Huawei Technical Proposal

For XX Anti-DDoS Project

Issue	01
Date	2016-6-8

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Huawei is pleased to answer to XX Anti-DDoS RFP. 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.

After carefully reading XX's requirements, Huawei understand that XX wants to …

//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 carefully reading HGC's requirements, Huawei understand that HGC want to deploy Anti-DDoS to protect its internal subscribers from various kind of DDoS attack. The key requirements are summarized as following:

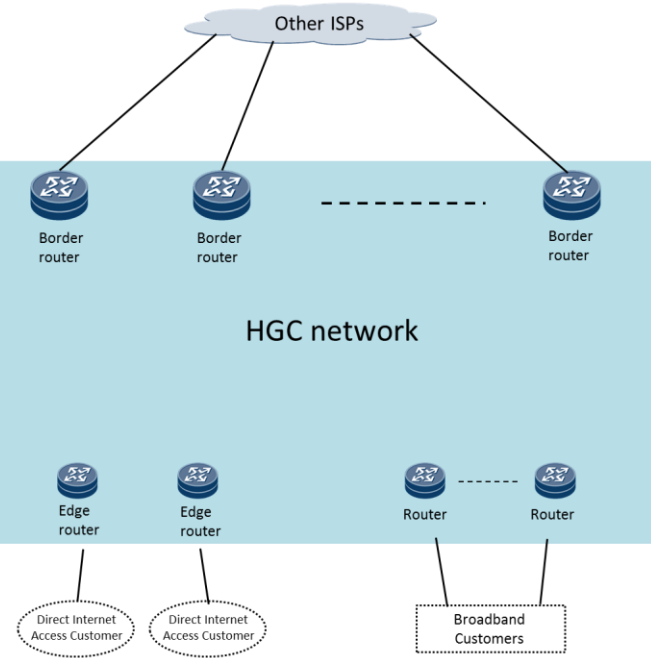
- *The solution should have 10Gbps (~18.4Mpps @68byte) capacity and be able to expanded to 40Gbps (~73.6Mpps @68byte)*
- *The solution should provide notification and reporting system, be capable of notifying customers automatically in case their traffic is under DDoS attack*
- *The solution should provide high availability and prevent single point of failure to the network service*

2 Huawei Proposed Solution for XX

2.1 XX Network Topology

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

//For example:

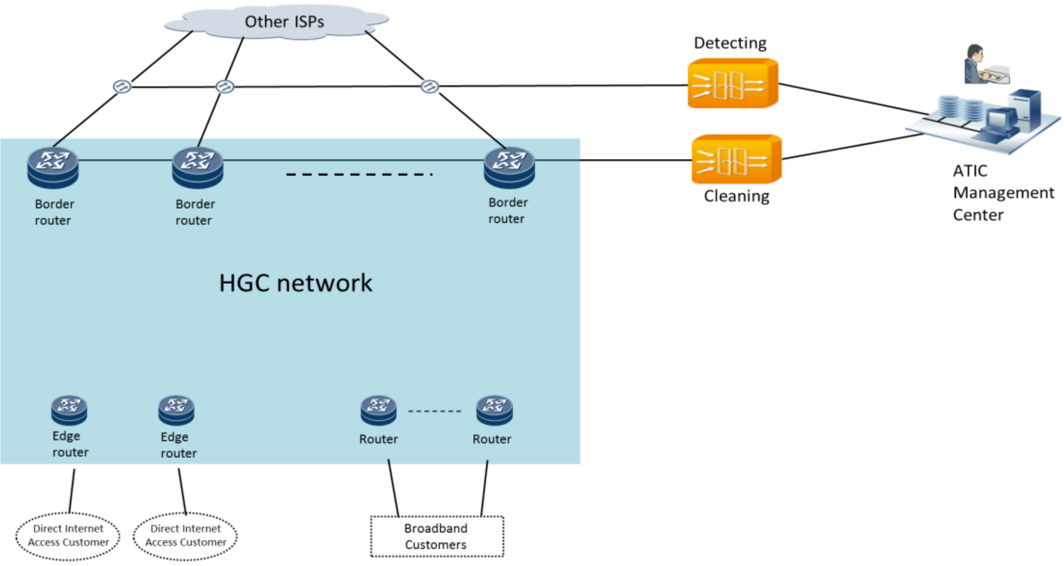


XX's network are mainly comprised of 8 x border routers (connecting to the other Internet Service Providers), 2 x edge routers (connecting to Direct Internet Access customers) and a set of routers in XX's broadband network (connecting to Broadband customers).

