

Huawei Technical Proposal

For Anti-DDoS Project

Prepared by Chenjia 00273721 Date:2019/09



HUAWEI

Huawei Technologies Co., Ltd.

All rights reserved

Copyright © Huawei Technologies Co., Ltd. 2013. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://www.huawei.com>

Index

1 Huawei's understanding of XX's Requirements.....	1
2 Huawei Proposed Solution for XX.....	2
2.1 XX Network Topology	2
2.2 Huawei Proposed Anti-DDoS Solution.....	3
2.3 Main Proposed Products and Quantity	5
2.3.1 Detecting Center	5
2.3.2 Cleaning Center	6
2.3.3 ATIC Management Center	7
3 Huawei Anti-DDoS Solution Details	7
3.1 Working Principle of Huawei Anti-DDoS Solution	7
3.2 Solution Highlights	8
3.2.1 High Availability	8
3.2.2 Easy to Manage.....	10
3.2.3 Additional Free Features	10
3.3 Management System	12
3.3.1 ATIC Management Portal.....	12
3.3.2 ATIC Traffic and Attack Reports.....	16
3.3.3 GenieATM6000 Management Portal	24
4 Anti-DDoS Products Introduction.....	26
4.1 Anti-DDoS8000 Series	27
4.1.1 Anti-DDoS8000 Hardware.....	错误!未定义书签。
4.1.2 Anti-DDoS8000 Software	41
4.2 GenieATM6300.....	42
4.2.1 GenieATM6300 Hardware	42
4.2.2 GenieATM6300 Software	44
4.3 ATIC System	46
4.3.1 ATIC System Architecture	46
4.3.2 ATIC System Hardware Requirements	47
4.3.3 ATIC System Software Requirements.....	48
Acronyms and Abbreviations.....	48
Attachments.....	49

1 Huawei's understanding of XX's Requirements

Huawei is pleased to propose Anti-DDoS solution for XX. We really appreciate the opportunities of sharing our industry leading software & hardware technologies, professional services, world-wide deployment experiences, and our visions & commitments with XX. Lately, Huawei has become the industry leading telecom solution supplier. We have successful records of large IP project delivery in 33 of TOP50 telecom operators in the world, including tier-1 operators in Europe like Telefónica, France Telecom, Deutsch Telekom, Vodafone, British Telecom, KPN, TeliaSonera, SFR and etc. We believe that our solution and product portfolios, massive projects delivery experience, fast response to customers' needs, and healthy company finance, can uniquely position Huawei as best partner for XX.

The objective of this response document is to outline Huawei proposed solution, our capability and commitment. We are looking forward to close relationship with XX and working together to develop a customized solution to fulfill XX future network and business needs.

//The words in blue fonts of this document should be modified based on actual projects, while //the words in normal black fonts may be kept unchanged.

//Describe Huawei's understanding of customer's requirements. Summarize the key //requirements. For example:

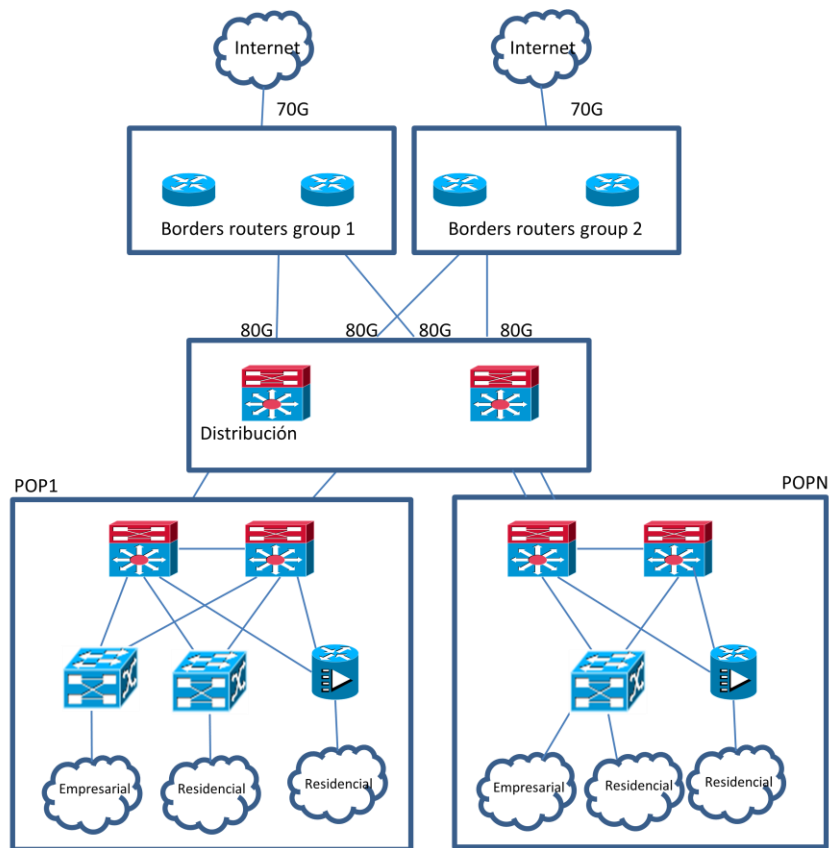
After discussing with MVI, Huawei understand that MVI want to deploy Anti-DDoS solution to protect its internal network from the increasing DDoS attack threats. The solution should be high capacity, easy to expansion, high availability.

2 Huawei Proposed Solution for XX

2.1 XX Network Topology

//This chapter describes the customer's network topology.

//For example:

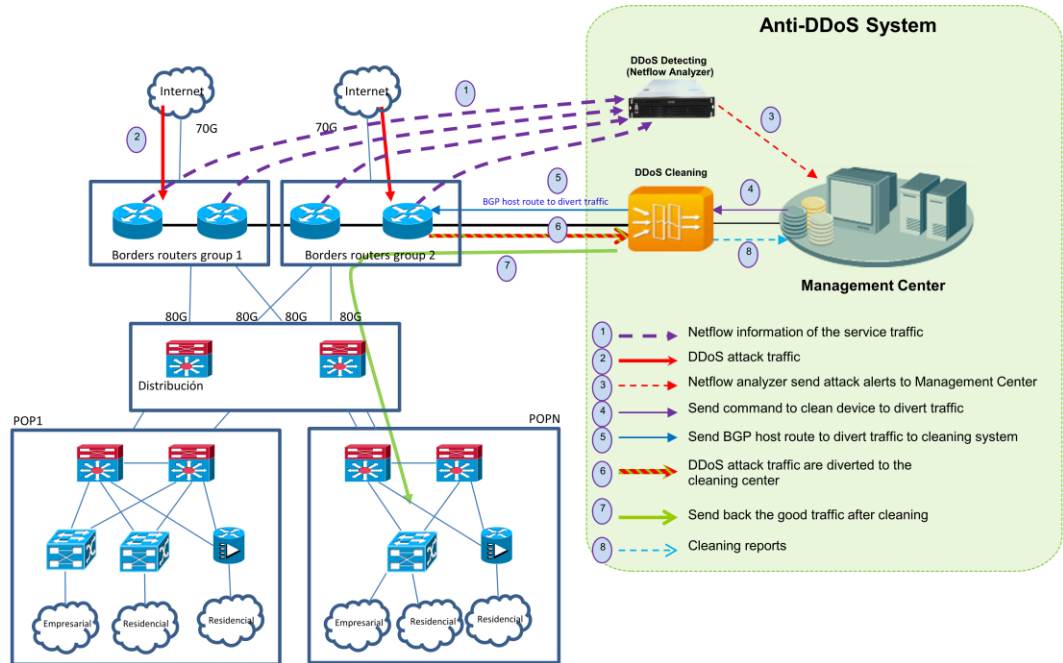


MVI's network are mainly comprised of 4 x border routers (connecting to the other Internet Service Providers), 2 x distribution routers (connecting to Border networks and POPs) and several POPs (connecting to subscribers). The total traffic bandwidth of internet connection is 70Gbps.

2.2 Huawei Proposed Anti-DDoS Solution

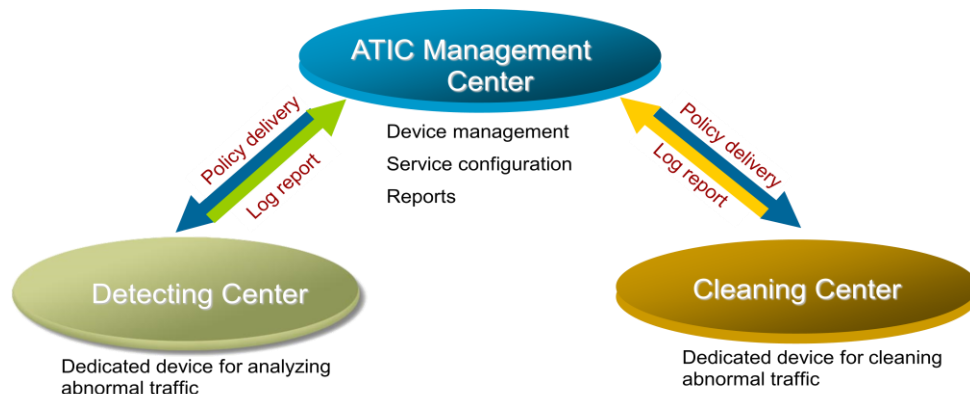
//This chapter describes the Huawei Anti-DDoS solution for XX customer.

//For example:



Based on the capacity and performance requirements of the MVI network, Huawei propose Anti-DDoS8080, deploy in off-line mode: collect and analysis the netflow information from the border routers for DDoS attack detecting, and dynamic divert the DDoS attack traffic to cleaning system for cleaning and then send the good traffic back.

The proposed solution contains three main parts: Detecting center, Cleaning center and ATIC (Abnormal Traffic Inspection Center) management center. The logical architecture of the three components is shown in the following figure:



The main functions of the three components are:

- **Detecting Center**

Netflow based detecting center collect netflow information from the network elements such as router and switches, and then summarize and analyze, if DDoS attack happen, detecting center will send syslog alarms to ATIC to do further mitigation. Flow based detecting center supports most of the general DDoS attacks, such as: ICMP Flooding, TCP SYN Flooding, TCP RST Flooding, TCP Flag Null or Misuse, TCP Fragment, UDP Flooding, UDP Fragment, IP Protocol Null, Land Attack, Host Total Traffic.

GenieATM6000 supports following types of netflow information: Cisco NetFlow (v1,v5,v7,v9), sFlow (v2, v4, v5), Huawei NetStream (v5,v9), IPFIX(The IPFIX standards requirements were outlined in the original [RFC 3917](#). Cisco [NetFlow](#) Version 9 was the basis for IPFIX) and cFlowd (supported by Alcatel-Lucent, Juniper, etc)

The netflow traffic bandwidth requirements: $\text{Netflow bandwidth} = \text{Flow rate} / 30 * 1500\text{Bytes} * 8\text{bits}$. For example: 50,000 flow/s, the netflow traffic required bandwidth is: $50,000 / 30 * 1500 * 8 = 20\text{Mbps}$; 20,000 flow/s, the netflow traffic required bandwidth is: $20,000 / 30 * 1500 * 8 = 8\text{Mbps}$.

Note: The number 30 in the above formula means each netflow packet contains 30 flows; the number 1500 means each netflow packet size is 1500 bytes; the number 8 means each bytes contains 8 bits.

- **Cleaning Center**

As the core of Huawei AntiDDoS, the cleaning device mitigates attack traffic on the network. Huawei cleaning device falls into two types, AntiDDoS1000 series and AntiDDoS8000 series. Integrated with Huawei-proprietary traffic cleaning engine, the cleaning device uses the layer-to-layer defense technology, mainstream defense technologies, and lots of Huawei-patented algorithms to cope with heavy-traffic attacks and application-layer attacks.

- **ATIC Management Center**

As a controller, the ATIC (Abnormal Traffic Inspection Center) management center integrates device management, policy management, data analysis, and data collection. Therefore, it delivers user-friendly GUIs and outstanding security analysis capability.

The ATIC management center consists of the ATIC collector and controller. The ATIC collector collects and stores data. The collector analyzes and summarizes data, manages the system in a unified manner, and displays GUIs.

2.3 Main Proposed Products and Quantity

//This chapter describes the Huawei proposed products and quantity, including the //chassis/card/auxiliaries/software/etc. model/type and quantity.

