Huawei Technical Proposal

For Anti-DDoS Project

Prepared by Chenjia 00273721 Date:2019/09



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	
3.3.1 ATIC Management Portal	
3.3.2 ATIC Traffic and Attack Reports	16
3.3.3 GenieATM6000 Management Portal	
4 Anti-DDoS Products Introduction	26
4.1 Anti-DDoS8000 Series	
4.1.1 Anti-DDoS8000 Hardware错误!未定义	书签。
4.1.2 Anti-DDoS8000 Software	41
4.2 GenieATM6300	
4.2.1 GenieATM6300 Hardware	
4.2.2 GenieATM6300 Software	44
4.3 ATIC System	
4.3.1 ATIC System Architecture	
4.3.2 ATIC System Hardware Requirements	
4.3.3 ATIC System Software Requirements	
Acronyms and Abbreviations	48
Attachments	49

1 Huawei's understanding of XX's Requir ements

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 <u>RFC 3917</u>. Cisco <u>NetFlow</u> Version 9 was the basis for IPFIX) and cFlowd (supported by Alcatel-Lucent, Juniper, etc)

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

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.

Device TypeChassis model and quantityCapacityMax. sup	ximum number of upported routers
--	-------------------------------------

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

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	GenieATM6333*2	20,000flow/s(72Gbps bandwidth)	2

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:

Device Type	Chassis Model and quantity	Clean board quantity	Current Capacity	Maximum Expansion Capacity
Cleaning Center	Anti-DDoS80 80 *1	1*160Gbps Clean board	160Gbps	720Gbps

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:

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

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



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

Anti-DDoS System DDoS Cle Borders r Management Center Netflow information of the service traffic DDoS attack traffic * Netflow analyzer send attack alerts to Management Ce nd command to clean device to divert traffic POPN nd BGP host route to divert traffic to cleaning system ¥ DDoS attack traffic are diverted to the <u>.</u> 6 Send back the good traffic after cleaning Cleaning reports

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.





Optional Pie Chart and Bar Chart





	Report > ROUTER >	Traffic			welcome casper
	Router Group: ALL Rou Time Range: Period: Daily	ters V Start Time: 2006 V Nov V 2 V Until: 2006 V Nov V 3 V	09:00 V Unit: bps V Out 09:00 V Chart: Stacked Ch	puti Download Graph C hart Show on Web	SV V Submit
Al to de la processa and the second	10100 10200.00 2020.00 2020.00 2020.00 1000	12:00 14:00 15:00 18:00			
	Download Excel-XML	22100 14:00 15:00 19:00 ** *Device Name *Device Name *Device Name ** **	VID 22100 00100 0214 VID 339.36K 322.43K 306.47K	Sout Average 320.99K 310.99K 306.47K 306.47K	00100 Current Maximum Difference 10.37K 11.45K 0.00