2.2 Huawei Proposed Anti-DDoS Solution

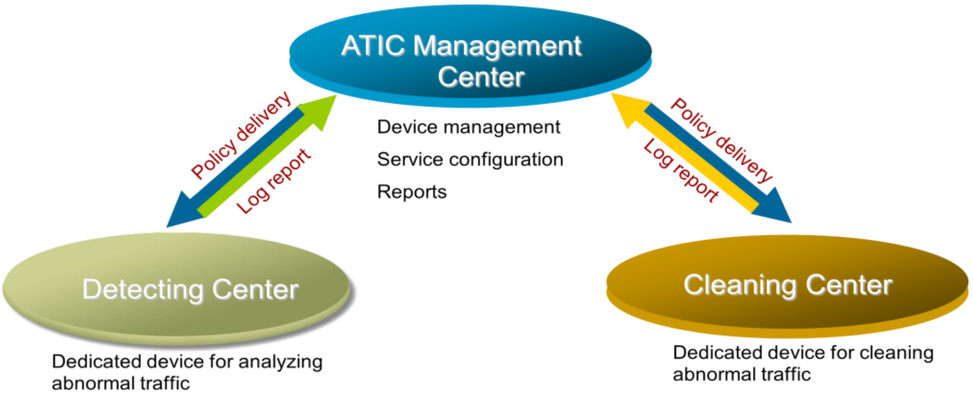
//This chapter describes the Huawei Anti-DDoS solution for XX customer.

//For example:



Based on the capacity and performance requirements in the RFP, Huawei propose Anti-DDoS8160 for XX's network, deploy in off-line mode: Per-packet detecting by split the traffic to detecting system 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**

The detecting device acts as a probe to analyze traffic and security threats on the live network in a timely manner. With the refined detecting technology of Huawei, the detecting device analyzes the volume and abruptness of TCP, UDP, HTTP, and DSN traffic, and accurately locates attack targets based on the destination IP address. This offers evidence for future dynamic traffic diversion in off-line mode.

- **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 Quantities

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

//For example:

Huawei Anti-DDoS detecting and cleaning device contains three models: Anti-DDoS8030, Anti-DDoS8080 and Anti-DDoS8160. All the software and feature is the same for the three models, the only different is the performance and expansion capability. Anti-DD8160 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.

Huawei proposed Anti-DDoS8160 for XX's network:

Devices	***Chassis***	***Detect board***	***Clean board***	***Total***	***Maximum Expansion Capacity***
Detecting	*Anti-DDoS 8160*1*	*160Gbps*	*NA*	*160Gbps*	*1440Gbps*
Cleaning	*Anti-DDoS 8160*1*	*NA*	*80Gbps*	*80Gbps*	*1440Gbps*
ATIC	*ATIC system *1 (ATIC management software + Hardware server + Windows Server platform software + auxiliaries)*			*NA*	*NA*

Note:

Attention：One SPU board(two SPC card) maximum throughput=160Gbps is the best performance under 1500bytes, for small packet and IMIX, the performance is lower.

1. ADS-SPC-40:

Detecting: 1500bytes=40Gbps; IMIX(1500bytes:512bytes:64bytes=7:4:1)=10Gbps; 64bytes=5Gbps;

Cleaning: 1500bytes=40Gbps; IMIX(1500bytes:512bytes:64bytes=7:4:1)=20Gbps; 64bytes=10Gbps.

2. ADS-SPC-80:

Detecting: 1500bytes=80Gbps; IMIX(1500bytes:512bytes:64bytes=7:4:1)=20Gbps; 64bytes=10Gbps;

Cleaning: 1500bytes=80Gbps; IMIX(1500bytes:512bytes:64bytes=7:4:1)=40Gbps; 64bytes=20Gbps.

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:

//This chapter describes the working principle of Huawei Anti-DDoS Solution

//The detecting board and cleaning board can be deployed in separated chassis or be deployed //within the same chassis (if the free slots are enough), the working principle is the same for //these two cases. Choose one of the following two figures based on the projects. The //following description is the same.