2.3.1 Detecting Center

The flow based detecting center device in Huawei Anti-DDoS solution is GenieATM6000 series. GenieATM6000 is the brand of “Genie Networks”, which is a Taiwan based network company that focuses on network performance and quality analysis. Genie Networks is the partners of Huawei. GenieATM6000 series are composed of three types: Controller, Collector and Load Balancer.

- *Controller provides the management, netflow collection and analysis, and report functions, it supports centrally manage up to 30 collectors to expand the capacity. Controller can works without collector (controller includes collector’s function)*
- *Collector provides the netflow collection and summary, it must be controlled by controller to provide management and report function*
- *Load balancer provides the netflow traffic load balancing function; it is designed for some very large scale network which Controller + Collector architecture cannot provide enough performance capacity.*

GenieATM6365 and 6333 is two special models that customized only for Huawei, their price are less than the related normal models (which provides the same performance). However these two special models have limitations: GenieATM6365 supports to collect netflow traffic from maximum 5 routers, and GenieATM6333 supports to collect netflow traffic from maximum2 routers, all the other function is the same.

GenieATM6365 and 6333also supports centrally manage up to 30 collectors to expand capacity. If some project choose GenieATM6365 or 6333 at the first stage, for the future expansion, can add new collectors.

<i>Device Type</i>	<i>Chassis model and quantity</i>	<i>Capacity</i>	<i>Maximum number of supported routers</i>
--------------------	-----------------------------------	-----------------	--

Detecting(C ontroller)	<i>GenieATM6365</i>	<i>50,000flow/s(equal to 180Gbps)</i>	<i>5</i>
Detecting(C ontroller)	<i>GenieATM6333</i>	<i>20,000flow/s(equal to 72Gbps bandwidth)</i>	<i>2</i>

For other models, please refer to following attached documents (at the end of this document):

“GenieATM Specifications.xlsx”, “GenieATM6000_Datasheet.pdf”.

//For example:

Huawei proposed GenieATM6333 as detecting device for MVI’s network:

Device Type	Chassis model and quantity	Capacity	Maximum number of supported routers
Detecting	<i>GenieATM6333*2</i>	<i>20,000flow/s(72Gbps bandwidth)</i>	<i>2</i>

*Note: 2*GenieATM6333 work in Active-Standby mode.*

2.3.2 Cleaning Center

Huawei Anti-DDoS cleaning device contains three models: Anti-DDoS8030, Anti-DDoS8080 and Anti-DDoS8080. All the software and feature is the same for the three models, the only different is the performance and expansion capability. Anti-DDoS8160 contains sixteen free slots and supports maximum 1440Gbps detecting or cleaning capacity; Anti-DD8080 contains eight free slots and supports maximum 720Gbps detecting or cleaning capacity; Anti-8030 contains three free slots and supports maximum 120Gbps detecting or cleaning capacity.

For example:

Huawei proposed Anti-DDoS8080 as cleaning device for XX’s network:

<i>Device Type</i>	<i>Chassis Model and quantity</i>	<i>Clean board quantity</i>	<i>Current Capacity</i>	<i>Maximum Expansion Capacity</i>
<i>Cleaning Center</i>	<i>Anti-DDoS80 *1</i>	<i>1*160Gbps Clean board</i>	<i>160Gbps</i>	<i>720Gbps</i>

Note: "Maximum Expansion Capacity" means expansion capacity of one chassis, if the actual traffic throughput exceeds the performance of one chassis, should deploy additional chassis.

2.3.3 ATIC Management Center

ATIC management system:

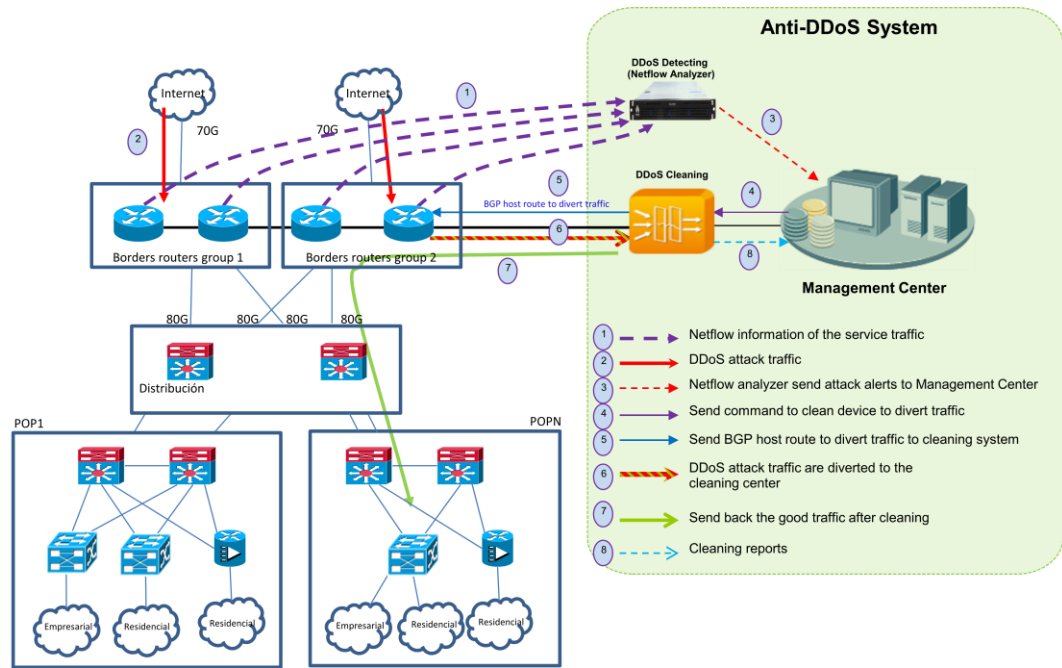
<i>Device Type</i>	<i>Chassis Model and quantity</i>
<i>ATIC</i>	<i>ATIC system *2 (ATIC management software + Hardware server + Windows Server platform software + auxiliaries)</i>

*Note: 2*ATIC system work in Active-Standby mode.*

3 Huawei Anti-DDoS Solution Details

3.1 Working Principle of Huawei Anti-DDoS Solution

Following figure show the working principle of Huawei Anti-DDoS solution:



- 1) The border routers send netflow information of the service traffic to the DDoS detecting center
- 2) DDoS attack traffic comes from internet
- 3) Detecting center detects DDoS attacks, sends DDoS attack alarms to ATIC
- 4) ATIC send traffic divert commands to Cleaning center
- 5) Cleaning center sends BGP divert route to the adjacent router, this route will divert all traffic that are going to the victim destination (including DDoS attack traffic and normal good traffic) to the cleaning center
- 6) All traffic that are going to the victim destination (including DDoS attack traffic and normal good traffic) are diverted to the Cleaning center for cleaning; Cleaning center starts clean the DDoS attack traffic
- 7) After cleaned the attack traffic, the Cleaning center sends the good legitimate traffic back to its original destination.
- 8) Detecting and cleaning center send detect and clean log to ATIC system.

3.2 Solution Highlights

3.2.1 High Availability

1. Product High Availability

Anti-DDoS8000:

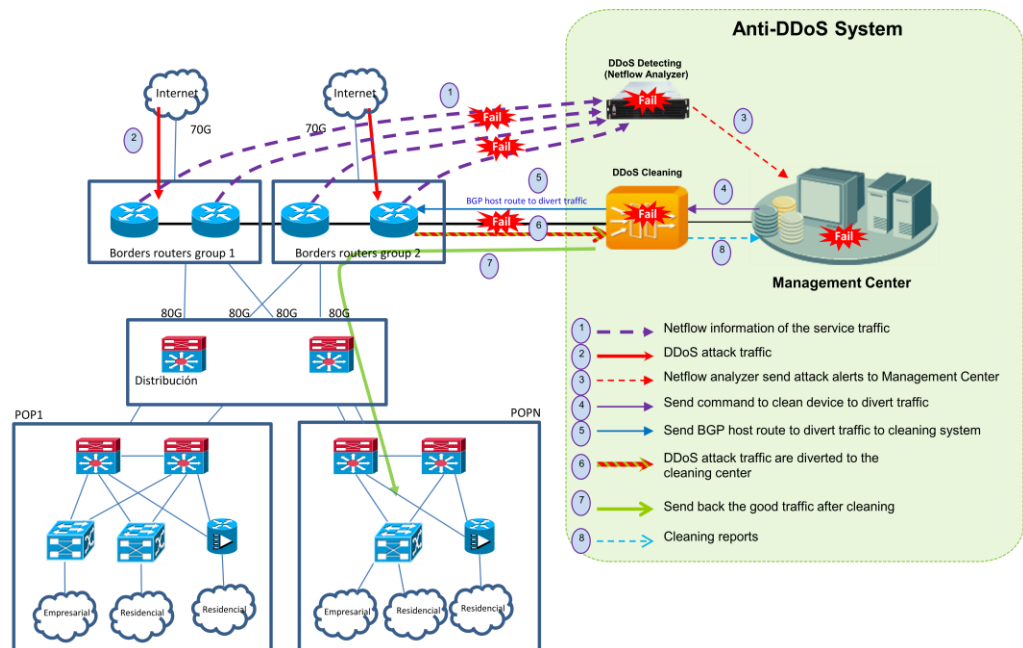
Huawei Anti-DDoS8000 share the same hardware platform of Huawei NE series routers and Huawei mature VRP software platform, they provide carrier level high availability, the NE-X series hardware and VRP software platform have been successfully commercial deployed at many carrier's network worldwide for many years.

GenieATM6000:

Power Redundancy : Hot Swappable Redundant Power Supply

System Redundancy : Master controller and Hot Standby controller through VRRP protocol

2. Solution Architecture High Availability



Huawei Anti-DDoS solution adopts off-line deployment mode and dynamic traffic divert and re-injection, any part of the solution's failure does not impact the user network's original service traffic.

For example, if the detecting link or device fails, the system will not detect the DDoS traffic and will not send divert route to the adjacent router, the original traffic will not be impacted;

If the cleaning link or device fails, although the detecting center can detect DDoS attack, ATIC send divert commands to cleaning center, but cleaning center cannot send divert route to the adjacent router, the original traffic will be not impacted;

If the ATIC link or device fails, although the detecting center can detect DDoS attack, ATIC cannot send divert commands to cleaning center, the cleaning center will not send divert route to the adjacent router, the original traffic will be not impacted.

If any part of the solution fails, it will send alarms to the network management system, so the network administrator can begin to fix the problem.

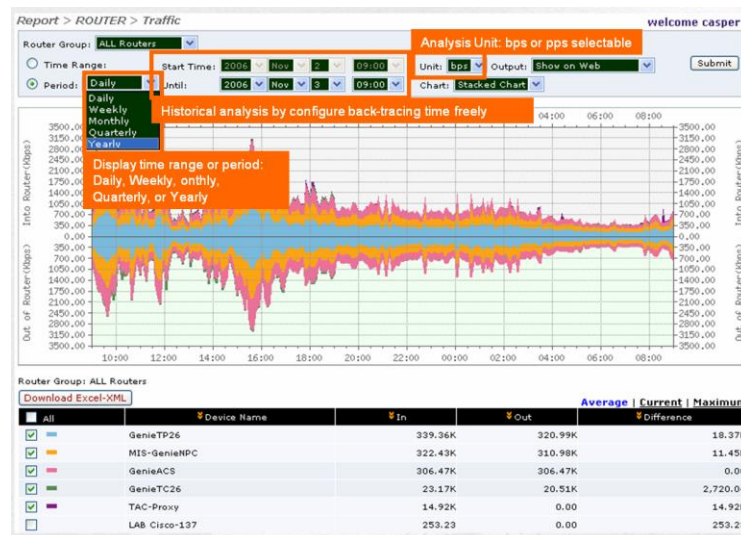
3.2.2 Easy to Manage

The AntiDDoS offers an intelligent traffic baseline learning system to free the administrator from configuring the threshold. To ease management and maintenance, Huawei proposes the easy-to-use GUIs as well as the excellent ATIC management system, which integrates device management, policy configuration, data collection, data analysis, alarm management, and operation support.