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

Close

Basic Information HE name : AntiDDoS1000	Create NE					?	
NE name: AntiDDoS1000 IP address: 2.2.0.200 NE Type: AntiDDoS Type: Image:	Basic Informatio	'n					
NE Type: ANUDDOS Tolnet parameter Type: admin admin Password: snAP parameter Type: ShMP/parameter Type: ShMP/parameter Type: ShMP/parameter Type: ShMP/parameter Type: ShMP/parameter Type: ShMP/parameter Type: ShMP/parameter Type: Type: ShMP/parameter Type: Type: ShMP/parameter OK Cancel OK Cancel Create NE Result OK Cancel Intervention OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel Concel OK Cancel Concel Cancel OK Cancel Concel OK Cancel Concel OK Cancel OK Cancel Concel OK Cancel Concel OK Cancel Concel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel OK Cancel	NE name :		AntiDDoS1000	*	IP address :	2.2.10.200	*
Type: Telnet Username: admin admin Password: SNMP parameter Type: SNMP journameter Type: SNMP journameter Read community: public public write community: private c Create NE Result Create NE Result C Supervise NE Synchronize NE Image: Passe	NE Type :		AntiDDoS	~			
Type: Telnet admin Password: SNMP parameter Type: SNMPv2c Read community: Public Public Write community: public Write community: private Cancel Create NE Result Create NE Result Image: Cancel Sinchronize NE Image: Parameter Image: Par	Telnet paramete	er					
Username: admin Password: SNMP parameter Type: SNMP/2C Read community: public Write community: private Create Account Create Create Create Account Create Create Create Create	Type :		Telnet	~			
SNMP parameter Type : Read community : public Write community : private OK Cancel Create NE Result Create NE Result 2 Create NE Result 100% Create All Result 100% Create All Result 100% Create All Result 2 Create All Result 100% Create All Result 100% Create All Result 2 Create All Result 2 Create All Result 3ave NE	Username :		admin	*	Password :	•••••	•
Type : SNMPv2c Read community : public write community : pr/vate OK Cancel Create NE Result Create NE Result ? × Create NE Result 100% Discovery Result Save NE Associate collector DDoSCollector success. Synchronize NE · Create default zone · Associate collector · Associate collector · Associate collector · Associate template · Associate template success. Deploy · Deploy	SNMP paramete	r					
Read community: public Write community: private OK Cancel OK Cancel OK Cancel Create NE Result 100% Discovery Result Save NE IP address: 2.2.10.200, NE type: AntiDDoS1520 Synchronize NE Image: Create default zone Create default zone Create default zone Create default zone Create default zone Create default zone Create default zone Create default zone Create default zone Create default zone Create default zone Associate template Associate template success. BASIC-100M Deploy Deploy success.	Type :		SNMPv2c	*			
OK Cancel Create NE Result ? × 100% Discovery Result Discovery Result Save NE ✓ Y IP address:22.10.200; NE type:AntbDDoS1520 Synchronize NE ✓ Associate collector ✓ Associate collector DDoSCollector success. Create default zone ✓ Create default zone success. DefaultZone2_2_10_200 Associate template ✓ Associate template success. BASIC-100M Deploy ✓ Deploy success.	Read community		public	*	Write community :	private	*
Discovery Result Save NE IP address:2.2.10.200; NE type:AntiDDoS1520 Synchronize NE Associate collector Associate collector DDoSCollector success. Create default zone Create default zone success. DefaultZone2_2_10_200 Associate template Associate template success. BASIC-100M Deploy Deploy success. 	Create NE Result						? ×
Discovery Result Save NE IP address:22.10.200; NE type:AntiDDoS1520 Synchronize NE IP address:22.10.200; NE type:AntiDDoS1520 Associate collector Associate collector DDoSCollector success. Create default zone Create default zone success. DefaultZone2_2_10_200 Associate template Associate template success. BASIC-100M Deploy Deploy success.				10	0%		
Save NE IP address: 2.2.10.200; NE type: AntiDDoS1520 Synchronize NE Associate collector Associate collector DDoSCollector success. Create default zone Create default zone success. DefaultZone2_2_10_200 Associate template Associate template success. BASIC-100M Deploy Deploy success. 	Discovery Result						
Synchronize NE Associate collector Associate collector DDoSCollector success. Create default zone Associate template Associate template Associate template Deploy	Save NE	🗸 IP addr	ess:2.2.10.200; NE type	:AntiDDoS152	D		
Associate collector Associate collector DDoSCollector success. Create default zone Create default zone success. DefaultZone2_2_10_200 Associate template Associate template success. BASIC-100M Deploy Deploy success. 	Synchronize NE	~					
Create default zone Create default zone success. DefaultZone2_2_10_200 Associate template Deptoy Deptoy	Associate collector	🖌 Associa	ate collector DDoSColle	ctor success.			
Associate template Associate template success. BASIC-100M Deploy Deploy success. 	Create default zone 🖌 Create default zone success. DefaultZone2_2_10_200						
Deploy Ceploy success.	Associate template 🛛 🖌 Associate template success. BASIC-100M						
	Deploy	🖌 Deploy	SUCCESS.				

• Policy configuration

Step1: Auto Configure Zone

Settings A	inti-DDoS Zone	\rangle								0
Zone List										
💠 Create 🗱	Delete 😰 Deploy	Deploy All	Undeploy Import	Export Street All	refresh ; Manual 💌		Account	Name :	Q, Search	Advanced Search 🗸
0	Zone	Туре	NE Name	Service Learning	Baseline Learning	State	Defense State	Diversion State	Deployment State	Operation
DefaultZone	2_2_10_201	Default	AntiDDoS8000	Notlearned	Not learned	Abnormal	Automatically Defended	Not diverted	Deploy Succeed	
DefaultZone	2_2_10_200	Default	AntiDDoS1000	Not learned	Notlearned	Normal	-	Not diverted	Deploy Succeed	🕞 🚳
Page 1	of 1 10	items per page	GO GO							Items 1 to 2 Total: 2

Step2: Click Operation column item to see Policy

Basic Policy Filter Defense Policy		
Traffic Diversion Mode :	Automatic Manual	3
Defense Mode :	◯ Automatic	(?)
Dynamic Blacklist Mode :	Automatic Close	(?)
Cleaning Bandwidth :	✓ Enable Threshold (Mbit/s): 1000 (1-10240)	(?)
Traffic Limiting for Single IP Address :	Enable Threshold (Mbit/s): 100 (1-10240)	3

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

DefaultZone2_2	_10_201's View Ano	maly							? ×
Abnormal Events	Dynamic Blacklist								
Abnormal Event	List								ø
📖 Defense				NE Name :	All		Defense State :	All 🗸	🔍 Search
IP Address	NE Name	Anti-DD	Anomaly Start Ti	Attack Type	Threshold	Actual Value	Number of At	State	Defense
3.3.10.6	AntiDDoS8000	Cleaning	2013-04-09 17:50:19	Other Flood Attack	1024kbps	1468kbps	0	Abnormal	AutomaticalI
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
1< < Page 1	of 1 10 item	ns per page						Items	1 to 4 Total: 4

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 Deft 🕨
Block							*
Traffic Limiting							
Defense TCP Abnormal Defense	efense						
The	eshold (pps) :		1000	((1-1200000)		
TCP Basic Defen	se						
SYN Flood /	Attack Defense						
Thr	eshold (pps) :		2000	((1-1200000)		
SYN-ACK FI	lood Attack Defen:	56					
The	eshold (pps) :		1000	((1-1200000)		
ACK Flood /	Attack Defense						
Sessi	on Check						-
		Import Servi	ice Policy Templat	e Export Ser	vice Policy Templa	ate OK	Cancel