Figure1: Detecting board and cleaning board are deployed in separated chassis

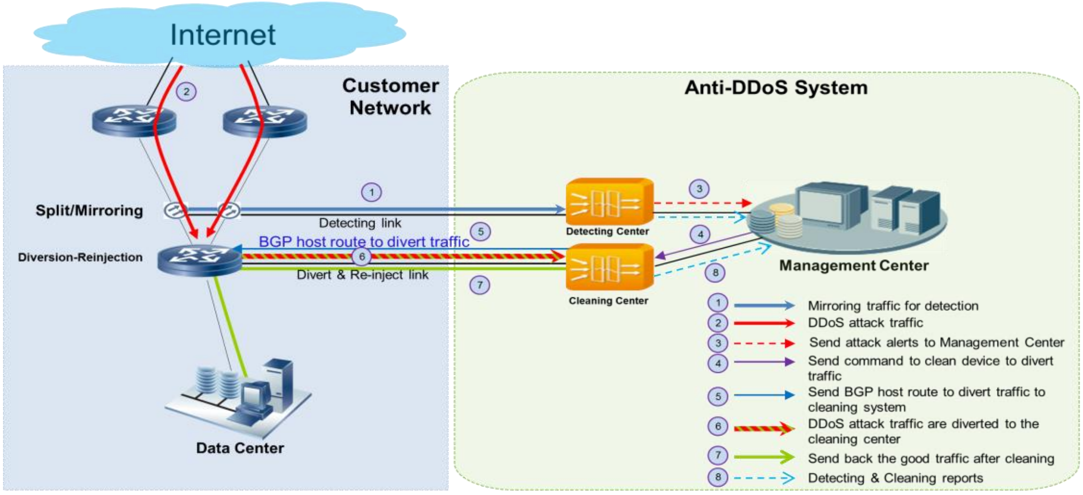
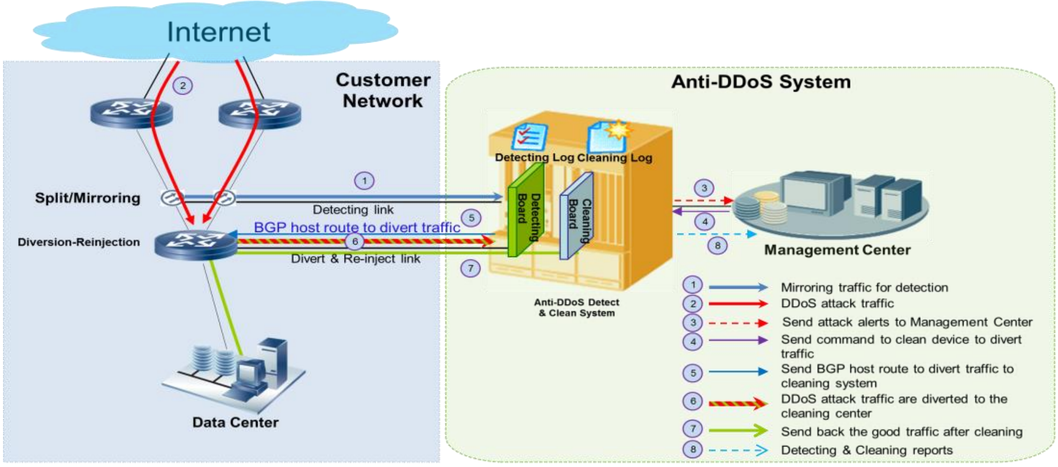

Internet
Customer Network
Anti-DDoS System
2
Split/Mirroring
Diversion-Reinjection
1
Detecting link
BGP host route to divert traffic
5
6
Divert & Re-inject link
7
Detecting Center
Cleaning Center
3
4
8
Management Center
Data Center
1 Mirroring traffic for detection
2 DDoS attack traffic
3 Send attack alerts to Management Center
4 Send command to clean device to divert traffic
5 Send BGP host route to divert traffic to cleaning system
6 DDoS attack traffic are diverted to the cleaning center
7 Send back the good traffic after cleaning
8 Detecting & Cleaning reports

Figure2: Detecting board and cleaning board are deployed within the same chassis


Internet
Customer Network
Anti-DDoS System
2
Split/Mirroring
Diversion-Reinjection
1
Detecting link
BGP host route to divert traffic
5
6
Divert & Re-inject link
7
Detecting Log
Cleaning Log
Detecting Board
Cleaning Board
Anti-DDoS Detect & Clean System
3
4
8
Management Center
Data Center
1 Mirroring traffic for detection
2 DDoS attack traffic
3 Send attack alerts to Management Center
4 Send command to clean device to divert traffic
5 Send BGP host route to divert traffic to cleaning system
6 DDoS attack traffic are diverted to the cleaning center
7 Send back the good traffic after cleaning
8 Detecting & Cleaning reports