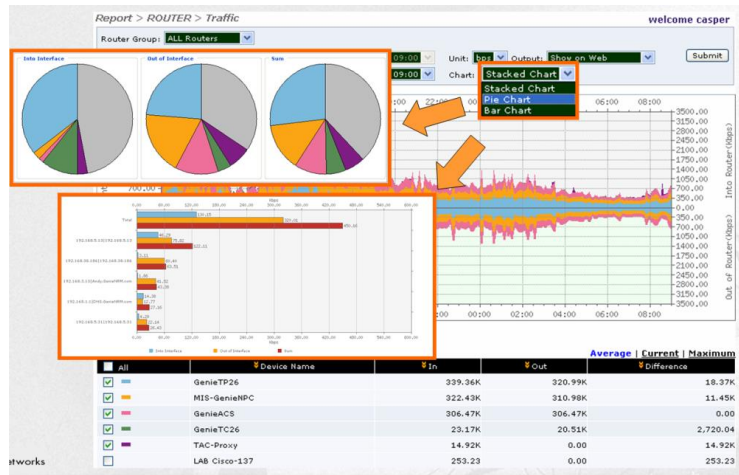
3.2.3 Additional Free Features

Besides the DDoS detection functions, GenieATM6000 also support rich traffic monitoring and analysis features, all these features are free of charge, no additional fees are needed.

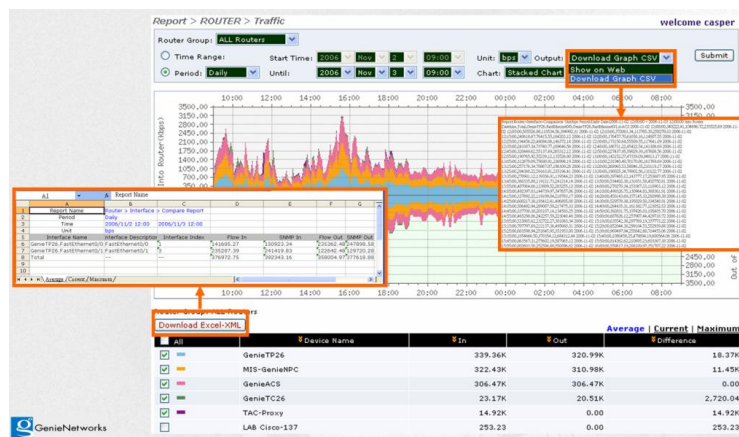
Historical Traffic Graphical Reports



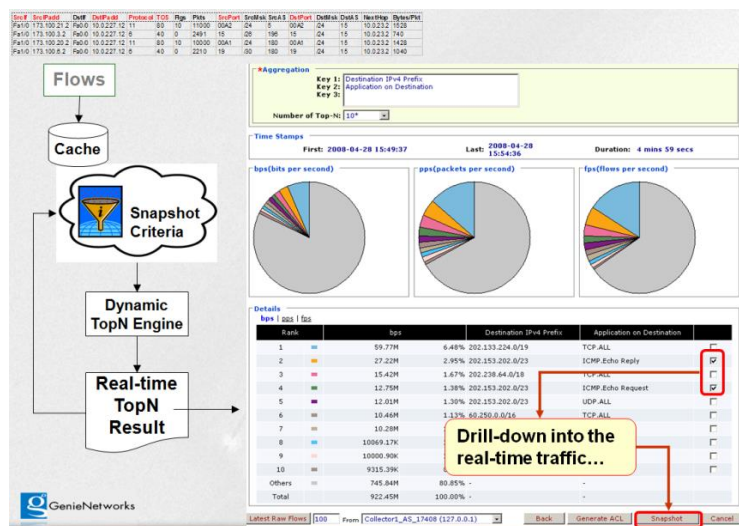
Optional Pie Chart and Bar Chart



Support export excel format detail data or CSV format raw data for further analysis



On-line Troubleshooting and Traffic Snapshot Tool



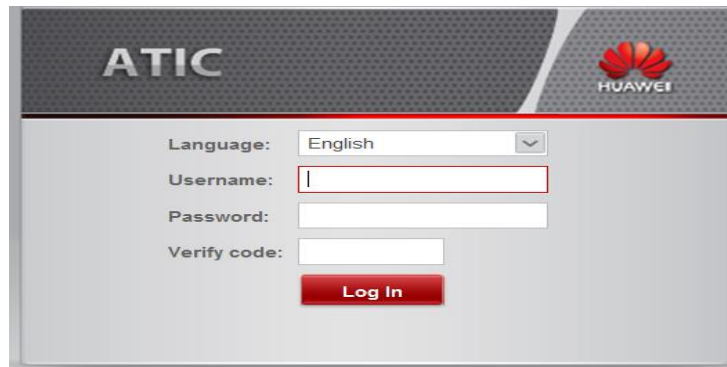
Note: For more detail information of GenieATM traffic analysis functions, please refer to attached documents “GenieATM6000_Datasheet.pdf”.

3.3 Management System

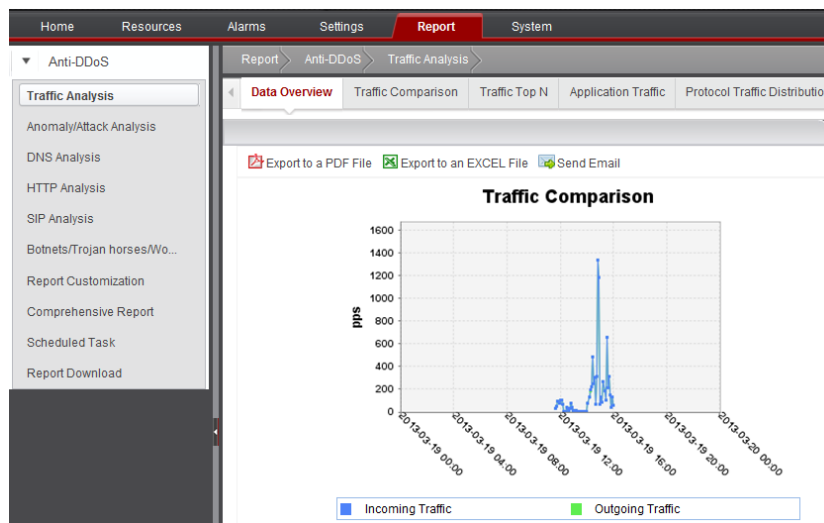
Huawei Anti-DDoS solution provides user friendly GUI management portal and powerful reports.

3.3.1 ATIC Management Portal

- Login portal



- Home page



- System configuration

- **Policy configuration**

Step1: Auto Configure Zone

Zone	Type	NE Name	Service Learning	Baseline Learning	State	Defense State	Diversion State	Deployment State	Operation
DefaultZone2_2_10_201	Default	AntiDDoS8000	Not learned	Not learned	Abnormal	Automatically Defended	Not diverted	Deploy Succeed	[Icon]
DefaultZone2_2_10_200	Default	AntiDDoS1000	Not learned	Not learned	Normal	-	Not diverted	Deploy Succeed	[Icon]

Step2: Click Operation column item to see Policy

Basic Policy | Filter | Defense Policy

Traffic Diversion Mode : Automatic Manual ?

Defense Mode : Automatic Manual ?

Dynamic Blacklist Mode : Automatic Close ?

Cleaning Bandwidth : Enable Threshold (Mbit/s) : (1-10240) ?

Traffic Limiting for Single IP Address : Enable Threshold (Mbit/s) : (1-10240) ?

Step3: Click State column item (e.g. Abnormal) to see event

IP Address	NE Name	Anti-DDoS	Anomaly Start Time	Attack Type	Threshold	Actual Value	Number of Attacks	State	Defense Action
3.3.10.6	AntiDDoS8000	Cleaning	2013-04-09 17:50:19	Other Flood Attack	1024kbps	1469kbps	0	Abnormal	Automaticall...
3.3.10.7	AntiDDoS8000	Cleaning	2013-04-09 17:58:25	Other Flood Attack	1024kbps	154kbps	0	Abnormal	Automaticall...
3.3.10.10	AntiDDoS8000	Cleaning	2013-04-09 17:52:10	Other Flood Attack	1024kbps	1306kbps	0	Abnormal	Automaticall...
3.3.10.11	AntiDDoS8000	Cleaning	2013-04-09 17:54:50	Other Flood Attack	1024kbps	1306kbps	0	Abnormal	Automaticall...

Attack defense configuration example:

TCP attack defense configuration: Page1/4

Configure Service

Basic Information | **TCP Defense** | UDP Defense | ICMP Defense | Other Defense | DNS Defense | SIP Defense | HTTP Def...

Block

Traffic Limiting

Defense

TCP Abnormal Defense
 Threshold (pps) : (1-1200000)

TCP Basic Defense

SYN Flood Attack Defense
 Threshold (pps) : (1-1200000)

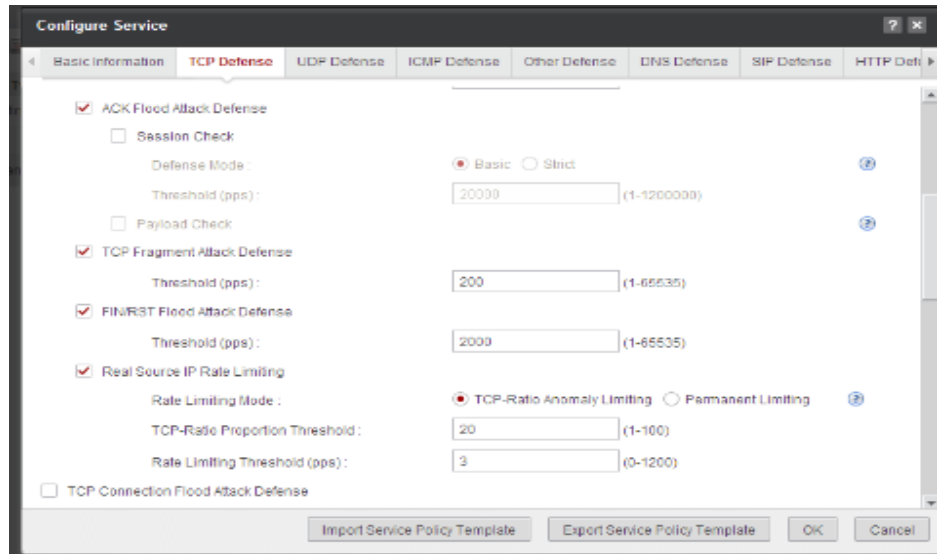
SYN-ACK Flood Attack Defense
 Threshold (pps) : (1-1200000)