Page2/4

Configure Service	,						? X
 Basic Information 	TCP Defense	UDP Defense	ICMP Defense	Other Defense	DNS Defense	SIP Defense	HTTP Deft 🕨
ACK Floor	d Atlack Defense						*
Ses	sion Check						
D	efense Mode :		 Basic 	 Strict 			۲
T	hreshold (pps) :				(1-1200000)		
Payl	oad Check						۲
TCP Frag	ment Attack Defens	e					
T	hreshold (pps) :		200		(1-65535)		
FINRST F	Flood Attack Defens	0					
т	hreshold (pps) :		2000		(1-65535)		
🗹 Real Sour	ce IP Rate Limiting						
R	ate Limiting Mode :		TCP-F	Ratio Anomaly Lin	niting 🔿 Perman	ent Limiting	۲
т	CP-Ratio Proportion	Threshold :	20		(1-100)		
R	ate Limiting Thresh	old (pps) :	3		(0-1200)		
TCP Connection	n Flood Attack Defe	nse					+
		Import Servi	ice Policy Template	Export Se	ervice Policy Templ	ate OK	Cancel

Page3/4

Configure Service							? ×			
Basic Information	TCP Defense	UDP Defense	ICMP Defense	Other Defense	DNS Defense	SIP Defense	HTTP Deft 🕨			
			L							
TCP Connection	Flood Attack Defe	nse								
Concurrent connection check by destination IP address										
n The	eshold :		6000		(1-1200000)					
New connection rate check by destination IP address										
The	eshold (Connectio	ons per Second) :			(1-1200000)					
New conne	New connection rate check by source IP address									
The	eshold:			((1-85535)					
Che	ack Cycle (s) :			ó (1-60)						
Connection	Number Check fo	or Source IP Addre	988							
The	eshold :			((1-65535)					
Rate Check	of Low-Rate Con	nection								
Che	ack times (Time) :			((3-20)					
Che	ack Cycle (s) :		8	((1-30)					
Abnormal S	ession Check						-			
		Import Servi	ice Policy Template	e Export Ser	rvice Policy Templa	ate OK	Cancel			

Page4/4

Abnorma	al Session Check						
Abnormal connection threshold :					(1-255)		
Check Cycle (s):			15	15 (1-240)			
Nu Nu	I connection check						
Minimum packets per connection :			1		(1-266)		
0	Check Cycle (s) :				(1-240)		
Retransmission session check							
F	Retransmission Pack Threshold :	at Number	200		(1-1023)		
Slo	w start connection ch	eck.					
Т	ICP Window Size Thi	reshold (Byte) :			(1-65535)		

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.



3) Attacks Top N logs

аске	acket Quantity Top N									
	NE IP Address	Zone Name	Zone IP Address	Anomaly Start Time	Attack Start Time	End Time	Attack Duration	Packet Quantity	Attack Type	Attack Status
1	128.18.60.41	TD4	49.7.1.123	2011-09-06 20:11:36	2011-09-06 20:11:36	2011-09-07 10:44:31	14:32:55	3936308008	SYN Flood	End
2	128.18.60.41	TD4	49.7.1.123	2011-09-06 20:11:44	2011-09-06 20:11:44	2011-09-07 10:43:43	14:31:58	3520221153	FIN/RST Flood	End
3	128.18.60.41	TD4	49.7.1.123	2011-09-06 20:11:44	2011-09-06 20:11:44	2011-09-07 10:43:43	14:31:58	3423771102	ACK Flood	End
4	128.18.60.41	TD4	49.7.1.123	2011-09-07 11:01:44	2011-09-07 11:01:44	-	00:40:05	179551167	SYN Flood	Attack
5	128.18.60.41	TD4	49.7.1.123	2011-09-07 11:03:06	2011-09-07 11:03:06	-	00:39:00	121795856	FIN/RST Flood	Attack
6	128.18.60.41	TD4	49.7.1.123	2011-09-07 11:03:06	2011-09-07 11:03:06	-	00:39:00	118640474	ACK Flood	Attack
7	128.18.60.36	lyf_a	200.6.1.100	2011-09-06 20:12:09	2011-09-06 20:12:09	-	15:30:17	28490790	SIP Flood	Attack
8	128.18.60.36	qj1	200.3.1.2	2011-09-06 20:11:14	2011-09-06 20:11:14	2011-09-07 10:11:56	14:00:41	8445946	Total Bandwidth Overflow	End
9	128.18.60.36	qj1	200.3.1.3	2011-09-06 20:11:20	2011-09-06 20:11:20	2011-09-07 10:12:02	14:00:41	8442326	Total Bandwidth Overflow	End
10	128.18.60.36	qj1	200.3.1.11	2011-09-06 20:11:56	2011-09-06 20:11:56	2011-09-07 10:11:33	13:59:36	8431530	Total Bandwidth Overflow	End
K <	Page 1 of 1	10 items pe	erpagel > >i GO						iten	ns 1 to 10 Total: 1
ack D	uration Top N									
	NE IP Address	Zone Name	Zone IP Address	Anomaly Start Time	Attack Start Time	End Time	Attack Duration	Packet Quantity	Attack Type	Attack Status
1	128.18.60.41	TD17	49.100.16.91	2011-09-06 20:11:09	2011-09-06 20:11:09	-	15:31:22	202259	FIN/RST Flood	Attack

Attacks Top N sorts attack events by top N number of attack packets or top N duration of attacks, and displays corresponding details.

