood	No detection	0/102.4K	0/128.0K	150	200	Divert Traffic of Low-level Alert
SIP Flood	No detection	0/4.1M	0/5.1M	150	200	Divert Traffic of Low-level Alert
Dark IP Abnormal	No detection	0/5.1M	0/10.2M	150	200	Divert Traffic of Low-level Alert
Private IP Abnormal	No detection	0/256.0K	0/512.0K	150	200	Divert Traffic of Low-level Alert
Traffic Abnormal	No detection	512.0G/0	768.0G/0	150	200	Divert Traffic of Low-level Alert
NTP Amplification	No detection	0/30.7M	0/61.4M	150	200	Divert Traffic of Low-level Alert

Edit

Alert Type: SYN Flood

Detect Mode: No detection

Latent Alert Threshold * bps Threshold: 0

pps Threshold: 384K

Direct Alert Threshold * bps Threshold: 0

pps Threshold: 460.8K

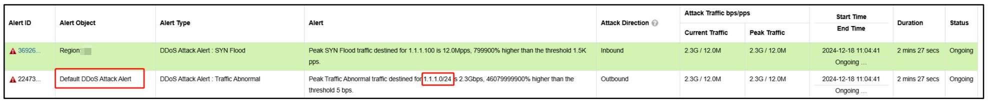
Diversion Level *: Divert Traffic of Low-level Alert

Alert Hierarchy(%) * Medium: 150

High: 200

Save

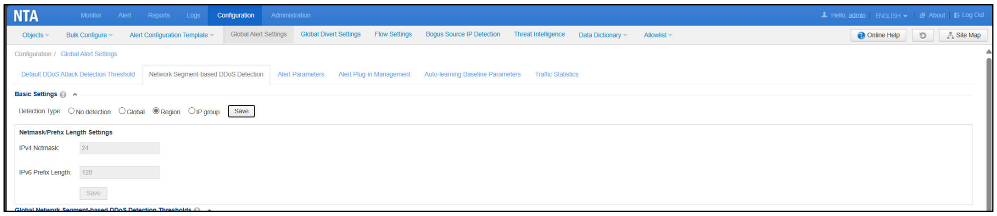
CPU- 44 %, MEM- 15 %, DISK- 1 %] Authorization Status: Authorized uptime: 15 hours 26 mins 10:57 2024-12-18 CS



Alert ID	Alert Object	Alert Type	Alert	Attack Direction	Attack Traffic bps/pps		Start Time End Time	Duration	Status
					Current Traffic	Peak Traffic			
36926...	Region[redacted]	DDoS Attack Alert : SYN Flood	Peak SYN Flood traffic destined for 1.1.1.100 is 12.0Mpps, 799900% higher than the threshold 1.5K pps.	Inbound	2.3G / 12.0M	2.3G / 12.0M	2024-12-18 11:04:41 Ongoing ...	2 mins 27 secs	Ongoing
22473...	Default DDoS Attack Alert	DDoS Attack Alert : Traffic Abnormal	Peak Traffic Abnormal traffic destined for 1.1.1.0/24 is 2.3Gbps, 46079999900% higher than the threshold 5 bps.	Outbound	2.3G / 12.0M	2.3G / 12.0M	2024-12-18 11:04:41 Ongoing ...	2 mins 27 secs	Ongoing

- **Region**: After this is selected, network segment-based DDoS detection can work for a region only when it is enabled and related detection thresholds are configured in the

Region DDoS Attack Alert for a Network Segment area of the **Region DDoS Attack Alert** page under **Configuration > Objects > Regions** during region creation/editing. Then, when network segment-specific alerts are generated, their objects are always this region regardless of whether the matched destination IP address belongs to any IP group in this region.



Basic Settings

Detection Type ○ No detection ○ Global ● Region ○ IP group Save

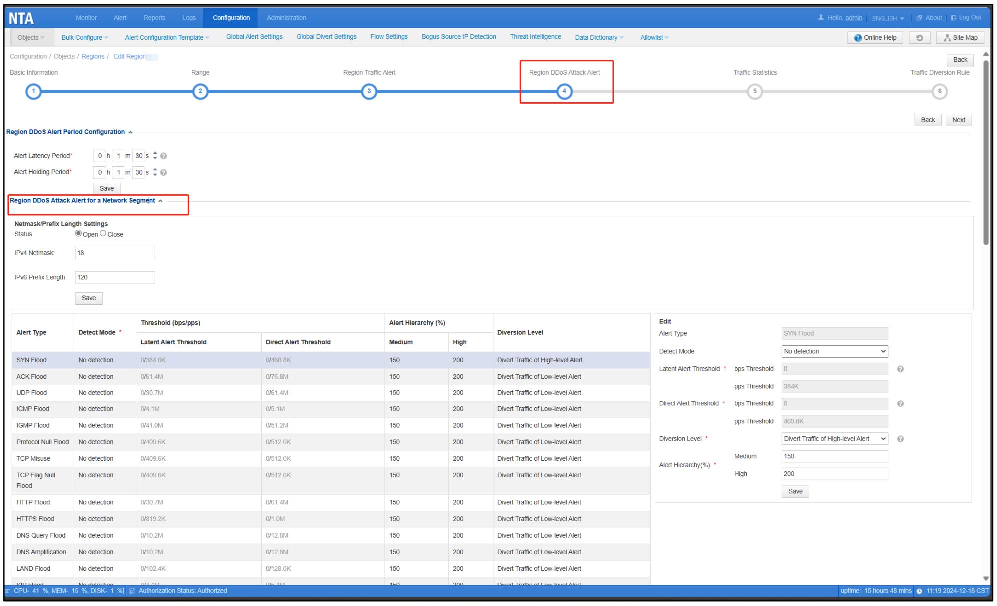
Netmask/Prefix Length Settings

IPv4 Netmask: 24

IPv6 Prefix Length: 120

Save

Global Network Segment-based DDoS Detection Thresholds



Configuration / Objects / Regions / Edit Region [redacted]