ACK Flood Attack Defense

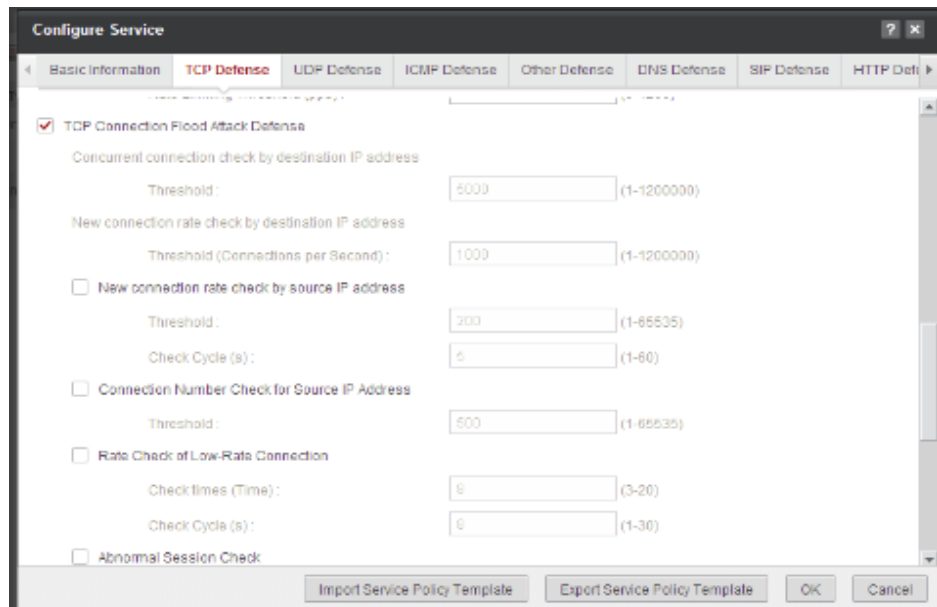
Session Check

Import Service Policy Template | Export Service Policy Template | OK | Cancel

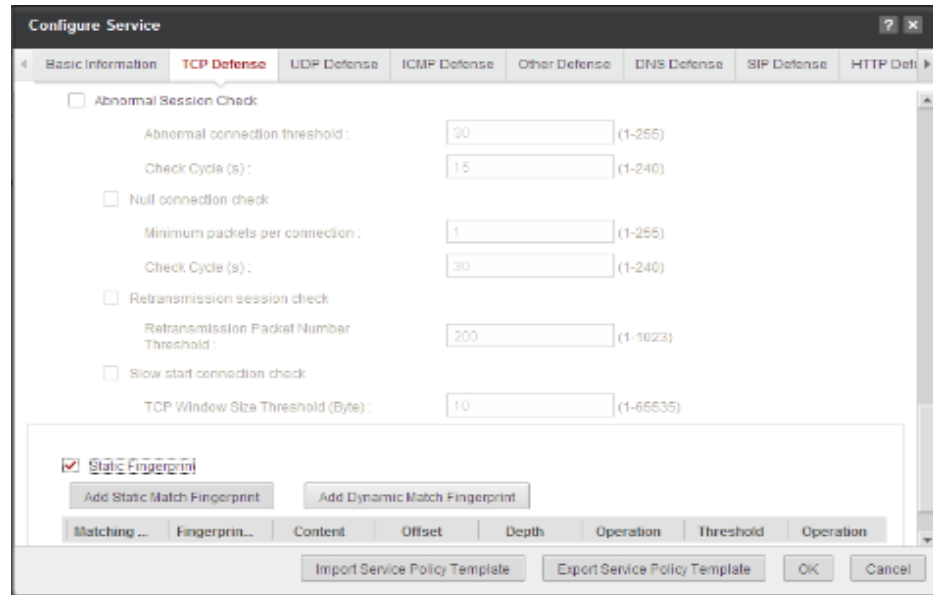
Page2/4



Page3/4



Page4/4



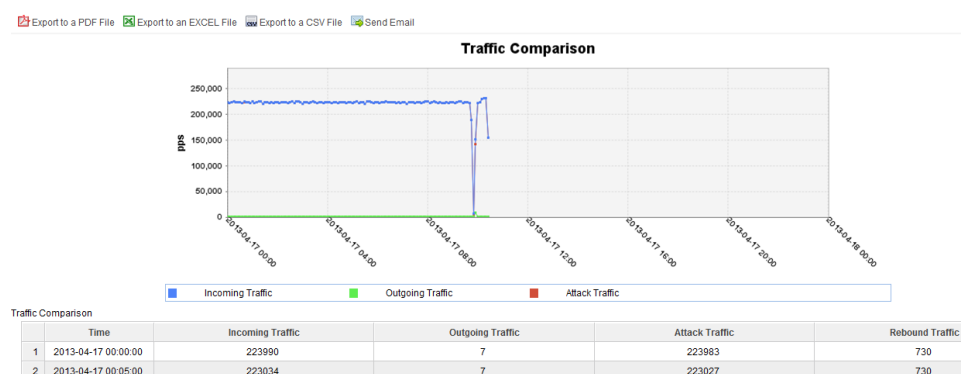
3.3.2 ATIC Traffic and Attack Reports

Reports are used to analyze network traffic and attack logs and summarize system and Zone traffic information and attack logs periodically.

The ATIC management center provides four types of analysis: traffic analysis, abnormality/attack analysis, DNS analysis, and botnet/Trojan horse/worm analysis. This analysis helps the administrator comprehensively learn about network data in real time. The ATIC management center also provides system and Zone reports in diversified forms. The reports can be generated periodically. This function is labor-saving and facilitates network status monitoring and query.

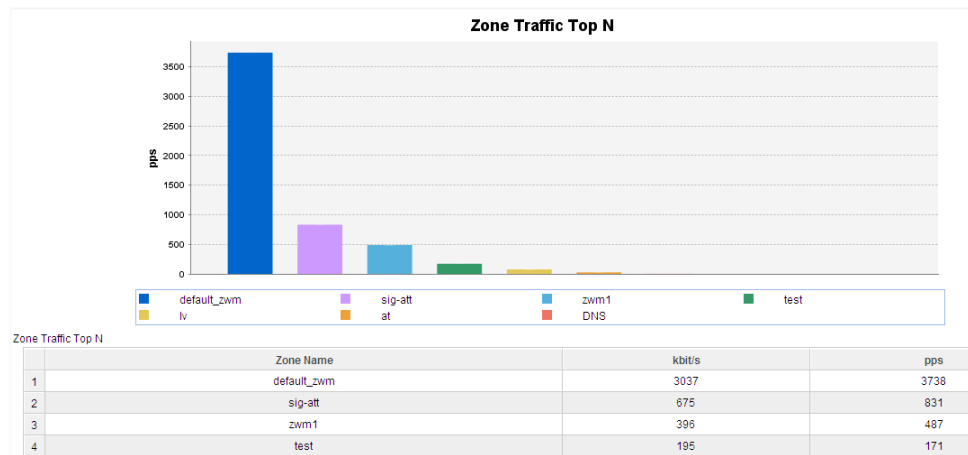
- **General Traffic Analysis**

- 1) **Traffic comparison**



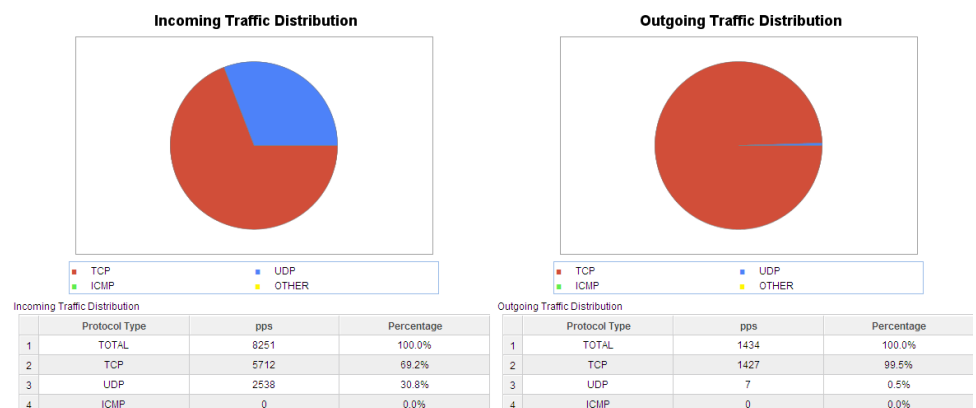
The traffic comparison report displays traffic comparisons and changes of an Anti-DDoS device, Zone, or IP address within a period of time. If the device is an anti-DDoS cleaning device, you can view the incoming, and outgoing traffic. If the device is an anti-DDoS detecting device, you can view the detected traffic.

2) Traffic Top N

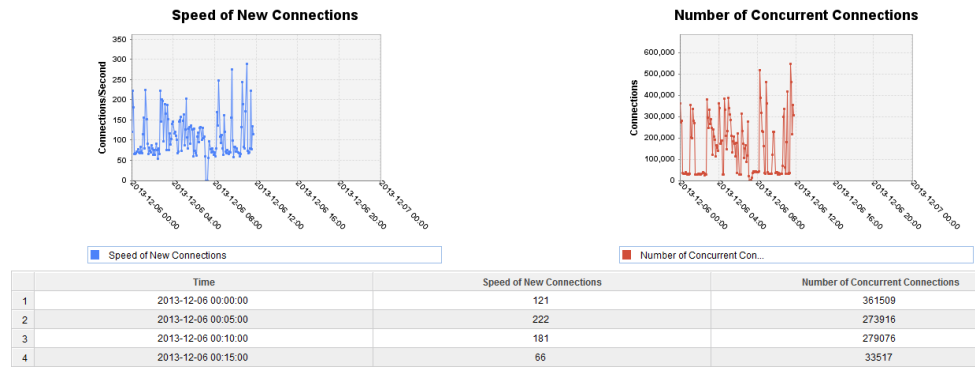


The ATIC management center collects statistics on Incoming Traffic or Attack Traffic in the specified interval and ranks the top N traffic. From the top N statistics, you can view the top N Zones, services, or IP addresses with the largest volumes of inbound or attack traffic.

3) Protocol traffic distribution

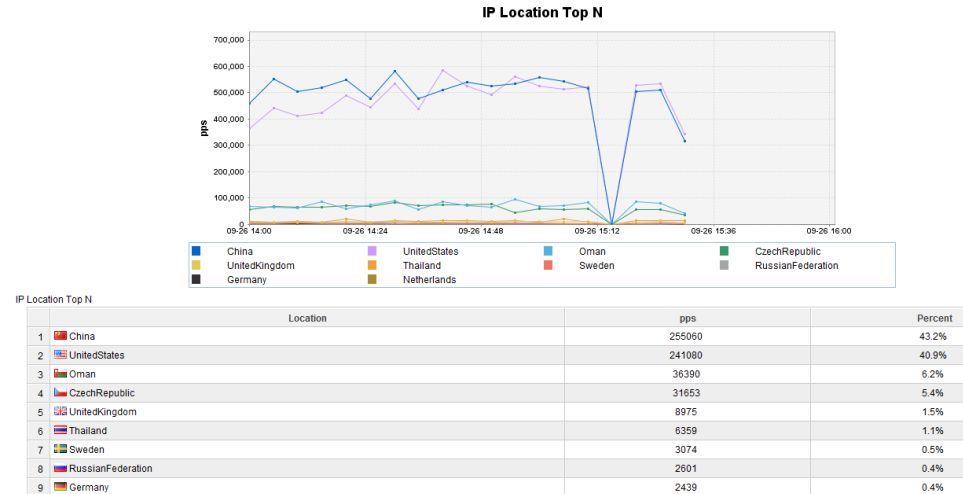


4) Number of new connections and concurrent connections by destination IP address



Number of TCP connections provides visibility into the number of new TCP connections and number of concurrent TCP connections by destination IP address, and number of new connections by source IP address with the most connections. In normal cases, observe and record the number of new connections and that of concurrent connections of services in the report. If the number of new connections or the number of concurrent connections is greater than the normal value, capture packets for analyzing anomalies or attacks.

5) IP Location Top N



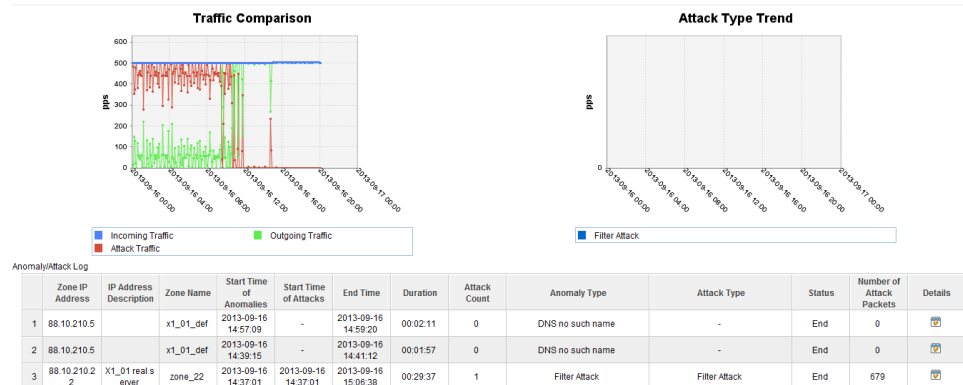
The IP Location Top N report provides visibility into the Top N IP locations that have the maximum volume of incoming or attack traffic.

- **Anomaly Attack Analysis**

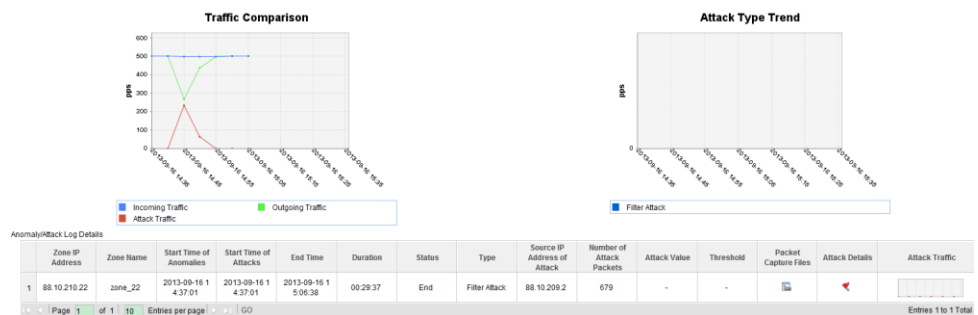
- 1) **Anomaly/Attack Details**

The anomaly/attack details records basic information about all anomalies and attacks, and you can locate anomaly or attack events.