• DNS Analysis

1) Top N Requested Domain Names and Top N DNS Source IP Addresses by Request Traffic Rate are enabled.



2) Top N Response Trend

Top N DNS Source IP Addresses by Response Traffic Rate is enabled



• 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.

Create Task					? ×
Basic Information	System Report	Zone Report			
Name : Plan : Run Time : * Life Cycle : Report Format : *	Daily 3 Hour 0 2013-11-18 00:0	* Minute 0:00 *To 20 ML EXCEL)13-11-18 23:59:59 📺 *		
Description :				2	

OK Cancel

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		
Run Time	Indicates the execution time of the task.	to 00:00 on the 8th day of each month, the system generates reports 00:00 on		
Life Cycle	Indicates the validity period of a task. The task becomes invalid when it expires.	the 8th day of each month from 2010-12-8 00:00:00 to 2011-12-8 23:59:59.		
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 is provides DDoS Detection function in Huawei Anti-DDoS solution, normally only need modify the threshold if DDoS attack.

- Image: space spac
- Overview of GenieATM6000 management portal

1) System Menu Tree

Display the system's main functions. The user can click "H" 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 " \boxdot{H} " 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" (Edit) and "Edit" (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)

5	System Aamin > Network > Sub-Network										
	Su	b-Net#	ork	Options							
	Sub-Net	work I	Management								
	Group:	LL Sub	-networks	Searching ID	• for Go						
	Add					< << 2/10 >>> > 25* • Entries/P					
	No			¥ Name	IP Space	Boundary Links Remarks					
	af 🖻	26	320	Zone_Corp_Packet_Core	permit 80.227.24.8/24	Internet Boundary					
	ef 🕏	27	319	Zone_Corp_Internet_Link	permik 80.227.6.232/29	Tinternet Boundary					
	af 🖻	28	318	Zone_CorpDIC4_BECS	permit 80.227.0.94/28	Internet Boundary					
	af 🗟	29	317	Zone_Corp_Emmar_PDC_IPTV	permit 65.39.136.0/21	Internet Boundary					
	af 🕸	30	316	Zone_Corp_DIC5_PS_Core	permit 94.201.224.0/24	Internet Boundary					
	af 🐮	31	315	Zone_Corp_Emaar_PDC_NAT	permit 80.227.1.0/24	Internet Boundary					
	af 🕸	32	314	Zone_Corp_DIC4_EITC_DNS	permit 80.227.2.0/24	Internet Boundary					

2) Configure the threshold for each kind of attack

Threshold page layout

otocol	Misuse Anomaly	Application Anomaly Mitigation			
tocol-I	Misuse Anomaly N	lanagement			
efault f	or Home and Use	r-defined Resources			
		Severity Latency: 10 min. Recover	er Latency: 5 m	in.	Edit
No.	¥ ID	* Name		Event Threshold	
			Enabled	15	Mbos
1	5120010	Protocol-Misuse Anomaly-Host Total Traffic	Disabled		pos
			Enabled	15	Mbps
2	5120009	Protocol-Misuse Anomaly.UDP Flooding	Disabled		pps
			Disabled		bps
3	5120008	Protocol-Misuse Anomaly, TCP RST Flooding	Enabled	5	Kpps
			Disabled		bps
4	5120007	Protocol-Misuse Anomaly.Land Attack	Enabled	1	Kpps
			Disabled		bps
5	5120006	Protocol-Misuse Anomaly.ICMP Misuse	Enabled	256	pps
			Disabled		bps
6	5120005	Protocol-Misuse Anomaly.UDP Fragment	Enabled	1	Kpps
	F100001	Particularity of the second states of the second	Disabled		bps
/	5120004	Protocol-Misuse Anomaly, ICP Fragment	Enabled	1	Kpps
	5100000	Parterel Minus Annual, TCD Firs Million Minus	Disabled		bps
9	5120003	Protocol-misuse Anomaly, TCP Flag Null or Misuse	Enabled	1	Kpps
	5120002	Protocol-Minuse Anomaly IP Protocol Null	Disabled		bps
9	5120002	Protocol Null	Enabled	1	Kpps
10	5120001	Protocol-Misuse Anomaly TCP SYN Flooding	Disabled		bps
	5120001	rioucor made anomaly. TCP STN Hooding	Enabled	1	Kpps