Region DDoS Alert Period Configuration

Alert Latency Period* 0 h 1 m 30 s

Alert Holding Period* 0 h 1 m 30 s

Save

Region DDoS Attack Alert for a Network Segment

Netmask/Prefix Length Settings

Status ● Open ○ Close

IPv4 Netmask: 18

IPv6 Prefix Length: 120

Save

Alert Type	Detect Mode *	Threshold (bps/pps)		Alert Hierarchy (%)		Diversion Level
		Latent Alert Threshold	Direct Alert Threshold	Medium	High	
SYN Flood	No detection	0/384.0K	0/460.8K	150	200	Divert Traffic of High-level Alert
ACK Flood	No detection	0/61.4M	0/76.8M	150	200	Divert Traffic of Low-level Alert
UDP Flood	No detection	0/30.7M	0/61.4M	150	200	Divert Traffic of Low-level Alert
ICMP Flood	No detection	0/4.1M	0/5.1M	150	200	Divert Traffic of Low-level Alert
IGMP Flood	No detection	0/41.0M	0/51.2M	150	200	Divert Traffic of Low-level Alert
Protocol Null Flood	No detection	0/409.6K	0/512.0K	150	200	Divert Traffic of Low-level Alert
TCP Misuse	No detection	0/409.6K	0/512.0K	150	200	Divert Traffic of Low-level Alert
TCP Flag Null Flood	No detection	0/409.6K	0/512.0K	150	200	Divert Traffic of Low-level Alert
HTTP Flood	No detection	0/30.7M	0/61.4M	150	200	Divert Traffic of Low-level Alert
HTTPS Flood	No detection	0/819.2K	0/1.0M	150	200	Divert Traffic of Low-level Alert
DNS Query Flood	No detection	0/10.2M	0/12.8M	150	200	Divert Traffic of Low-level Alert
DNS Amplification	No detection	0/10.2M	0/12.8M	150	200	Divert Traffic of Low-level Alert
LAND Flood	No detection	0/102.4K	0/128.0K	150	200	Divert Traffic of Low-level Alert
SIP Flood	No detection	0/4.1M	0/5.1M	150	200	Divert Traffic of Low-level Alert

Edit

Alert Type: SYN Flood

Detect Mode: No detection

Latent Alert Threshold * bps Threshold: 0

pps Threshold: 384K

Direct Alert Threshold * bps Threshold: 0

pps Threshold: 460.8K

Diversion Level *: Divert Traffic of High-level Alert

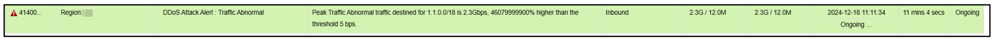
Alert Hierarchy(%) * Medium: 150

High: 200

Save

CPU- 41 %, MEM- 15 %, DISK- 1 %] Authorization Status: Authorized

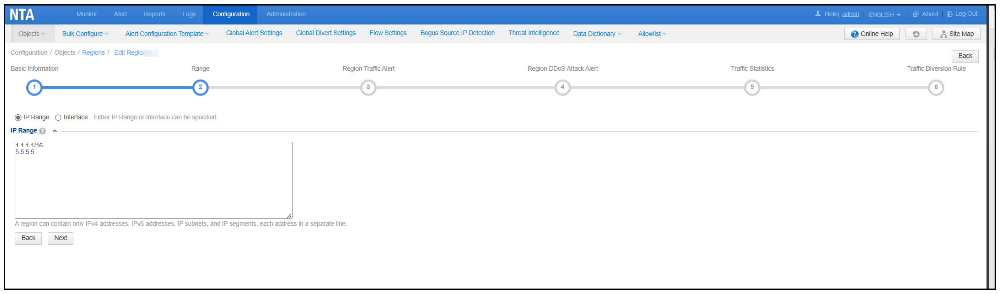
uptime: 15 hours 48 mins 11:19 2024-12-18 CST



41400...	Region [redacted]	DDoS Attack Alert : Traffic Abnormal	Peak Traffic Abnormal traffic destined for 1.1.0.0/18 is 2.3Gbps, 46079999900% higher than the threshold 5 bps.	Inbound	2.3G / 12.0M	2.3G / 12.0M	2024-12-18 11:11:34 Ongoing ...	11 mins 4 secs	Ongoing

Configuration constraints of the network segment-based DDoS detection function are as follows:

1. For a region or IP group to use the network segment-based DDoS detection function, all its IP addresses must be in CIDR notation.



Configuration / Objects / Regions / Edit Region

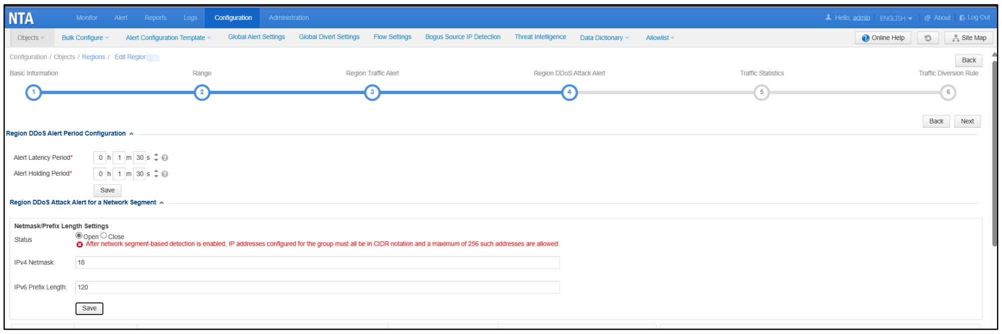
Basic Information — Range — Region Traffic Alert — Region DDoS Attack Alert — Traffic Statistics — Traffic Diversion Rule

● IP Range ○ Interface Either IP Range or Interface can be specified.

IP Range

```
1.1.1.1/16
5.5.5.5
```

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



Region DDoS Alert Period Configuration

Alert Latency Period*: 0 h 1 m 30 s

Alert Holding Period*: 0 h 1 m 30 s

Region DDoS Attack Alert for a Network Segment

Netmask/Prefix Length Settings

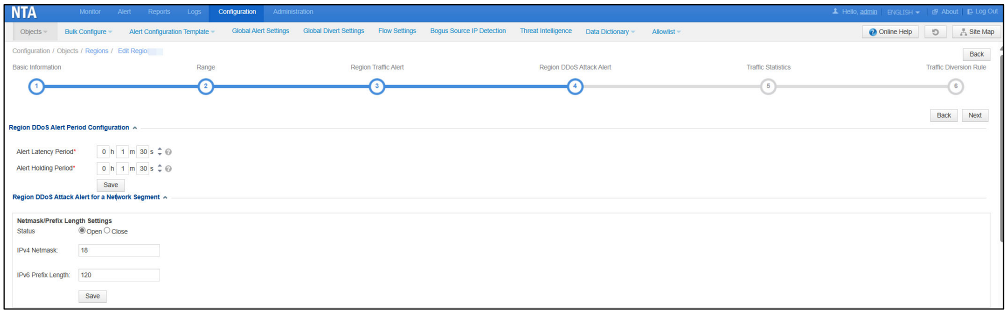
Status: ● Open ○ Close

After network segment-based detection is enabled, IP addresses configured for the group must all be in CIDR notation and a maximum of 256 such addresses are allowed.