Anomaly/attack Details

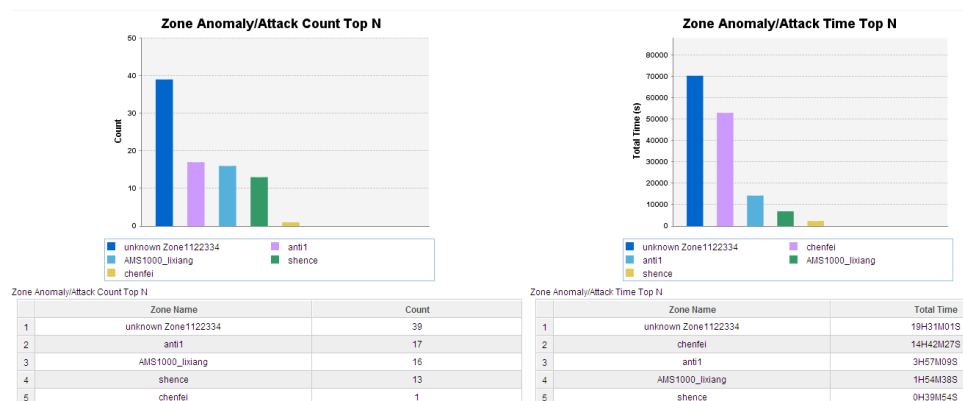


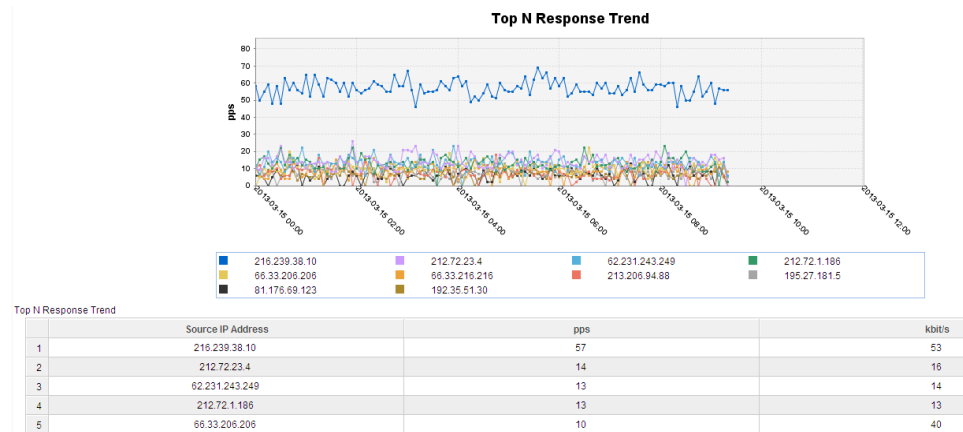
Anomaly/attack Logs Details



2) Anomaly/Attack top N

Zone anomaly/attack top N sorts top N Zones by number or duration of anomalies/attacks.

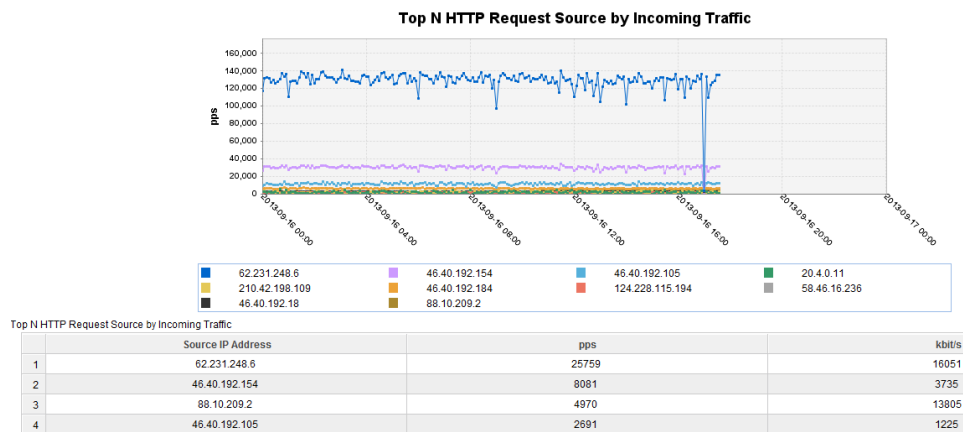




- **HTTP(S) Analysis**

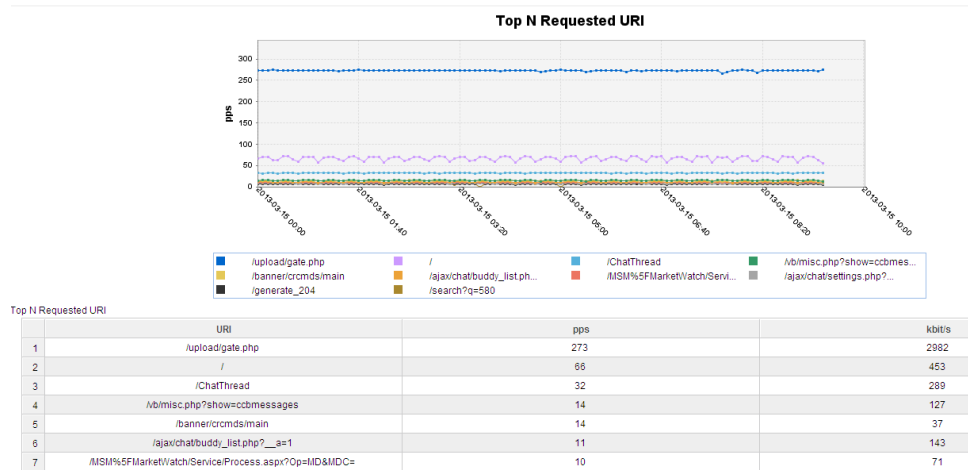
- 1) **Top N HTTP Request Sources by Traffic**

Top N HTTP Source IP Addresses by Traffic Rate is enabled.



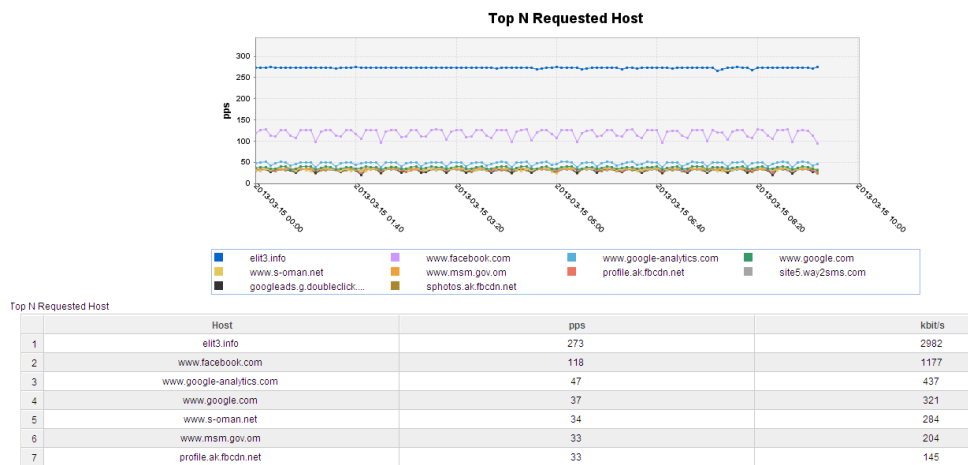
- 2) **Top N Requested URI**

Top N HTTP URIs display top N URI fields in the HTTP traffic destined for the Zone.



3) Top N Requested Host

Top N HTTP host fields display those in the HTTP traffic destined for the Zone.



- **Managing Scheduled Task**

A scheduled task is the task that generates reports periodically within the specified life cycle. It helps the user query synthesis reports and sends the reports to the specified email box periodically.

Meaning of Parameters:

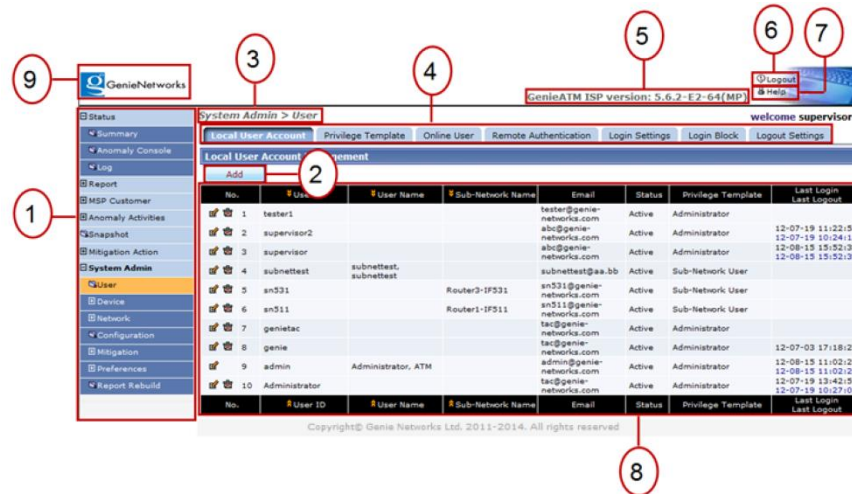
Parameter	Description	Setting
Name	Identifies the name of a task for easy search.	It cannot contain any spaces or characters such as "", " ", "\", ", "<", ">", "&", ";", "''", and "%". The value contains a maximum of 32 characters and cannot start with null .
Plan	Indicates the execution period of the task.	For example, if you set the life cycle from 2010-12-8 00:00:00 to 2011-12-8 23:59:59, and the Plan time for the task to 00:00 on the 8th day of each month, the system generates reports 00:00 on the 8th day of each month from 2010-12-8 00:00:00 to 2011-12-8 23:59:59.
Run Time	Indicates the execution time of the task.	
Life Cycle	Indicates the validity period of a task. The task becomes invalid when it expires.	
Report Format	Indicates the format for exporting the report. Multiple formats are available.	You need to select at least one format.
Description	Indicates the description of a task.	Its length cannot exceed 255 characters.

Notes: For more details of Anti-DDoS configuration and reports, please refer to Anti-DDoS product documents.

3.3.3 GenieATM6000 Management Portal

GenieATM6000 provides DDoS Detection function in Huawei Anti-DDoS solution, normally only need modify the threshold if DDoS attack.

- Overview of GenieATM6000 management portal



1) System Menu Tree

Display the system's main functions. The user can click “+” next to a main function on the system menu tree to unfold the sub-main functions or enter the window of the selected function. To close a sub-menu function, click “-” next to it.

2) Action Buttons

The system provides two types of action buttons: one is in the text-form, such as “Add” and “Edit”; the other is in the icon-form, such as “✎”(Edit) and “✖”(Delete).

3) Menu Path

Menu Path indicates where the current operation page is located. The menu path is relative to the selected item in the System Menu Tree.

4) Sub Menu Tab

Sub Menu Tab provides an individual sub-function under a menu function.

5) System Version

Display the running version of the Controller.

6) Logout Button

Click the Logout button to exit the system. The system will automatically record the login and logout time after the user clicks the button.

7) Online Help

It is a glossary located next to a selected menu path and gives the descriptions of the corresponding function.

8) Configuration View List / Report Area

The configured data or traffic report will be displayed in the view area. The user can click the action buttons to manage the system configuration or query the reports.

9) Default Page Link

If the login user clicks the logo area, it will link to the Status Summary main page (Status > Summary > (Tab) Global).

• **Configure threshold for DDoS attack detection**

1) Configure the network to be detected (defined by network address range)

No.	#ID	Name	IP Space	Boundary Links	Remarks
26	320	Zone_Corp_Packet_Core	permit 80.227.24.0/24	Internet Boundary	
27	319	Zone_Corp_Internet_Link	permit 80.227.0.232/29	Internet Boundary	
28	318	Zone_Corp_OIGI_BBECS	permit 80.227.0.96/28	Internet Boundary	
29	317	Zone_Corp_Emmar_PDC IPTV	permit 65.29.126.0/21	Internet Boundary	
30	316	Zone_Corp_DICCS_PIS_Core	permit 94.201.224.0/24	Internet Boundary	
31	315	Zone_Corp_Emmar_PDC_NAT	permit 80.227.1.0/24	Internet Boundary	
32	314	Zone_Corp_DICCS_EITTC_DNS	permit 80.227.2.0/24 permit 94.200.200.200/32	Internet Boundary	

2) Configure the threshold for each kind of attack

Threshold page layout

System Admin > Network > Anomaly

Protocol-Misuse Anomaly | Application Anomaly | Mitigation

Protocol-Misuse Anomaly Management

Default for Home and User-defined Resources

Severity Latency: 10 min. Recover Latency: 5 min.