Press "Edit" button to modify the thresholds

System Adn	nin > Network > J	Anomaly		Minimum s Latency car	everity 1 be 1 min	welcome justin		
Protocorr	isuse Anomary	Application Anomaly Plicigation						
Protocol-Mi	isuse Anomaly Man	nagement						
Default for	r Home and User-d	efined Resources						
		Severity Latency: 10 min.		Recover Latency:	S min.	Edit		
No.		¥ Name		Stat	Event Thr	eshold loit		
1	5120010	Protocol-Misuse Anomaly.Host Te	Edit Prot Latency	locol Misuse Anomaly-De Severity Latency:	efai It for Home and User	defined Resources Recover Latence	et 5 × min.	
2	5120009	Protocol-Misuse Anomaly.UDP Fl	No. 2	0	Name	Etablet	Event Threshold Value	UNI
з	5120008	Protocol-Misuse Anomaly.TCP R	1 5120	010 Protocol-Mause Anome	iy:Hoat Total Traffic	Disabled • Enabled • 15	pp Ho	05.7
4	5120007	Protocol-Misuse Anomaly.Land A	3 5120	008 Protocol-Misuse Anoma	ly:TCP RST Flooding	Disabled • Disabled • Enabled • 5	ter Ke	
5	5120006	Protocol-Misuse Anomaly.ICMP N	4 5120	007 Protocol-Misuse Anoma	ly:Land Attack	Disabled • Enabled • 1	ka ka	s * ps *
6	5120005	Protocol-Misuse Anomaly.UDP Fr	5 5120	006 Protocol-Misuse Anoma	Internet Marine	Enabled • 256 Disabled •	ppr bpr	
7	5120004	Protocol-Misuse Anomaly.TCP Fr	6 5120 7 5120	005 Protocol-Mause Anoma 004 Protocol-Mause Anoma	ly:UDP Pregment	Enabled • 1 Disabled •	Kan bar	
8	5120003	Protocol-Misuse Anomaly.TCP Fil	8 5120	003 Protocol-Mouse Anoma	iyiTCP Flag Null or Misuse	Disabled • 1 Disabled • 1 Enabled • 1	Kan k	98 * 4 *
9	5120002	Protocol-Misuse Anomaly. IP Prot	9 5120	002 Protocol-Misuse Anoma	Iy: DP Protocol Null	Disabled • Enabled • 1	ter Ke	ps .*
10	F120001	Destand Mission Assessed 700 CD	10 5120	001 Protocol-Misuse Anoma	ly:TCP Shi Rooding	Enabled ¥ Enabled ¥ 1	Kor Value	os 🔹
No.	\$10001	R Name	Subm	it Reset Cen Stat	us Vi Event Thr	ilue Unit eshold	create szeszégés	

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
LPU/SPU	LPU/SPU	LPU/SPU	M P U	M P U	L P U / S P U	LPU/SPU	LPU/SPU	L P U / S P U
				SFl	J			19
				SFI	J			20
SFU								21
				SFI	J			22
L L J < 0 F J	LPU/0PU		L P V & P D	L P V / 0 P U		L P J < 0 P J	LPJ/0PJ	⊔ Р / ⊗ Р ∪
8	9	10	11	12	13	14	15	16

Slot	Quantity	Slot Width	Description
1 to 16	16	41 mm (1.6	Indicates the slots for LPUs and
		inches)	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	2	41 mm (1.6	Indicates the slots dedicated for
18		inches)	MPUs. The slots can house two
			MPUs to form 1:1 backup.
19 to	4	41 mm (1.6	Indicates the slots for SFUs. The
22		inches)	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 MPU	the	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 (Wid Depth x Height ^b)	lth ^a x	442 mm x 650 mm x 1420 mm (32 U). The depth is 770 mm covering the dust filter and cable rack.		
Installation positi	on	N68E cabinet or a standard 19-inch cabinet		
Weight	Empt y chassi s	94.4 kg		
	Full config uratio n (maxi mal)	233.9 kg		
Power specificat	ions			
Power supply	DC	8 hot-swappable PEM modules		
mode	AC	8 PEM modules+2 external AC power chassises		
Rated input	DC	-48 V		
voltage	AC	175 V AC to 264 V AC; 50/60 Hz		
Maximum input	DC	-72 V to -38 V		
voltage range	AC	90 V AC to 264 V AC; 50/60 Hz		
Typical power	DC	7387 W		
(six LPUF-240s and nine SPUs are configured.)	AC	7858 W		
Maximum	DC	8930 W		
Power ((six LPUF-240s and nine SPUs are configured.)	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 spe	ecificatio	ns			
System reliability	MTB F (year)	25			
	MTT R (hour)	0.5			
Ambient temperature ^c	Long- term ^d	0°C to 45°C			
	Short- term	-5°C to 50°C			
	Rema rks	Limit of the temperature change rate: 30°C/hour			
Storage temperatu	ure	-40°C to 70°C			
Ambient relative	Long- term	5% RH to 85% RH, no coagulation			
humidity	Short- term	5% RH to 95% RH, no coagulation			
Storage relative h	umidity	0% RH to 95% RH			
Long-term altitud	e	Lower than 3000 m			
Storage altitude		Lower than 5000 m			
NOTE a. The width does	not include	e 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	I	2	3	4	9	11	10	5	6	7	8
			LPU/SPU	LPU/SPU	S R U	SFU	S R U				
1		2	3	4	9	11	10	5	6	7	8