IPv4 Netmask: 18

IPv6 Prefix Length: 120

2. After network segment-based DDoS detection is enabled for a region or IP group, its IP addresses cannot be changed to non-CIDR notation.



Region DDoS Alert Period Configuration

Alert Latency Period*: 0 h 1 m 30 s

Alert Holding Period*: 0 h 1 m 30 s

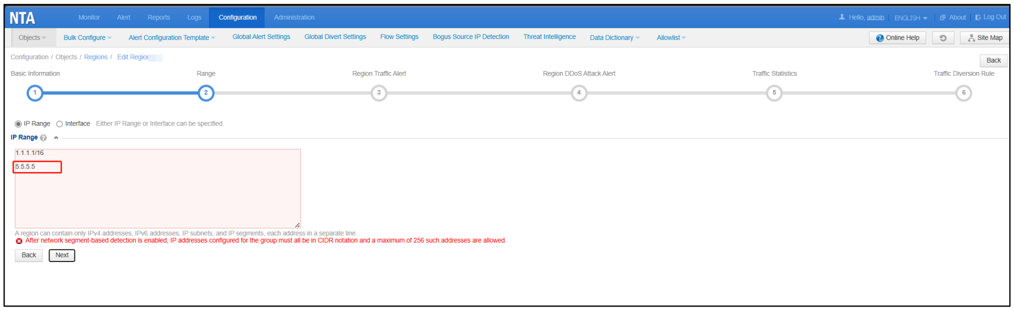
Region DDoS Attack Alert for a Network Segment

Netmask/Prefix Length Settings

Status: ● Open ○ Close

IPv4 Netmask: 18

IPv6 Prefix Length: 120



● IP Range ○ Interface Either IP Range or Interface can be specified.

IP Range

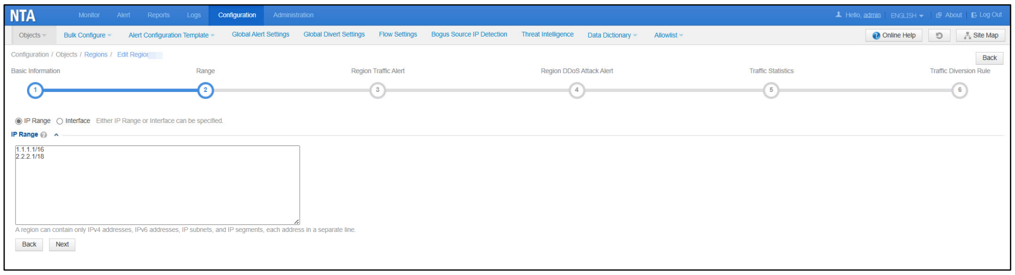
```
1.1.1.1/16
5.5.5.5
```

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

After network segment-based detection is enabled, IP addresses configured for the group must all be in CIDR notation and a maximum of 256 such addresses are allowed.

3. When all IP addresses of a region or IP group are in CIDR notation and the network segment-based DDoS detection is enabled, the IPv4 netmask configured in the

Region/IP Group DDoS Attack Alert for a Network Segment area should be less than or equal to the minimum netmask of CIDR blocks plus 8, but greater than or equal to the maximum netmask of CIDR blocks. The same rule applies to the IPv6 prefix length. As shown in the following figure, the minimum netmask of CIDR blocks is 16 and the maximum is 18. Therefore, the IPv4 netmask on the **Region DDoS Attack Alert** page should be in the range of 18–24.

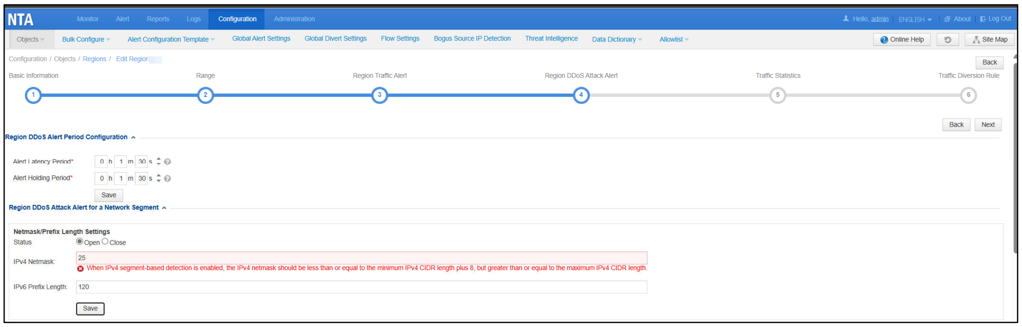


● IP Range ○ Interface Either IP Range or Interface can be specified.

IP Range

```
1.1.1.1/16
2.2.2.1/18
```

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



Region DDoS Alert Period Configuration

Alert Latency Period* 0 h 1 m 30 s

Alert Holding Period* 0 h 1 m 30 s

Region DDoS Attack Alert for a Network Segment

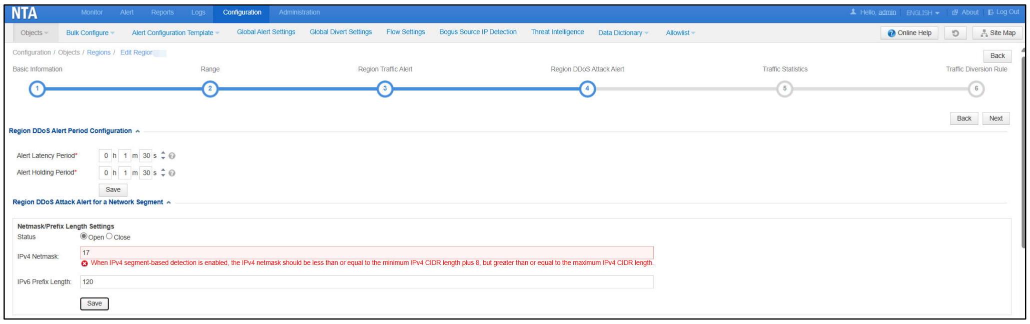
Netmask/Prefix Length Settings

Status ● Open ○ Close

IPv4 Netmask: 25

When IPv4 segment-based detection is enabled, the IPv4 netmask should be less than or equal to the minimum IPv4 CIDR length plus 8, but greater than or equal to the maximum IPv4 CIDR length.