No.	ID	Name	Status	Event Threshold	Unit
1	S120010	Protocol-Misuse Anomaly,Host Total Traffic	Enabled Disabled	15	Mbps
2	S120009	Protocol-Misuse Anomaly,UDP Flooding	Enabled Disabled	15	Mbps
3	S120008	Protocol-Misuse Anomaly,TCP RST Flooding	Disabled Enabled	5	Kpps
4	S120007	Protocol-Misuse Anomaly,Land Attack	Disabled Enabled	1	Kpps
5	S120006	Protocol-Misuse Anomaly,ICMP Misuse	Disabled Enabled	256	pps
6	S120005	Protocol-Misuse Anomaly,UDP Fragment	Disabled Enabled	1	Kpps
7	S120004	Protocol-Misuse Anomaly,TCP Fragment	Disabled Enabled	1	Kpps
8	S120003	Protocol-Misuse Anomaly,TCP Flag Null or Misuse	Disabled Enabled	1	Kpps
9	S120002	Protocol-Misuse Anomaly,IP Protocol Null	Disabled Enabled	1	Kpps
10	S120001	Protocol-Misuse Anomaly,TCP SYN Flooding	Disabled Enabled	1	Kpps

Press "Edit" button to modify the thresholds

System Admin > Network > Anomaly

Protocol-Misuse Anomaly | Application Anomaly | Mitigation

Protocol-Misuse Anomaly Management

Default for Home and User-defined Resources

Severity Latency: 10 min. Recover Latency: 5 min.

Minimum severity Latency can be 1 min

welcome Justin

Edit Protocol-Misuse Anomaly: Default for Home and User-defined Resources

Severity Latency: 10 min. Recover Latency: 5 min.

No.	ID	Name	Status	Event Threshold	Unit
1	S120010	Protocol-Misuse Anomaly,Host Total Traffic	Enabled Disabled	15	Mbps
2	S120009	Protocol-Misuse Anomaly,UDP Flooding	Enabled Disabled	15	Mbps
3	S120008	Protocol-Misuse Anomaly,TCP RST Flooding	Disabled Enabled	5	Kpps
4	S120007	Protocol-Misuse Anomaly,Land Attack	Disabled Enabled	1	Kpps
5	S120006	Protocol-Misuse Anomaly,ICMP Misuse	Disabled Enabled	256	pps
6	S120005	Protocol-Misuse Anomaly,UDP Fragment	Disabled Enabled	1	Kpps
7	S120004	Protocol-Misuse Anomaly,TCP Fragment	Disabled Enabled	1	Kpps
8	S120003	Protocol-Misuse Anomaly,TCP Flag Null or Misuse	Disabled Enabled	1	Kpps
9	S120002	Protocol-Misuse Anomaly,IP Protocol Null	Disabled Enabled	1	Kpps
10	S120001	Protocol-Misuse Anomaly,TCP SYN Flooding	Disabled Enabled	1	Kpps

4 Anti-DDoS Products Introduction

4.1 Anti-DDoS8000 Series

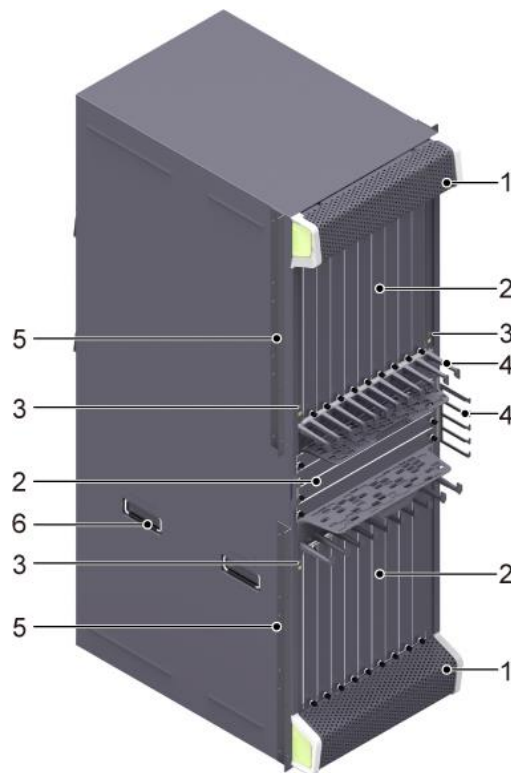
4.1.1 Anti-DDoS8000 Hardware

This chapter will introduce [Anti-DDoS8XXX](#) (e.g. 8160/8080/8030) product hardware and main specifications:

//Please choose Anti-DDoS8160/8080/8030 based on the project.

//Anti-DDoS8160

- **Front View**



- **Rear View**



1. Air intake vent	2. Board cage	3. ESD jack	4. Cabling trough	5. Rack-mounting ear
6. Handle	7. Fan module	8. PFU	9. PEM module	10. AC power management interface
11. CMU	12. PGND terminal (M6)			

- Slots layout on the AntiDDoS8160

1	2	3	17	18	4	5	6	7
L	L	L	M	M	L	L	L	L
P	P	P	P	P	P	P	P	P
U	U	U	U	U	U	U	U	U
/	/	/	/	/	/	/	/	/
S	S	S	S	S	S	S	S	S
P	P	P	P	P	P	P	P	P
U	U	U	U	U	U	U	U	U
SFU								19
SFU								20
SFU								21
SFU								22
n	n	n	n	n	n	n	n	n
d	d	d	d	d	d	d	d	d
s	s	s	s	s	s	s	s	s
/	/	/	/	/	/	/	/	/
n	n	n	n	n	n	n	n	n
d	d	d	d	d	d	d	d	d
7	7	7	7	7	7	7	7	7
8	9	10	11	12	13	14	15	16

Slot	Quantity	Slot Width	Description
1 to 16	16	41 mm (1.6 inches)	Indicates the slots for LPUs and SPUs. The LPUs and SPUs can be inserted at the same time. Select the LPUs and SPUs as required, but at least one LPU and one SPU are required.
17 to 18	2	41 mm (1.6 inches)	Indicates the slots dedicated for MPUs. The slots can house two MPUs to form 1:1 backup.
19 to 22	4	41 mm (1.6 inches)	Indicates the slots for SFUs. The slots can house four SFUs to form 3+1 backup for load balancing.

- **Anti-DDoS8160 system technical specification**

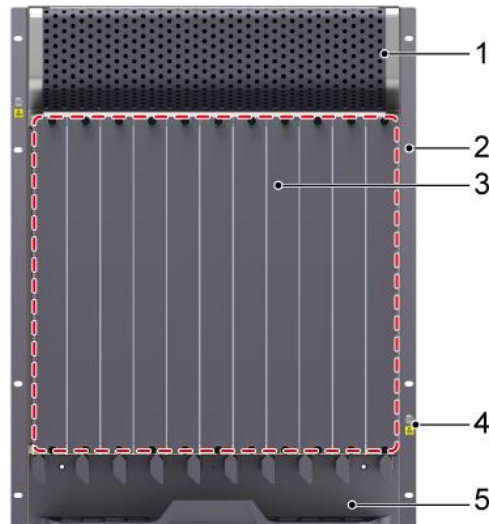
Item	Description
System specifications	
Processing unit of the MPU	Main frequency: 1.5 GHz
BootROM capacity of the MPU	8 MB
SDRAM capacity of the MPU	4 GB

Item		Description
NVRAM capacity of the MPU		4 MB
Flash capacity of the MPU		32 MB
CF card		2 x 2 GB
Number of slots	MPU	2 (slots 17 and 18)
	SFU	4 (slots 19 to 22)
	LPU/SPU	16 (slots 1 and 16)
Dimensions and weight		
Dimensions (Width ^a x Depth x Height ^b)		442 mm x 650 mm x 1420 mm (32 U). The depth is 770 mm covering the dust filter and cable rack.
Installation position		N68E cabinet or a standard 19-inch cabinet
Weight	Empty chassis	94.4 kg
	Full configuration (maximal)	233.9 kg
Power specifications		
Power supply mode	DC	8 hot-swappable PEM modules
	AC	8 PEM modules+2 external AC power chassis
Rated input voltage	DC	-48 V
	AC	175 V AC to 264 V AC; 50/60 Hz
Maximum input voltage range	DC	-72 V to -38 V
	AC	90 V AC to 264 V AC; 50/60 Hz
Typical power (six LPUF-240s and nine SPUs are configured.)	DC	7387 W
	AC	7858 W
Maximum Power ((six LPUF-240s and nine SPUs are configured.)	DC	8930 W
	AC	9500 W

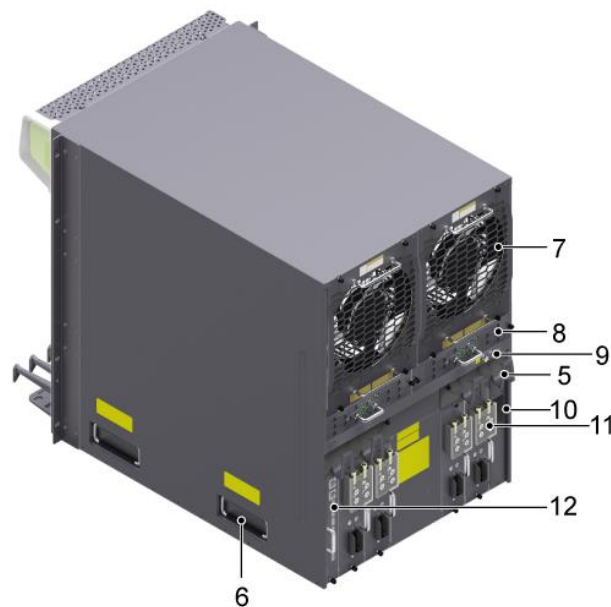
Item		Description
Heat dissipation		
Fan module		4 hot-swappable fan modules, each of which has one fan
Air flow		Upper and lower air channels: draw air from the front and discharge air from the back. Middle air channels: draw air from the left side and discharge air from the upper and lower back.
Air filter		3 air filters in the air intake vents of air channels
Environment specifications		
System reliability	MTBF (year)	25
	MTTR (hour)	0.5
Ambient temperature ^c	Long-term ^d	0°C to 45°C
	Short-term	-5°C to 50°C
	Remarks	Limit of the temperature change rate: 30°C/hour
Storage temperature		-40°C to 70°C
Ambient relative humidity	Long-term	5% RH to 85% RH, no coagulation
	Short-term	5% RH to 95% RH, no coagulation
Storage relative humidity		0% RH to 95% RH
Long-term altitude		Lower than 3000 m
Storage altitude		Lower than 5000 m
NOTE		
a. The width does not include the width of the mounting ear attached. b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards. c. The measurement point of the temperature and humidity is 1.5 m over the floor and 0.4 m in front of the cabinet without the front and the back doors. d. Short-term operation means that the continuous operation time does not exceed 96 hours and the accumulated operation time per year does not exceed 15 days. Otherwise, it is called long-term operation.		

//Anti-DDoS8080

• **Front View**



• **Rear View**



1. Air intake vent	2. Rack-mounting ear	3. Board cage	4. ESD jack
5. Cabling trough	6. Handle	7. Fan	8. PFU
9. PGND terminal (M6)	10. AC power management interface	11. PEM module	-

- **Slots layout on the AntiDDoS8080**

1	2	3	4	9	11	10	5	6	7	8
L	L	L	L	S	S	S	L	L	L	L
P	P	P	P	R	F	R	P	P	P	P
U	U	U	U	U	U	U	U	U	U	U
/	/	/	/				/	/	/	/
S	S	S	S				S	S	S	S
P	P	P	P				P	P	P	P
U	U	U	U				U	U	U	U
1	2	3	4	9	11	10	5	6	7	8

Slot Name	Slot Number	Quantity	Slot Width	Remarks
LPU/SPU	1 to 8	8	41 mm (1.6 inches)	These slots are used to hold LPUs and SPUs.
SRU	9 to 10	2	36 mm (1.4 inches)	These slots hold SRUAs in 1:1 backup mode.
SFU	11	1	36 mm (1.4 inches)	The slot is used to hold an SFU.