Slot Name	Slot Number	Quan tity	Slot Width	Remarks
LPU/SP U	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 specif	fications	
Processing un	it 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 SRU		2 (slots 9 and 10)
slots	SFU	1 (slot 11)
	LPU/SPU	8 (slots 1 and 8)

Item		Description	
Dimensions a	nd 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 configuratio n (maximal)		112.9 kg	

Power specifications		
Power	DC	4 hot-swappable PEM modules
supply mode	AC	4 PEM modules+1 external AC power chassis
Rated input	DC	-48 V
voltage	AC	175 V AC to 264 V AC; 50/60 Hz
Maximum	DC	-72 V to -38 V
input voltage range	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	DC	4823 W
Power (Three LPUF-240s and five SPUs are configured.)	AC	5132 W
Heat dissipat	ion	
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	t specifications		
System reliability	MTBF (year)	25	
	MTTR (hour)	0.5	
Ambient	Long-term ^d	0°C to 45°C	
temperature	Short-term	-5°C to 50°C	
	Remarks	Limit of the temperature change rate: 30°C/hour	
Storage tempe	erature	-40°C to 70°C	
Ambient	Long-term	5% RH to 85% RH, no coagulation	
relative humidity	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 altitud	de	Lower than 5000 m	
1			

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-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 ₀

Board distribution in the board cage of the Anti-DDoS8030

Slot	Slot	Quant	Slot	Remarks
Name	Number	ity	Width	
LPU/SPU	1 to 3	3	41 mm (1.6	These slots are used to hold SPUs or

Slot Name	Slot Number	Quant ity	Slot Width	Remarks
			inches)	LPUs.
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 specifica	tions	
Processing unit of	f the MPU	Main frequency: 1 GHz
BootROM capaci	ty of the MPU	1 MB
SDRAM capacity	v 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 (Wid Height ^b)	th ^a x Depth x	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 positi	on	N68E cabinet or a standard 19-inch cabinet
Weight	Empty chassis	DC chassis: 15kg
		AC chassis: 25kg
	Full	DC chassis: 30.7 kg
	(maximal)	AC chassis: 40.7 kg
Power specificat	ions	
Power supply	DC	Double hot-swappable power

Item		Description
mode		modules
	AC	Double hot-swappable power modules
Rated input	DC	-48 V
voltage	AC	175 V AC to 264 V AC; 50/60 Hz
Maximum input	DC	-72 V to -38 V
voltage range	AC	90 V AC to 264 V AC; 50/60 Hz
Typical power	DC	1066 W
(One LPUF-120 and two SPUs are configured.)	AC	1185 W
Maximum	DC	1272 W
Power (One LPUF-120 and two SPUs are configured.)	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 sp	ecifications	
System	MTBF (year)	25
reliability	MTTR (hour)	0.5
Ambient	Long-term ^d	0°C to 45°C
temperature	Short-term	-5°C to 50°C
	Remarks	Limit of the temperature change rate: 30°C/hour
Storage temperate	ure	-40°C to 70°C
Ambient relative	Long-term	5% RH to 85% RH, no coagulation
numiaity	Short-term	5% RH to 95% RH, no coagulation
Storage relative h	umidity	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 o b. The height is 1 U (1 U = 1.75 inches, unit defined in International Electrotecher standards.	of the mounting ear attached. or about 44.45 mm), which is a height nical Commission (IEC) 60297
c. The measurement point of the tempera floor and 0.4 m in front of the cabinet wi	ture and humidity is 1.5 m over the thout the front and the back doors.
d . Short-term operation means that the c exceed 96 hours and the accumulated op 15 days. Otherwise, it is called long-term	continuous operation time does not eration time per year does not exceed n 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

MPU 1: 1 backup • Routing protocol • Configuration management • NMS	 Patch management Forwarding table synchronization Syslog 	 System status monitoring HA status monitoring Others
LPU Packet forwarding Layer2 protocol processing Link status monitoring Statistics QoS ARP table maintenance MAC table maintenance	Switch network N+1 backup	FW-SPU Packet resolution Session table maintenance Security policy IPv4/IPv6 NAT VPN IPS-SPU Anti-DDoS SPU

• 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

•	Addition the state of the second	REPAIRE TRANSPORT	•
•			

• 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 GenieATM6365and GenieATM6333

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

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

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

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.





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:

ID		Severity	Duration	Start Time End Time	Direction	Туре	Resource
3270		Red 40.80 Kpps over 256.00 pps	50 mins	04-28 15:29 to 04-20 16:19	Incoming	Protocol-Misuse ICMP Misuse pps	[Global] Home 202.153.202.167
affic -			The second	244 E		Remarks	(10)
	Grap	Time: 2008 • 04 • 28	- 115	: 26* Duration: 01	hours 00		
		75000.00 4 4 4 4 4 4	15150	15:00 15:10 1	-120 -120-00,00		
		60000.00 -			-60000,00		
	22	45000.00 - 4			-45000.00 g		
	55	30000.00			-30000.00	1 - [11]]R1011_05R.19
		15000.00	1		-15000.00		
		0.00			0.00		
raffic C	hara	teristics [2008-04-28]	5:32001	TNET			
raffic C	hara	teristics [2008-04-28 1	Si BC	TNET	Dectination IRud Add		VICTI
raffic C Source I	harai Pv4 A	teristics [2008-04-28 1 ddress	B'B'C	TNET	Destination IPv4 Add	ress bps	VICTI
Source I	hara Pv4 A	ddress	••• *B C	TNET	Destination IPv4 Add	ress bps 393.48M	
raffic C Source I 61.146.16 123.131.1	hara Pv4 A 50.11	teristics [2008-04-28] ddress 76.64M 87.20M	•• B C		Destination IPv4 Add 202.153.202.167	ress bps 393.48M	VICTI 40.80K
raffic C Source I 61.146.16 123.131.1 61.185.13	harat Pv4 A 50.11 109.103 36.71	teristics [2008-04-28 1 ddress 76.64M 87.20M 66.88M	••• B C	11.44K 8.09K 6.17K	Destination IPv4 Add 202.153.202.167 Destination Port	ress bps 393.48M bps	VICTII 40.80K
raffic C Source I 61.146.16 123.131.1 61.185.13 218.93.11	harat Pv4 A 50.11 109.103 36.71 14.126	teristics [2008-04-28 1 ddress 76.64M 87.20M 66.86M 63.53M	^{5:3:} BC	11 44K 8.09K 6.17K 5.89K	Destination IPv4 Add 202.153.202.167 Destination Porc Icmp/0	ress bps 393.48M bps 259.34M	VICTII 40.80K
raffic C Source 1 61.146.10 123.131.1 61.185.13 218.93.11 221.199.2	haron Pv4 A 50.11 109.103 36.71 14.126 203.228	teristics [2008-04-28 1 ddress 76.54M 87.20M 66.86M 63.53M 27.54M	5:3 *B*C	11.44K 8.09K 6.17K 5.89K 2.58K	Destination JPv4 Add 202.153.202.167 Destination Porc komp/0 komp/2048	ress bps 393.46M bps 258.34M 135.15M	Pp* 40.80K Pp5 29 10K 11.62K
raffic C Source 1 61.146.16 123.131.1 61.185.13 218.93.11 221.199.2 222.170.1	harai Pv4 A 50.11 109.103 36.71 14.126 203.220 19.134	teristics [2008-04-28 1 ddress 76.54M 97.20M 66.80M 63.53M 27.54M 17.46M	5:3 *B*C	11.44K 0.09K 6.17K 5.09K 2.58K 1.63K	Destination IPv4 Add 202.153.202.167 Destination Port komp/0 komp/2048	ress bps 393.40M bps 259.34M 135.15M	PP* 40.80K 29.10K 11.62K
raffic C Source 1 123.131.1 61.185.13 218.93.11 221.199.3 222.170.1 125.120.6	hara Pv4 A 50.11 109.103 36.71 14.126 203.228 19.134 39.255	tteristics [2008-04-28 1 ddress 76.64M 87.20M 68.56M 63.55M 17.46M 9.96M	*** B 'O	11.44k 0.09K 6.17K 5.79K 2.58K 1.53K 933.30	Destination IPv4 Add 202.153.202.167 Destination Port icmp/0 icmp/2048	ress 393.46M bps 259.34M 135.15M	PP* 40.80K PP5 29.10K 11.62K
raffic C Source 1 123.131.1 61.185.13 218.93.11 221.199.2 222.170.1 125.120.6 58.56.12	Pv4 A 50.11 109.103 36.71 14.126 203.226 19.134 39.255 130	teristics [2008-04-28 1 ddress 76.644 87.204 66.854 63.534 27.544 17.464 9,964 9,964 9,964	••• B C	11.44k 8.09k 6.17k 5.99k 2.58k 1.53k 933.30 950.00	Destination IPv4 Add 202.153.202.167 Destination Porc komp/0 komp/2048	ress bps 393.46M bps 258.34M 135.15M	PP# 40.00K PP# 29.10K 11.62K
raffic C Source 1 61 146 16 123 131 1 61 185 13 218 93 11 221 199 2 222 170 1 125 120 6 58 56 12 61 164 13	Pv4 A 50.11 109.103 36.71 14.126 203.228 19.134 39.255 130 30.26	teristics [2008-04-28] ddress 76,644 66,854 63,534 63,534 17,464 9,964 9,964 0,944 0,264	••• B C	11.44K 0.09K 6.17K 5.69K 2.59K 15.33K 033.30 650.00 703.30	Destination IPv4 Add 202.153.202.167 Destination Port Icomp/2048	ress 393.404 8ps 250.3444 135.154	PP* 40.00K PP* 20.10K 11.62K