IPv6 Prefix Length: 120



Region DDoS Alert Period Configuration

Alert Latency Period* 0 h 1 m 30 s

Alert Holding Period* 0 h 1 m 30 s

Region DDoS Attack Alert for a Network Segment

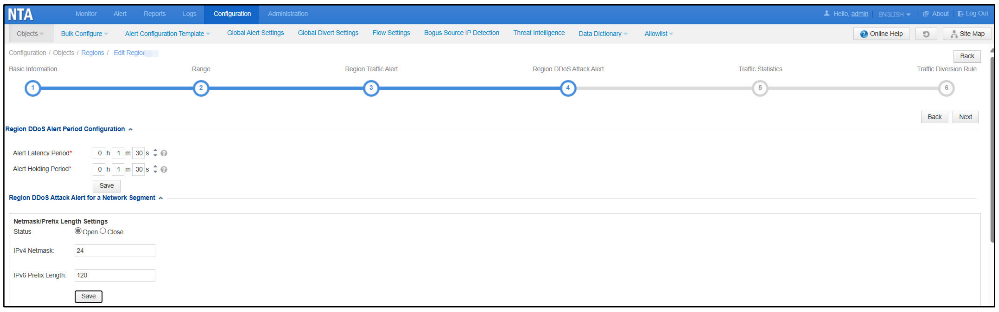
Netmask/Prefix Length Settings

Status ● Open ○ Close

IPv4 Netmask: 17

When IPv4 segment-based detection is enabled, the IPv4 netmask should be less than or equal to the minimum IPv4 CIDR length plus 8, but greater than or equal to the maximum IPv4 CIDR length.

IPv6 Prefix Length: 120



Configuration / Objects / Regions / Edit Regio[redacted]

Region DDoS Alert Period Configuration

Alert Latency Period*: 0 h 1 m 30 s

Alert Holding Period*: 0 h 1 m 30 s

Region DDoS Attack Alert for a Network Segment

Netmask/Prefix Length Settings

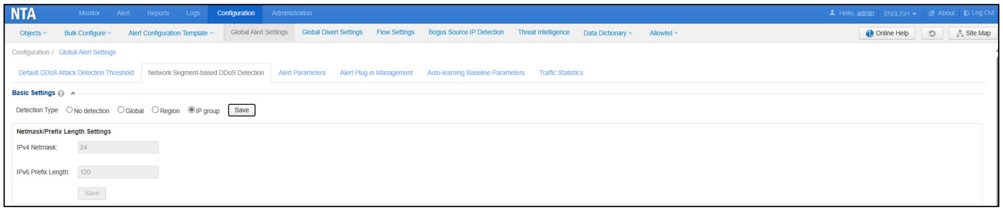
Status: ● Open ○ Close

IPv4 Netmask: 24

IPv6 Prefix Length: 120

4. When network segment-based DDoS detection is enabled and the IPv4 netmask and IPv6 prefix length are configured on the **Region DDoS Attack Alert** page, modifying the IP range on the **Range** page should also be bound by rule 3.

- **IP group**: After this is selected, network segment-based DDoS detection can work for an IP group only when it is enabled and related detection thresholds are configured in the **IP Group DDoS Attack Alert for a Network Segment** area of the **IP Group DDoS Attack Alert** page under **Configuration > Objects > Regions** during IP group creation/editing. Then, when network segment-specific alerts are generated, their objects are always this IP group.



Configuration / Global Alert Settings

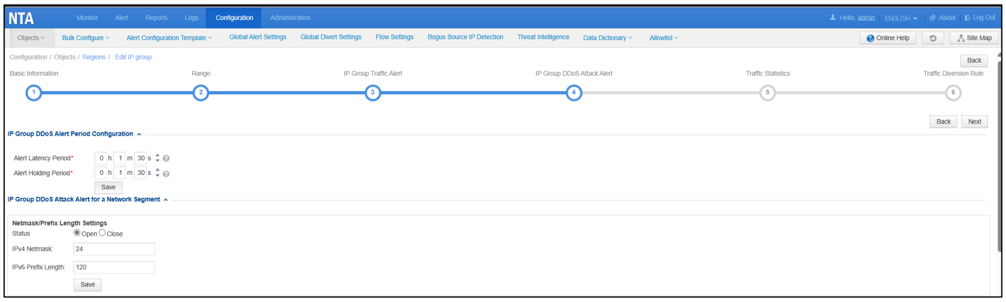
Basic Settings

Detection Type: ○ No detection ○ Global ○ Region ● IP group

Netmask/Prefix Length Settings

IPv4 Netmask: 24

IPv6 Prefix Length: 120



Configuration / Objects / Regions / Edit IP group

IP Group DDoS Alert Period Configuration

Alert Latency Period*: 0 h 1 m 30 s

Alert Holding Period*: 0 h 1 m 30 s

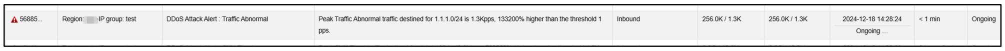
IP Group DDoS Attack Alert for a Network Segment

Netmask/Prefix Length Settings

Status: ● Open ○ Close

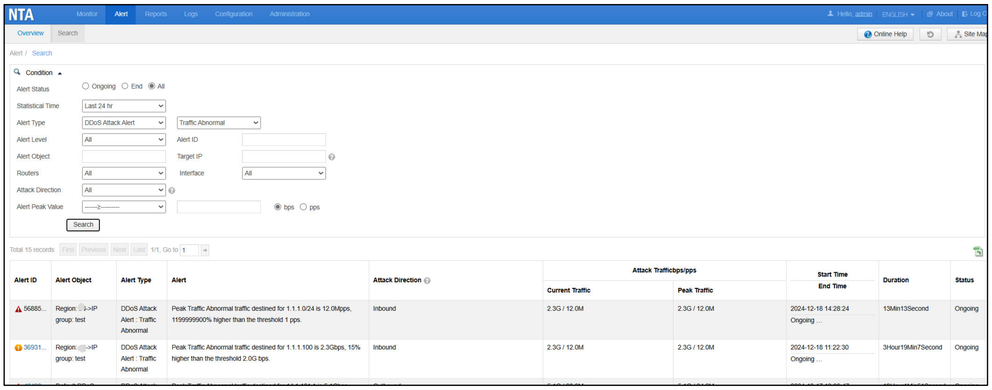
IPv4 Netmask: 24

IPv6 Prefix Length: 120



▲ 56885...	Region:[redacted]-IP group: test	DDoS Attack Alert : Traffic Abnormal	Peak Traffic Abnormal traffic destined for 1.1.1.0/24 is 1.3Kpps, 133200% higher than the threshold 1 pps.	Inbound	256.0K / 1.3K	256.0K / 1.3K	2024-12-18 14:28:24 Ongoing ...	< 1 min	Ongoing

You can query network segment-specific DDoS attacks under **Alert > Search**.