- **Anti-DDoS8080 system technical specification**

Item	Description	
System specifications		
Processing unit of the SRU	Main frequency: 1.5 GHz	
BootROM capacity of the SRU	8 MB	
SDRAM capacity of the SRU	4 GB	
NVRAM capacity of the SRU	4 MB	
Flash capacity of the SRU	32 MB	
CF card	2 x 2 GB	
Number of slots	SRU	2 (slots 9 and 10)
	SFU	1 (slot 11)
	LPU/SPU	8 (slots 1 and 8)

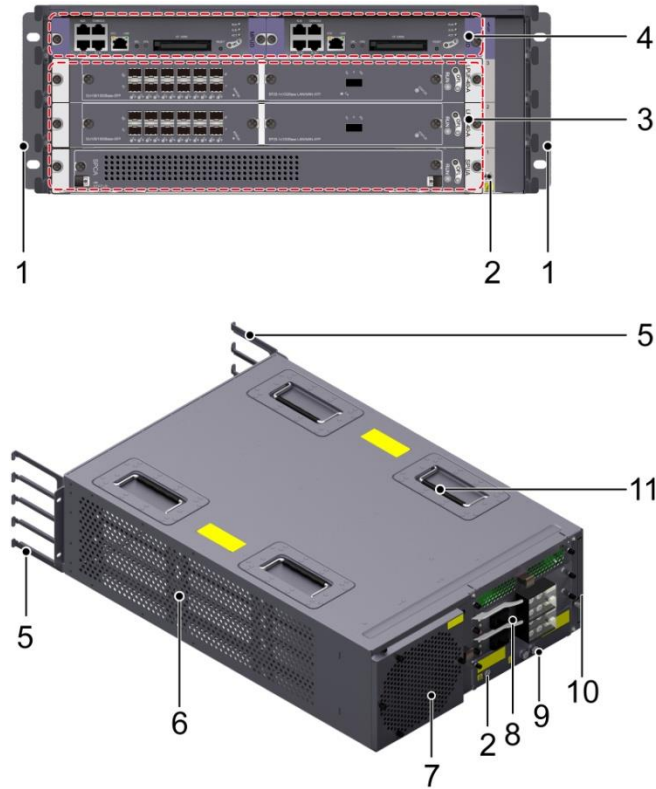
Item		Description
Dimensions and weight		
Dimensions (Width ^a x Depth x Height ^b)		442 mm x 650 mm x 620 mm (14 U). The depth is 770 mm covering the dust filter and cable rack.
Installation position		N68E cabinet or a standard 19-inch cabinet
Weight	Empty chassis	43.2 kg
	Full configuration (maximal)	112.9 kg

Power specifications		
Power supply mode	DC	4 hot-swappable PEM modules
	AC	4 PEM modules+1 external AC power chassis
Rated input voltage	DC	-48 V
	AC	175 V AC to 264 V AC; 50/60 Hz
Maximum input voltage range	DC	-72 V to -38 V
	AC	90 V AC to 264 V AC; 50/60 Hz
Typical power (Three LPUF-240s and five SPUs are configured.)	DC	4025 W
	AC	4282 W
Maximum Power (Three LPUF-240s and five SPUs are configured.)	DC	4823 W
	AC	5132 W
Heat dissipation		
Fan module		2 hot-swappable fan modules, each having one fan
Air flow		Front-to-back airflow

Air filter		1 air filter in the air intake vent of the air channel
Environment specifications		
System reliability	MTBF (year)	25
	MTTR (hour)	0.5
Ambient temperature ^c	Long-term ^d	0°C to 45°C
	Short-term	-5°C to 50°C
	Remarks	Limit of the temperature change rate: 30°C/hour
Storage temperature		-40°C to 70°C
Ambient relative humidity	Long-term	5% RH to 85% RH, no coagulation
	Short-term	5% RH to 95% RH, no coagulation
Storage relative humidity		0% RH to 95% RH
Long-term altitude		Lower than 3000 m
Storage altitude		Lower than 5000 m
<p>NOTE</p> <p>a. The width does not include the width of the mounting ear attached.</p> <p>b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards.</p> <p>c. The measurement point of the temperature and humidity is 1.5 m over the floor and 0.4 m in front of the cabinet without the front and the back doors.</p> <p>d. Short-term operation means that the continuous operation time does not exceed 96 hours and the accumulated operation time per year does not exceed 15 days. Otherwise, it is called long-term operation.</p>		

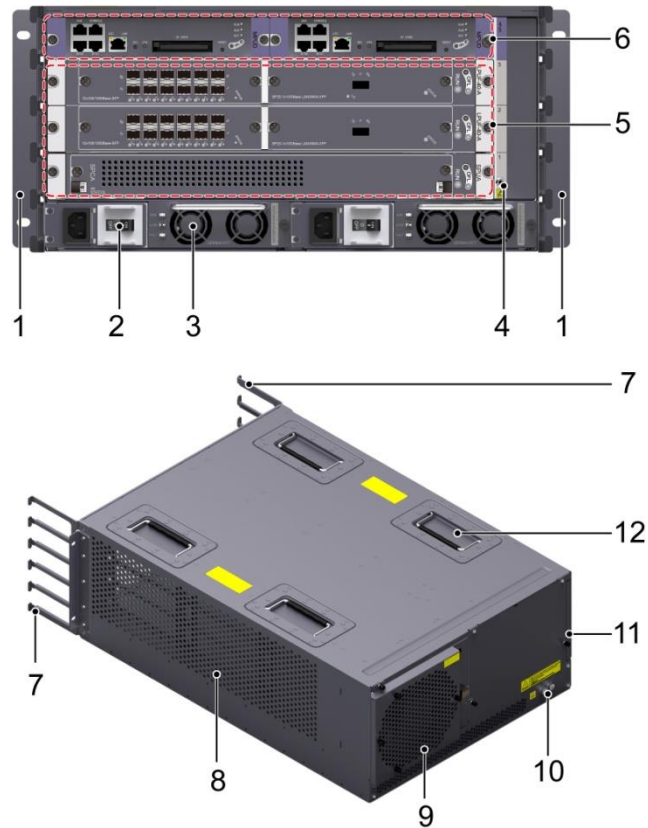
//Anti-DDoS8030

• **Components of the Anti-DDoS8030 DC chassis**



1. Rack-mounting ear	2. ESD jack	3. LPU/SPU cage	4. MPU cage
5. Cabling rack	6. Air intake vent	7. Fan	8. PEM module
9. PGND terminal (M6)	10. Air filter	11. Handle	-

• **Components of the Anti-DDoS8030 AC chassis**



1. Rack-mounting ear	2. Power switch and power socket	3. AC power module	4. ESD jack
5. LPU cage	6. MPU cage	7. Cabling rack	8. Air intake vent
9. Fan	10. PGND terminal (M6)	11. Air filter	12. Handle

• **Slots layout on the Anti-DDoS8030**

4	MPU	MPU	5
	LPU/SPU		3
	LPU/SPU		2
	LPU/SPU		1

Board distribution in the board cage of the Anti-DDoS8030

Slot Name	Slot Number	Quantity	Slot Width	Remarks
LPU/SPU	1 to 3	3	41 mm (1.6	These slots are used to hold SPU's or

Slot Name	Slot Number	Quantity	Slot Width	Remarks
			inches)	LPU.
MPU	4 to 5	2	41 mm (1.6 inches)	These slots hold MPUs that work in 1:1 backup mode.

- **Anti-DDoS8030 system technical specification**

Item		Description
System specifications		
Processing unit of the MPU		Main frequency: 1 GHz
BootROM capacity of the MPU		1 MB
SDRAM capacity of the MPU		2 GB
NVRAM capacity of the MPU		512 MB
Flash capacity of the MPU		32 MB
CF card		1 x 2 GB
Number of slots	MPU	2 (slots 4 and 5)
	SFU	-
	LPU/SPU	3 (slots 1, 2, and 3)
Dimensions and weight		
Dimensions (Width ^a x Depth x Height ^b)		DC chassis: 442 mm x 650 mm x 175 mm (4 U) AC chassis: 442 mm x 650 mm x 220 mm (5 U) The depth is 750 mm covering the dust filter and cable rack.
Installation position		N68E cabinet or a standard 19-inch cabinet
Weight	Empty chassis	DC chassis: 15kg AC chassis: 25kg
	Full configuration (maximal)	DC chassis: 30.7 kg AC chassis: 40.7 kg
Power specifications		
Power supply	DC	Double hot-swappable power

Item		Description
mode		modules
	AC	Double hot-swappable power modules
Rated input voltage	DC	-48 V
	AC	175 V AC to 264 V AC; 50/60 Hz
Maximum input voltage range	DC	-72 V to -38 V
	AC	90 V AC to 264 V AC; 50/60 Hz
Typical power (One LPUF-120 and two SPUs are configured.)	DC	1066 W
	AC	1185 W
Maximum Power (One LPUF-120 and two SPUs are configured.)	DC	1272 W
	AC	1414 W
Heat dissipation		
Fan module		1 hot-swappable fan module that has two fans
Air flow		Left-to-back airflow
Air filter		1 air filter in the air intake vent of the air channel
Environment specifications		
System reliability	MTBF (year)	25
	MTTR (hour)	0.5
Ambient temperature ^c	Long-term ^d	0°C to 45°C
	Short-term	-5°C to 50°C
	Remarks	Limit of the temperature change rate: 30°C/hour
Storage temperature		-40°C to 70°C
Ambient relative humidity	Long-term	5% RH to 85% RH, no coagulation
	Short-term	5% RH to 95% RH, no coagulation
Storage relative humidity		0% RH to 95% RH

Item	Description
Long-term altitude	Lower than 3000 m
Storage altitude	Lower than 5000 m
NOTE a. The width does not include the width of the mounting ear attached. b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards. c. The measurement point of the temperature and humidity is 1.5 m over the floor and 0.4 m in front of the cabinet without the front and the back doors. d. Short-term operation means that the continuous operation time does not exceed 96 hours and the accumulated operation time per year does not exceed 15 days. Otherwise, it is called long-term operation.	

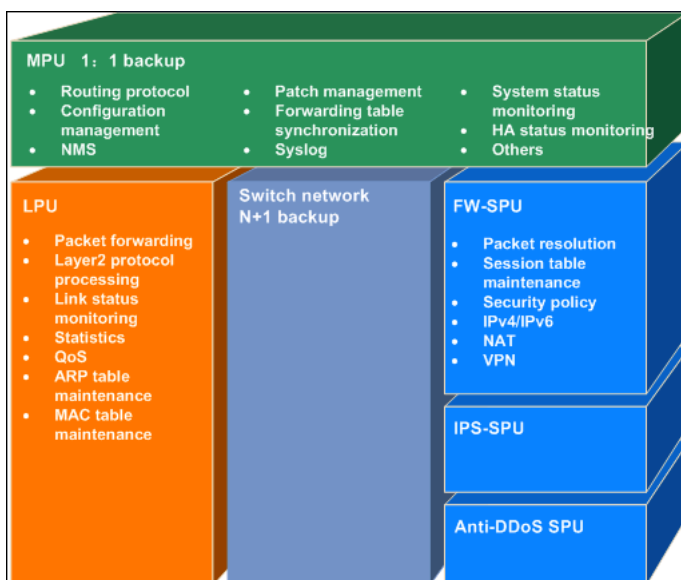
4.1.2 Anti-DDoS8000 Software

- **Logical Software Architecture**

The Anti-DDoS8000 adopts the flexible and sophisticated versatile routing platform (VRP). Based on the component technology, the VRP supports the distributed architecture and improves security features and reliability.

Figure 1 shows the logical diagram of the software architecture.

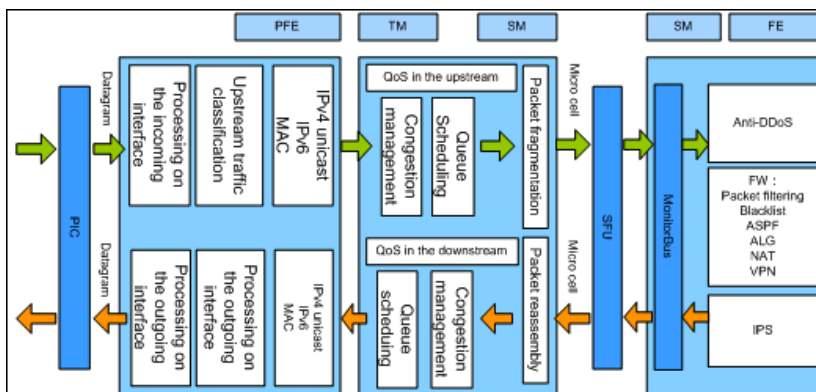
Figure 1 Diagram of the logical software architecture



- **Data Forwarding Process**

Anti-DDoS8000 shows the flowchart of forwarding data.

Figure 1 Flowchart of forwarding data



According to data direction, data forwarding can be divided into the following three processes:

4.2 GenieATM6300

4.2.1 GenieATM6300 Hardware

This chapter will introduce GenieATM6000 product hardware and main specifications:

- **Front View**



- **Rear View**



- **Specifications**

Note: All GenieATM6000 hardware appearance is the same, the specification is different, please choose the correct specification according to the datasheets.