raffic C Source 1 61.146.16 123.131.1 61.165.13 218.93.11 221.199.2 222.170.1 125.120.6 59.56.12 61.164.13 117.88.99	harai Pv4 A 50.11 109.103 36.71 14.126 203.228 19.134 39.255 130 30.26 4.221	teristics [2008-04-28] ddress 76.64M 07.50M 06.55M 05.55M 17.64M 0.90M 0.90M 0.90M 0.90M 0.90M 0.90M	•• ·B C	11.44K 0.09K 6.17K 5.69K 1.53K 933.30 850.00 783.30 650.00	Destination IPv4 Add 202153.202167 Desumation Porc icmp/0 icmp/2048	ress bps 393.40M bps 263.34M 135.15M	PP* 40.80K PP* 29.10K 11.62K
raffic C Source 1 61.146.16 123.131.1 61.165.13 218.93.11 221.199.3 222.170.1 125.120.6 58.56.12 61.164.13 117.88.99 222.1614	harai Pv4 A 50.11 109.103 36.71 14.126 203.228 19.134 39.255 130 30.26 4.221 49.211	teristics [2008-04-28] ddress 76,644 07,204 07,204 07,204 07,204 07,204 07,204 07,204 0,9	••• B C	11.44K 0.09K 6.17K 5.89K 2.56K 1.63K 933.30 850.00 783.30 650.00 103.30	Destination IPv4 Add 202153-202167 Destination Porc kmp/2048	ress bps 393,40M bps 280,34M 135,15M	PP* 40.80K PP* 20.10K 11.62K
raffic C Source 1 61.146.18 123.131.1 61.185.13 218.93.11 221.199.2 222.170.1 125.120.6 59.56.12 61.164.13 117.88.94 222.161.4 222.161.4	hara Pv4 A 50.11 109.103 36.71 14.126 203.228 19.134 39.255 130 30.26 4.221 49.211 3.88	teristics [2008-04-28 1 ddress 76.540 66.800 65.530 65.530 9.3530 9.35400 9.35400 9.35400 9.35400 9.35400 9.35400 9.35400 9.354000 9.354000000000000000000000000000000000000	•• ·B C	11.44K 0.09K 6.17K 5.89K 1.63K 933.30 850.00 783.30 650.00 183.30 333.30	Destination IPv4 Add 202153.302167 Destination Port kmp/2049	ress 8pr 393.40M hps 280.34M 135.16M	PF 40.00K PP 20.10K 11.62K
raffic C Source 1 61 146 10 123 131 1 61 165 13 218 93 11 221 199 2 222 170 1 125 120 6 58 56 12 61 164 13 117 86 9 222 161 4 221 725 222 161	hara Pv4 A 50.11 109.103 36.71 14.126 203.226 19.134 39.255 130 30.26 4.221 49.211 3.88 228.50	teristics [2008-04-28] 50%es 70.56M 70.56M 70.56M 70.56M 70.56M 70.56M 70.56M 9.35M 9.39M 9.39M 9.39M 7.00M 9.39M 7.00M 9.39M 7.00M 9.39M 7.00M 1.11,127 9.00 (11,127) 9.00 (11,12	••• B C	11.44K 0.09K 6.17K 5.69FK 2.50K 1.63K 953.30 850.00 783.30 650.00 933.30 650.00 933.30 933.30 933.30 933.30	Destination IPv4 Add 202153-202167 Destination Port Icmp/0 Icmp/2049	ress kps 393.40M kps 293.34M 135.15M	VICTII 97 20 JOR 20 10R 11 62R
raffic C Source 1 61.146.11 123.131.1 61.185.12 218.99.3 222.170.1 125.120.6 58.56.12 61.164.13 117.88.94 222.101.4 221.725 220.109.2 220.109.2	harat Pv4 A 109 103 36 71 14 126 203 228 19 134 39 255 130 30 26 4 221 49 211 3 88 220 50 27 9	territics [2000-04-20] ddess 	••• B C	11.44K 0.09K 6.17K 5.89K 2.50K 15.3X 650.00 703.30 650.00 303.30 106.70 133.30	Destination IPv4 Add 202153.302167 Destination Por iomp/0 kmp/2048	ress 203.48M bps 259.38M 135.16M	P# 20.10K
raffic C Source 1 61.146.1 123.131.1 61.165.12 218.93.11 221.993.1 222.170.1 125.120.6 59.56.12. 69.56.12. 61.164.12 117.88.94 222.161.4 221.7.252 220.169.5 218.26.15 218.26.15 218.26.15 218.26.15 218.26.15 218.26.15 219.27.15 219.26.15 219.27.15	hara Pv4 A 109.103 36.71 14.126 203.228 19.134 39.255 130 30.26 4.221 49.211 3.88 220.50 37.9 159	teristics [2008-04-28] 50%es 70.66M 70.56M 70.56M 70.56M 70.56M 70.56M 70.56M 9.35M 70.56M 9.39M 9.39M 70.06M 70.00M 9.39M 70.00M 19.30M 70.00M 19.30M 70.00M 19.30M 70.00M 19.30M 70.00M 19.30M 19	5-3 B C	11.44K 0.09K 6.17K 5.69K 2.26K 1.63K 533.30 160.00 333.30 150.30 333.30 150.30 133.30 130.30	Destination IPv4 Add 202153-202167 Destination Port Icmp/0 Icmp/2049	ress kps 393.40M kps 293.34M 135.15M	VICTII 97 20 JOR 20 106 11 626

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.



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	Operating system	Windows Server 2003 R2 Standard with SP2
Windows)	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
НА	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