Alert Status ○ Ongoing ○ End ● All

Statistical Time: Last 24 hr

Alert Type: DDoS Attack Alert | Traffic Abnormal

Alert Level: All | Alert ID:

Alert Object: | Target IP:

Routers: All | Interface: All

Attack Direction: All

Alert Peak Value: ------≥--------- | ● bps ○ pps

Total 15 records 1/1, Go to 1

Alert ID	Alert Object	Alert Type	Alert	Attack Direction	Attack Trafficbps/pps		Start Time End Time	Duration	Status
					Current Traffic	Peak Traffic			
56885...	Region: [redacted]->IP group: test	DDoS Attack Alert : Traffic Abnormal	Peak Traffic Abnormal traffic destined for 1.1.1.0/24 is 12.0Mpps, 1199999900% higher than the threshold 1 pps.	Inbound	2.3G / 12.0M	2.3G / 12.0M	2024-12-18 14:28:24 Ongoing ...	13Min13Second	Ongoing
36931...	Region: [redacted]->IP group: test	DDoS Attack Alert : Traffic Abnormal	Peak Traffic Abnormal traffic destined for 1.1.1.100 is 2.3Gbps, 15% higher than the threshold 2.0G bps.	Inbound	2.3G / 12.0M	2.3G / 12.0M	2024-12-18 11:22:30 Ongoing ...	3Hour19Min7Second	Ongoing

4.2 Support for Netmask/Prefix Length Customization for Network Segment-specific Diversion

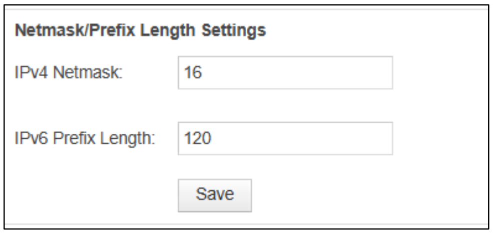
Overview

Network segment-based DDoS detection is now supported for regions, IP groups, and the global scope. To adapt to this function, NTA now allows you to customize the netmask/prefix length in related policies.

Configuration and Use

Diversion types supported for this function include no diversion, scrubbing device diversion, BGP diversion, and null-route diversion. You are allowed to configure two diversion rules in a policy. For scrubbing device diversion, BGP diversion, and null-route diversion, you must configure the IPv4 netmask and IPv6 prefix length.

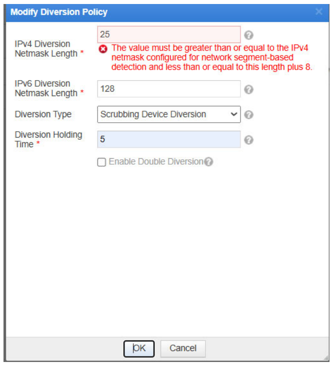
How the netmask and prefix length are configured here depends on the IPv4 netmask and IPv6 prefix length set on the **Region DDoS Attack Alert** page. Besides, the netmask/prefix length for traffic diversion should be greater than or equal to the netmask/prefix length configured for DDoS detection, but less than or equal to that length plus 8. As shown in the following figures, when the IPv4 netmask for DDoS detection is 16, the IPv4 netmask configured for traffic diversion must be in the range of 16–24.



Netmask/Prefix Length Settings

IPv4 Netmask: 16

IPv6 Prefix Length: 120



Modify Diversion Policy

IPv4 Diversion Netmask Length *: 25

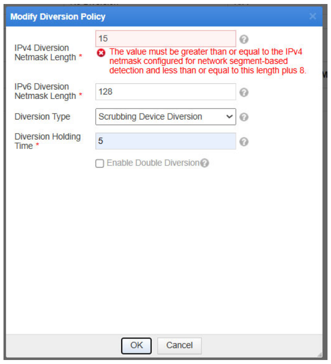
The value must be greater than or equal to the IPv4 netmask configured for network segment-based detection and less than or equal to this length plus 8.

IPv6 Diversion Netmask Length *: 128

Diversion Type: Scrubbing Device Diversion

Diversion Holding Time *: 5

☐ Enable Double Diversion



Modify Diversion Policy

IPv4 Diversion Netmask Length *: 15

The value must be greater than or equal to the IPv4 netmask configured for network segment-based detection and less than or equal to this length plus 8.

IPv6 Diversion Netmask Length *: 128

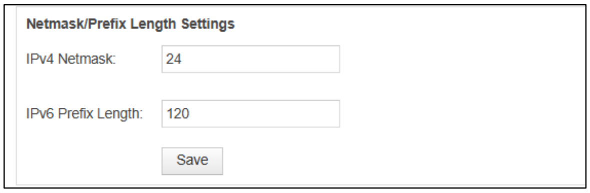
Diversion Type: Scrubbing Device Diversion

Diversion Holding Time *: 5

☐ Enable Double Diversion

- When the network segment-based DDoS detection type is set to **Global**, network segment-specific diversion policies configured under **Configuration > Global Divert Settings > Default Diversion Configuration** take effect.
- When the network segment-based DDoS detection type is set to **Region**, network segment-specific diversion policies configured for a region take effect as long as the related function is enabled for that region.
- When the network segment-based DDoS detection type is set to **IP group**, network segment-specific diversion policies configured for an IP group take effect as long as the related function is enabled for that IP group.

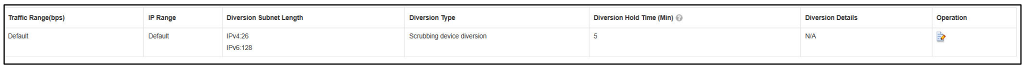
The following uses IPv4 as an example. Assume the IPv4 netmask for DDoS detection is A and the IPv4 netmask for traffic diversion is B. When a network segment-specific DDoS alert is triggered, the actual number of diversion entries issued is 2^(B–A).



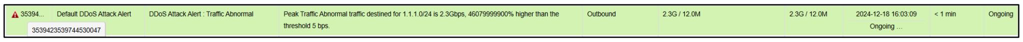
Netmask/Prefix Length Settings

IPv4 Netmask: 24

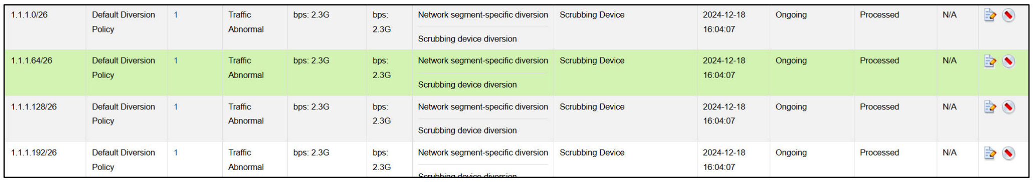
IPv6 Prefix Length: 120



Traffic Range(bps)	IP Range	Diversion Subnet Length	Diversion Type	Diversion Hold Time (Min)	Diversion Details	Operation
Default	Default	IPv4:26 IPv6:128	Scrubbing device diversion	5	N/A	✎