For example, following is the specification of GenieATM6365 and GenieATM6333

GenieATM6365	
Item	Specifications
Flow Capacity	50,000/s
Protected Link Bandwidth	180G

<i>CPU</i>	<i>Intel Xeon 6-Core E5-2620 @ 2.00GHz x2</i>
<i>Memory</i>	<i>16G</i>
<i>Hard Drives</i>	<i>1x300GB SAS HD for Controller 63xx; 1x 1TB SATA HD for Collector 61xx [Optional : Up to 4 SAS/SATA disks, hot-swap]</i>
<i>Power supply</i>	<i>Dual 750W Hot-swap redundant AC power supply 100-240VAC 50/60 Hz</i>
<i>Interface</i>	<i>LAN Port: Dual GbE ports, supporting 10/100/1000BASE - T Console Port: RS-232</i>
<i>Dimensions</i>	<i>H/D/W : 43.2 / 728 / 438 mm Chassis : 19" Rack mount, 1U</i>

GenieATM6333	
Item	Specifications
<i>Flow Capacity</i>	<i>20,000/s</i>
<i>Protected Link Bandwidth</i>	<i>72G</i>
<i>CPU</i>	<i>Intel Xeon 4-Core E5-2603 x2 or above</i>
<i>Memory</i>	<i>16G</i>
<i>Hard Drives</i>	<i>1x300GB SAS HD for Controller 63xx; 1x 1TB SATA HD for Collector 61xx [Optional : Up to 4 SAS/SATA disks, hot-swap]</i>
<i>Power supply</i>	<i>Dual 750W Hot-swap redundant AC power supply 100-240VAC 50/60 Hz</i>
<i>Interface</i>	<i>LAN Port: Dual GbE ports, supporting 10/100/1000BASE - T Console Port: RS-232</i>
<i>Dimensions</i>	<i>H/D/W : 43.2 / 728 / 438 mm Chassis : 19" Rack mount, 1U</i>

Note: For other models, please refer to following attached documents (at the end of this document):

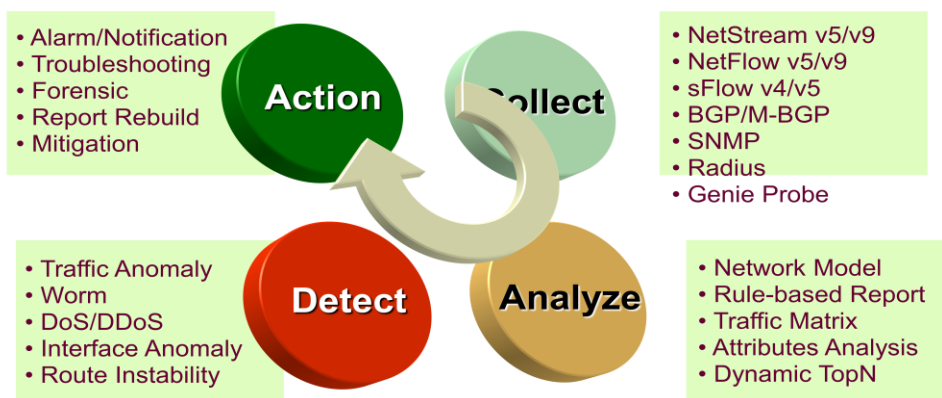
“GenieATM Specifications.xlsx”, “GenieATM6000_Datasheet.pdf”.

4.2.2 GenieATM6300 Software

● GenieATM Capability Overview

With embedded intelligence and high performance, GenieATM provides a total solution for Network-wide Flow Analysis, DDoS Attack Detection, and Network Anomaly Detection.

-- A Flow-based Traffic Analysis and Anomaly Detection Solution



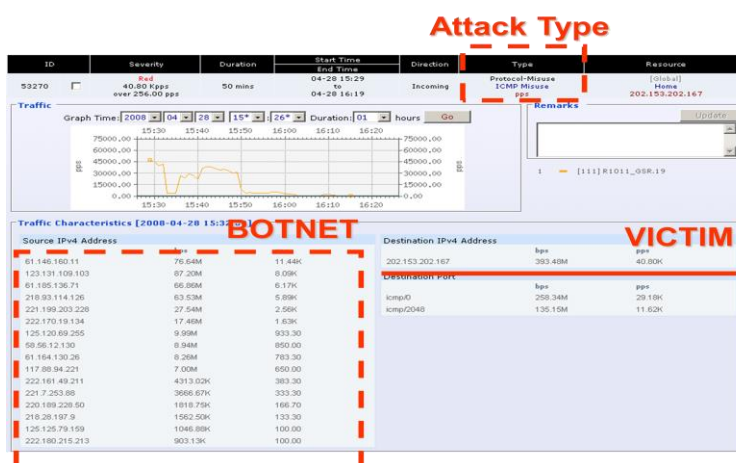
GenieATM 6000 is based on network-wide traffic collection for data mining and anomaly detection. It can automatically generate various pre-defined traffic reports and detect abnormal network behaviors, DDoS attacks, and unusual routings from interior or exterior networks, and then send out alerts to network operators in time. Meanwhile, GenieATM 6000 also provides powerful Snapshot and Forensic tools which can support the integration of third-party devices to promptly intercept anomaly traffic.

● GenieATM supports detect following types of DDoS attacks:

GenieATM is able to detect the prevalent Protocol-Misuse anomalies and DDoS attacks efficiently by finding abnormal behaviors against protocol rules built in the system and examining if the misused traffic is over the threshold.

- TCP SYN Flooding: TCP SYN packets are sent in large number and exceed the threshold value configured.
- IP Protocol Null: Anomaly traffic is detected when IP Protocol = 0.
- TCP Flag Null or Misuse: Found TCP Flag = 0 or SYN+FIN, SYN+RST, FIN, ACK and RST misuse after matching TCP.
- TCP Fragment: Fragmented packets do not have TCP headers (except for the first one); hence the system uses this trait to detect excess TCP fragments.
- UDP Fragment: Fragmented packets do not have UDP headers (except for the first one); hence the system uses this trait to detect excess UDP fragments.
- ICMP Misuse: ICMP packets are sent in large number and exceed the threshold value configured.
- Land Attack: Source IP address is mistakenly equivalent to the destination IP address.
- TCP RST Flooding: TCP RST packets are sent in large number and exceed the threshold value configured.
- UDP Flooding: UDP packets are sent in large number and exceed the threshold value configured.
- Host Total Traffic: Huge traffic is sent to a certain host and exceeds the threshold value configured.

For example, following graphical figure show an ICMP flood attack:



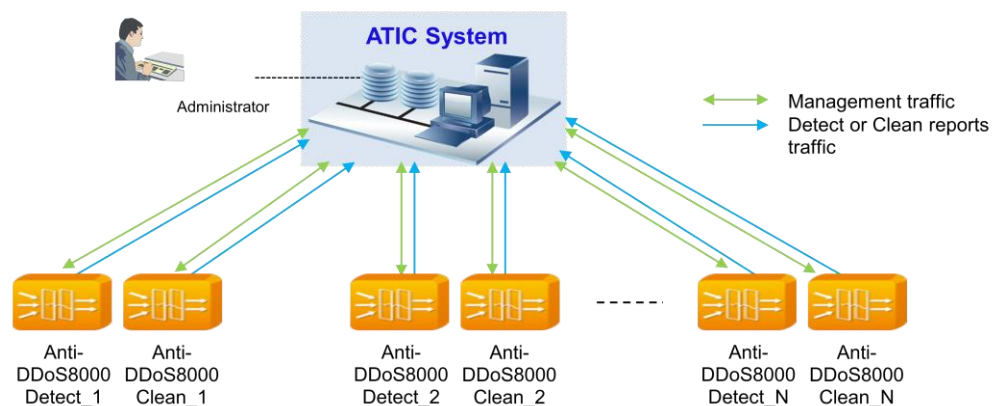
Note: In the GenieATM, the Protocol-Misuse anomalies are system built-in and cannot be modified or deleted. Below are supported Protocol Misuses of the system.

4.3 ATIC System

4.3.1 ATIC System Architecture

ATIC (Abnormal Traffic Inspection Center) is Huawei self-developed Anti-DDoS system management software, it is installed on standard Windows Servers.

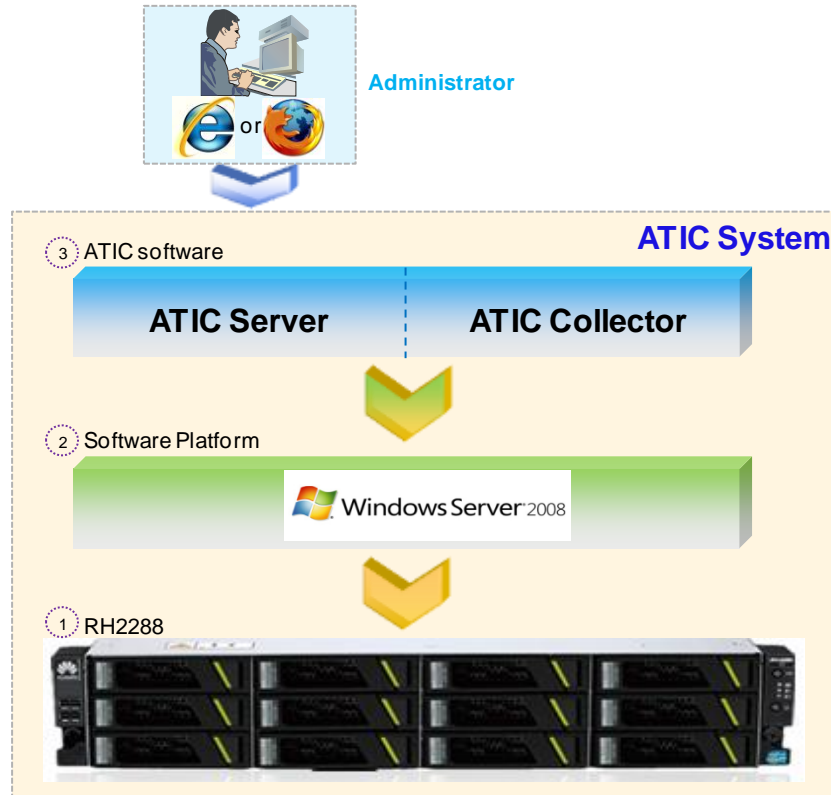
- **ATIC System Network Architecture**



1. One ATIC system can manage up to 50 Anti-DDoS detect/clean devices
2. Administrator can configure Anti-DDoS detect/clean device via ATIC web UI
3. ATIC receive attack alert logs from detect device, and automatically send divert command to clean device
4. When the attack ends, ATIC automatically send command to clean device to remove the divert command
5. ATIC receive clean logs from clean device and make reports


- **ATIC System Architecture**

ATIC (Abnormal Traffic Inspection Center) is Huawei self-developed Anti-DDoS system management software, it is installed on standard Windows Servers.



Note: ① Hardware@Huawei ② Software@Microsoft ③ Software@Huawei

4.3.2 ATIC System Hardware Requirements

Options	Requirements	Hardware Appearance
Recommended Configuration	CPU: Xeon quad-core E5506 2.13 GHz or higher; Memory: 8 GB; Hard disk: 2 x 300 GB RAID1	For example, Huawei RH2288 series server 
Minimum Configuration	CPU: dual-core X86 processor; Memory: 4 GB; Hard disk: 100 GB	Depends on the customer's choice

4.3.3 ATIC System Software Requirements

Software Platform	Software Type	Software Version
x86 (64-bit Windows)	Operating system	Windows Server 2008 R2 Standard with SP1
	Web browsers that can access the server	Internet Explorer 8.0 or above Mozilla Firefox 4.0 or above
x86 (32-bit Windows)	Operating system	Windows Server 2003 R2 Standard with SP2
	Web browsers that can access the server	Internet Explorer 8.0 or above Mozilla Firefox 4.0 or above

Acronyms and Abbreviations

ATIC	Abnormal Traffic Inspection Center
DDoS	Distributed Denial of Service
FW	Firewall
HA	High Availability
NE	network element
NMS	Network Management System
VPN	Virtual Private Network
NGFW	Next Generation Firewall

Attachments

Attention: The documents of this chapter are intended to be used as reference during writing Technical Proposals for projects. "GenieATM Specifications.xlsx" contains all model of GenieATM6000 series and related performance, it is only for internal usage, please delete them after finished the technical proposal.

The GenieATM datasheet and product description



GenieATM
Specifications. xl



GenieATM6000_Data
sheet. pdf