▲ 35394... 3539423539744530047	Default DDoS Attack Alert	DDoS Attack Alert : Traffic Abnormal	Peak Traffic Abnormal traffic destined for 1.1.1.0/24 is 2.3Gbps, 46079999900% higher than the threshold 5 bps.	Outbound	2.3G / 12.0M	2.3G / 12.0M	2024-12-18 16:03:09 Ongoing ...	< 1 min	Ongoing



1.1.1.0/26	Default Diversion Policy	1	Traffic Abnormal	bps: 2.3G	bps: 2.3G	Network segment-specific diversion Scrubbing device diversion	Scrubbing Device	2024-12-18 16:04:07	Ongoing	Processed	N/A	✎ ⊘
1.1.1.64/26	Default Diversion Policy	1	Traffic Abnormal	bps: 2.3G	bps: 2.3G	Network segment-specific diversion Scrubbing device diversion	Scrubbing Device	2024-12-18 16:04:07	Ongoing	Processed	N/A	✎ ⊘
1.1.1.128/26	Default Diversion Policy	1	Traffic Abnormal	bps: 2.3G	bps: 2.3G	Network segment-specific diversion Scrubbing device diversion	Scrubbing Device	2024-12-18 16:04:07	Ongoing	Processed	N/A	✎ ⊘
1.1.1.192/26	Default Diversion Policy	1	Traffic Abnormal	bps: 2.3G	bps: 2.3G	Network segment-specific diversion Scrubbing device diversion	Scrubbing Device	2024-12-18 16:04:07	Ongoing	Processed	N/A	✎ ⊘

Considering the system performance of NTA, the number of BGP/null-route diversion entries is limited to 5000 and that of ADS diversion entries is limited to 2000.

4.3 Sending of Power Status Information via SNMP

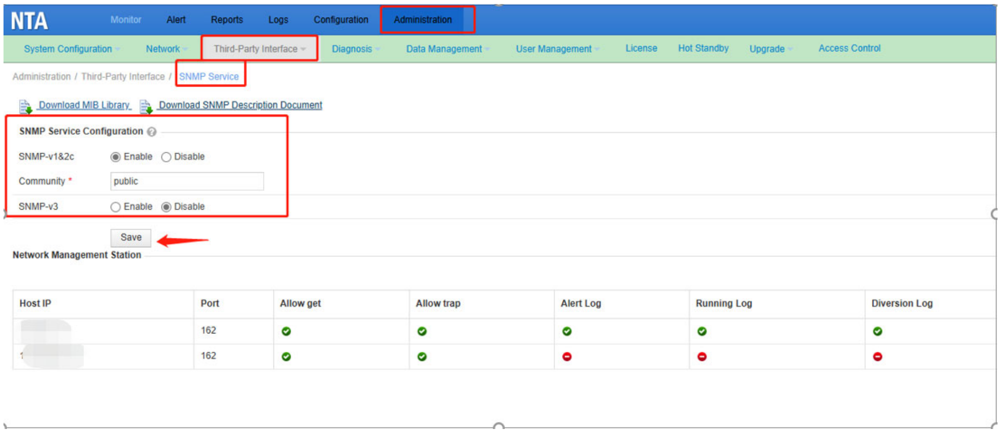
Overview

The status of dual power supplies is added as a new field in SNMP GET messages about device performance. The OID is 1.3.6.1.4.19849.4.6.2.7.0. The return values and meanings are explained as follows:

- **0**: Both are normal (this is the default value returned for a virtual device, which has no physical power supply)
- **1**: Power supply 1 is abnormal.
- **2**: Power supply 2 is abnormal.
- **3**: Both are abnormal.

Configuration and Use

Choose **Administration > Third-Party Interface > SNMP Service**, enable a desired version of SNMP, and click **Save**.



SNMP Service Configuration

SNMP-v1&2c ● Enable ○ Disable

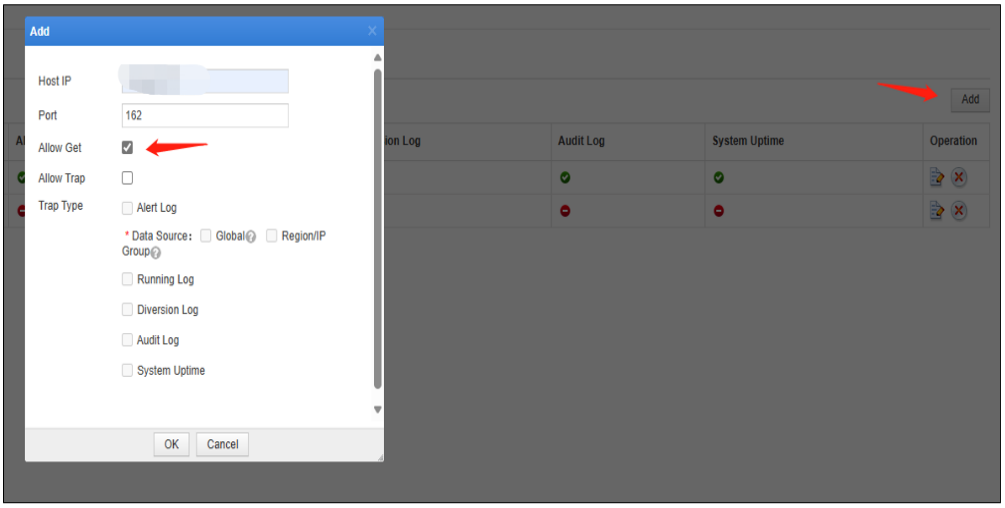
Community * public

SNMP-v3 ○ Enable ● Disable

Network Management Station

Host IP	Port	Allow get	Allow trap	Alert Log	Running Log	Diversion Log
[redacted]	162	✓	✓	✓	✓	✓
[redacted]	162	✓	✓	⊖	⊖	⊖

In the **Network Management Station** area, click **Add**, configure the host IP and port, select the **Allow Get** check box.


Add

Host IP [redacted]

Port 162

Allow Get ☑

Allow Trap □

Trap Type
□ Alert Log
* Data Source: □ Global □ Region/IP Group
□ Running Log
□ Diversion Log
□ Audit Log
□ System Uptime

OK Cancel

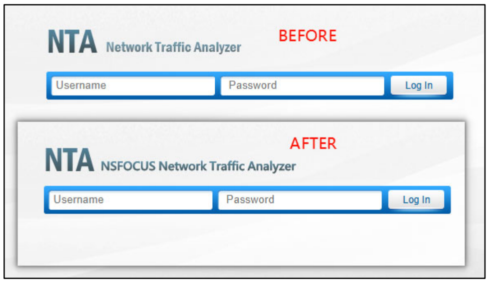
4.4 "NSFOCUS" Added Before the Product Name on the Login Page

Overview

In line with NSFOCUS's NFR requirements for major versions of non-OEM and non-customized devices, "NSFOCUS" is added before the product name on the login page.

Configuration and Use

No need for configuration.


NTA Network Traffic Analyzer
BEFORE
Username
Password
Log In
NTA NSFOCUS Network Traffic Analyzer
AFTER
Username
Password
Log In

4.5 Adaptation of Third-Party Interfaces

Overview

To adapt to the new function of network segment-based DDoS detection for regions, IP groups, and the global scope, the **Administration > Third-Party Interface** module now supports sending of network segment-specific alert and diversion messages via email/SNMP/syslog/SFTP and to a cloud cleaning platform and management platform.

In addition, for collaboration with ADS M, bps traffic statistics of interfaces are optimized. For collaboration with ADBOS, alerts on built-in attack types can be reported and DDoS alerts reported to ADBOS provide more information, namely top 10 ports, top 10 router interfaces, and top 10 packet lengths.

Configuration and Use

To adapt to network segment-specific DDoS alert types, the **netmask** field is added to alerts sent via email, SNMP, syslog (including syslog messages sent to the cloud cleaning platform), and SFTP to indicate a network segment-specific alert. For other DDoS attacks, this field has a fixed value. The following table lists the field values for each type of DDoS alert.

For the cloud cleaning platform and management platform, the destination IP address in network segment-specific DDoS alerts should be in CIDR notation like 1.2.3.0/24.

Alert Type	Value of the netmask Field
IP address-specific DDoS alert	32 (IPv4) or 128 (IPv6)
Network segment-specific DDoS alert	16–30 (IPv4) or 64–126 (IPv6)
Traffic abnormal alert (non-syslog)	Invalid field, with **0** as the default value
Traffic abnormal alert (syslog)	32 (IPv4) or 128 (IPv6)
TI-triggered alert	32 (IPv4) or 128 (IPv6)
Custom featured traffic alert	32 (IPv4) or 128 (IPv6)
Router interface bandwidth alert	Invalid field, with **0** as the default value
Router performance alert	Invalid field, with **0** as the default value
Router data acquisition abnormal alert	Invalid field, with **0** as the default value
System performance alert	Invalid field, with **0** as the default value

Network segment-specific diversion is added for diversion of attack traffic destined for a network segment upon a related alert being triggered.

1.1 NPAI Interface Upgrade

Overview

The NPAI interface has been upgraded to 3. 2. 0. 91240919.

5. Fixed Bugs

1. NTA-12536 [DPI] When HTTP flood traffic initiated by xddos exceeds the SYN flood threshold and triggers a related alert, no HTTP flood alert is reported.
2. NTA-12488 [A device produced in the production center cannot have port 50022 opened for SSH access] Port 50022 cannot be used for SSH access on the web-based manager.

3. NTA-11666 [HTTP slow attack] A link to NTI is provided (not removed as expected) in the source IP information of HTTP slow attack alerts.
4. NTA-12539: After password strength checking is enabled, the password error message displayed for an invalid password does not provide complete information of special characters.
5. NTA-12537: Resetting access control settings does not work after the settings are configured and saved.
6. NTA-11906 [Cloud-side authentication] After manual selection of cloud-side authentication and the authorization status changes from unauthorized to authorized, a message is displayed, providing information different from what has actually happened.
7. NTA-11655 [Logo] The product logo is missing in the upper-left corner of pages of the web-based manager.
8. NTA-13117: When configuring BGP FlowSpec settings, users can set passwords although the **Encryption** check box is cleared.

6. Upgrade Procedure

Note: You must perform the 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 > Upgrade > System Software Upgrade**.

Step 2 Browse to **update_nta_x86_V4.5R90F06.241220build50693.bin** and click **Upload**.

Step 3 Read release notes and, if nothing is wrong, click **Confirm Upgrade** to start the upgrade.

Step 4 Wait about 5 minutes and then 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 **V4.5R90F06.241220build50693**, the upgrade succeeded. If not, the upgrade failed and you need to contact NSFOCUS technical support for help.

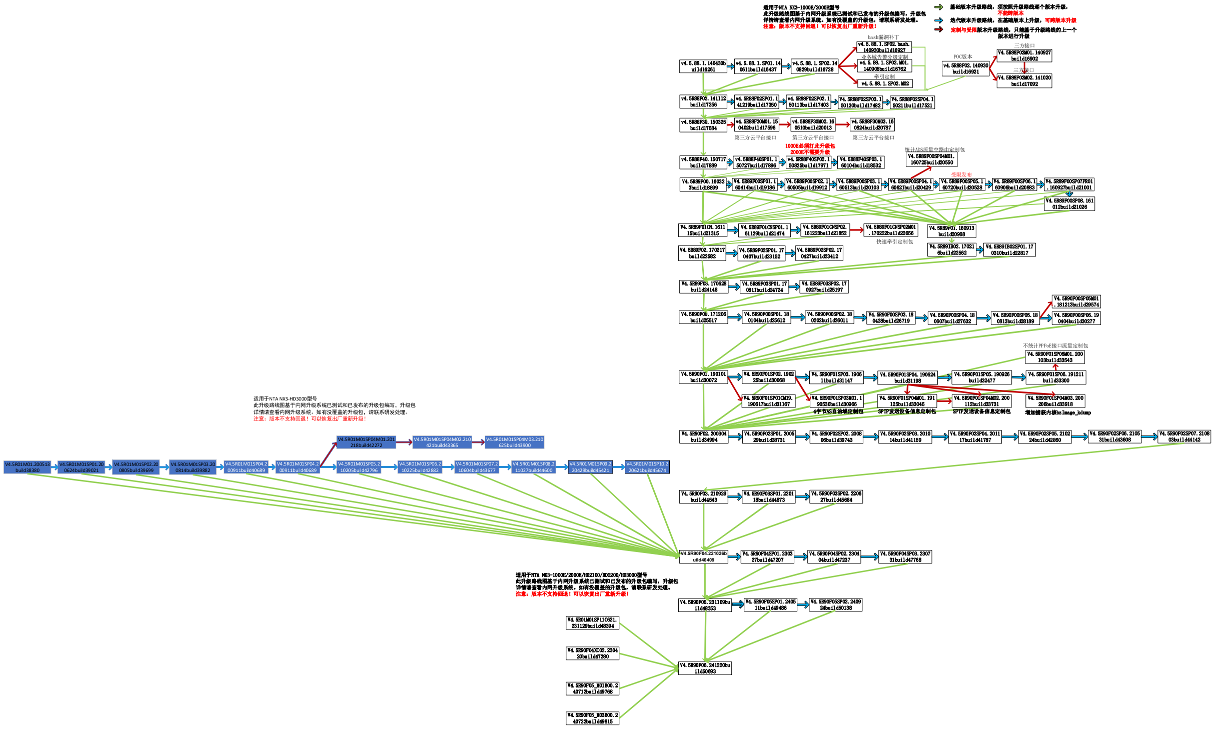
----End

It is normal that the following situations arise in the upgrade process:

- 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 five minutes, you need to manually refresh the page.

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

7. Upgrade Path



适用于NTA NX3-1000E/2000E型号
此升级路线图基于内网升级系统已测试和已发布的升级包编写，升级包详情请查看内网升级系统。如有没覆盖的升级包，请联系研发处理。
注意：版本不支持回退！可以恢复出厂重新升级！

基础版本升级路线，须按照升级路线逐个版本升级，不能跨版本

迭代版本升级路线，在基础版本上升级，可跨版本升级

定制与受限版本升级路线，只能基于升级路线的上一个版本进行升级

适用于NTA NX3-HD3000型号
此升级路线图基于内网升级系统已测试和已发布的升级包编写，升级包详情请查看内网升级系统。如有没覆盖的升级包，请联系研发处理。
注意：版本不支持回退！可以恢复出厂重新升级！

适用于NTA NX3-1000E/2000E/HD2100/HD2200/HD3000型号
此升级路线图基于内网升级系统已测试和已发布的升级包编写，升级包详情请查看内网升级系统。如有没覆盖的升级包，请联系研发处理。
注意：版本不支持回退！可以恢复出厂重新升级！

bash漏洞补丁
v4.5.88.1.140430build16261
v4.5.88.1.SP01.140611build16437
v4.5.88.1.SP02.140829build16728
v4.5.88.1.SP02.bash.140930build16927
业务域告警分级定制
v4.5.88.1.SP02.M01.140905build16762
牵引定制
v4.5.88.1.SP02.M02
POC版本
v4.5R88F02.140930build16921
三方接口
V4.5R88F02M01.140927build16902
三方接口
V4.5R88F02M02.141020build17092
v4.5R88F02.141112build17256
v4.5R88F02SP01.141219build17350
v4.5R88F02SP02.150113build17403
V4.5R88F02SP03.150130build17482
V4.5R88F02SP04.150211build17521
v4.5R88F30.150325build17584
v4.5R88F30M01.150402build17596
v4.5R88F30M02.160510build20013
v4.5R88F30M03.160824build20787
第三方云平台接口
第三方云平台接口
第三方云平台接口
1000E必须打此升级包
2000E不需要升级
v4.5R88F40.150717build17889
v4.5R88F40SP01.150727build17896
v4.5R88F40SP02.150825build17971
V4.5R88F40SP03.160104build18532
统计ADS流量空路由定制包
V4.5R89F00SP04M01.160725build20550
受限发布
V4.5R89F00.160323build18899
V4.5R89F00SP01.160414build19186
V4.5R89F00SP02.160505build19912
V4.5R89F00SP03.160513build20103
V4.5R89F00SP04.160621build20429
V4.5R89F00SP05.160720build20528
V4.5R89F00SP06.160906build20883
V4.5R89F00SP07PR01.160927build21001
V4.5R89F00SP08.161012build21026
V4.5R89F01CN.161115build21315
V4.5R89F01CNSP01.161129build21474
V4.5R89F01CNSP02.161223build21852
V4.5R89F01CNSP02M01.170222build22656
快速牵引定制包
V4.5R89F01.160913build20968
V4.5R89IB02.170216build22562
V4.5R89IB02SP01.170310build22817
V4.5R89F02.170217build22582
V4.5R89F02SP01.170407build23152
V4.5R89F02SP02.170427build23412
V4.5R89F03.170628build24148
V4.5R89F03SP01.170811build24724
V4.5R89F03SP02.170927build25197
V4.5R90F00SP05M01.181213build29574
V4.5R90F00.171206build25517
V4.5R90F00SP01.180104build25612
V4.5R90F00SP02.180202build26011
V4.5R90F00SP03.180428build26719
V4.5R90F00SP04.180607build27632
V4.5R90F00SP05.180813build28189
V4.5R90F00SP06.190404build30277
不统计PPPoE接口流量定制包
V4.5R90F01SP06M01.200103build33543
V4.5R90F01.190101build30072
V4.5R90F01SP02.190225build30068
V4.5R90F01SP03.190611build31147
V4.5R90F01SP04.190624build31198
V4.5R90F01SP05.190926build32477
V4.5R90F01SP06.191211build33300
V4.5R90F01SP01CM19.190617build31167
V4.5R90F01SP03M01.190530build30966
4字节AS自治域定制包
V4.5R90F01SP04M01.191125build33045
SFTP发送设备信息定制包
V4.5R90F01SP04M02.200112build33731
SFTP发送设备信息定制包
V4.5R90F01SP04M03.200206build33918
增加捕获内核bzImage_kdump
V4.5R90F02.200304build34994
V4.5R90F02SP01.200529build38731
V4.5R90F02SP02.200806build39743
V4.5R90F02SP03.201014build41159
V4.5R90F02SP04.201117build41787
V4.5R90F02SP05.210224build42860
V4.5R90F02SP06.210531build43608
V4.5R90F02SP07.210803build44142
V4.5R01M01SP04M01.201218build42272
V4.5R01M01SP04M02.210421build43365
V4.5R01M01SP04M03.210625build43900
V4.5R01M01.200513build38380
V4.5R01M01SP01.200624build39021
V4.5R01M01SP02.200805build39699
V4.5R01M01SP03.200814build39882
V4.5R01M01SP04.200911build40689
V4.5R01M01SP04.200911build40689
V4.5R01M01SP05.210205build42796
V4.5R01M01SP06.210225build42882
V4.5R01M01SP07.210604build43677
V4.5R01M01SP08.211027build44600
V4.5R01M01SP09.220429build45421
V4.5R01M01SP10.220621build45674
V4.5R90F03.210929build44543
V4.5R90F03SP01.220118build44873
V4.5R90F03SP02.220627build45684
V4.5R90F04.221026build46408
V4.5R90F04SP01.230327build47207
V4.5R90F04SP02.230404build47237
V4.5R90F04SP03.230731build47768
V4.5R90F05.231109build48353
V4.5R90F05SP01.240511build49486
V4.5R90F05SP02.240924build50138
V4.5R01M01SP11C621.231129build48394
V4.5R90F04XC02.230420build47280
V4.5R90F05_M01B00.240712build49768
V4.5R90F05_M03B00.240722build49815
V4.5R90F06.241220build50693