1) Use optical splitter to split one copy of the traffic to the Detecting center for detection

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

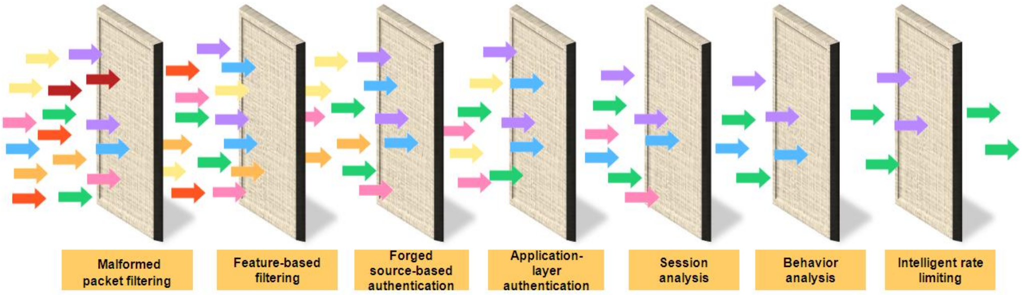
3.2.1 Fast Detection time and Application layer detection

Per-packet detection method will detect all packets of the original network traffic; it can detect the DDoS attack in 2~3 seconds and start cleaning, while traditional flow based detection method need several minutes. Most of the servers cannot endure minutes of DDoS attack before crash, per-packet detection method is more suitable for this kind of scenario.

Per-packet detection method can detect not only large bandwidth attack traffic, but also application layer DDoS attack which usually does not consume too much network bandwidth while enough to make the victim servers not able to provide services . Netflow detection method is based on network traffic samples, it is helpless during facing application layer DDoS attack such as http, DNS, etc, while per-packet detection method can deal with it.

3.2.2 Muli-layer defense

The cleaning system uses the layer-to-layer defense mechanism using the malformed packet check, feature-based filtering, source authentication, session analysis, behavior analysis, intelligent rate limiting, and anti-worms/Trojan horses/zombies. The powerful defense mechanism can tackle various DDoS attacks, safeguarding the server.


Malformed packet filtering
Feature-based filtering
Forged source-based authentication
Application-layer authentication
Session analysis
Behavior analysis
Intelligent rate limiting

3.2.3 High Availability

1. **Product High Availability**

   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.

2. **Solution Architecture High Availability**

   //Choose one of the following two figures based on the projects. The following description is //the same.

   Figure1: Detecting board and cleaning board are deployed in separated chassis

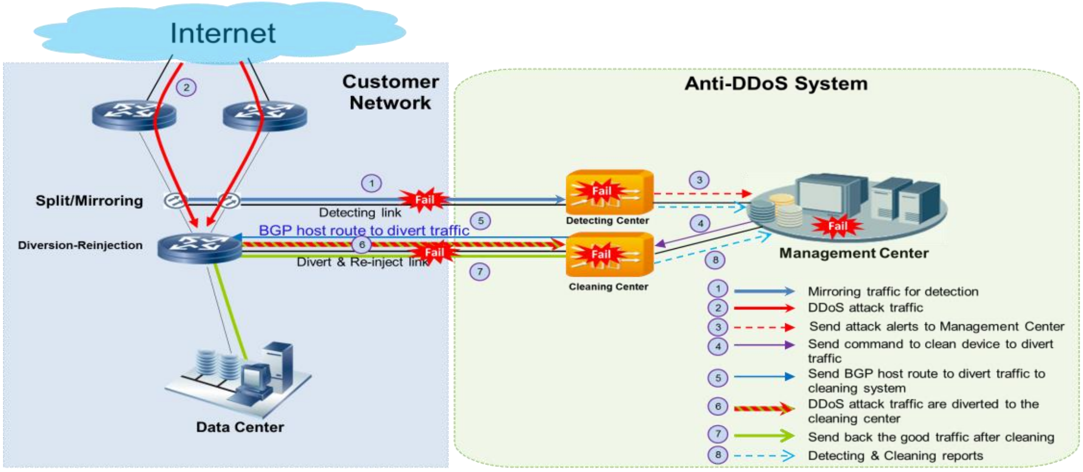
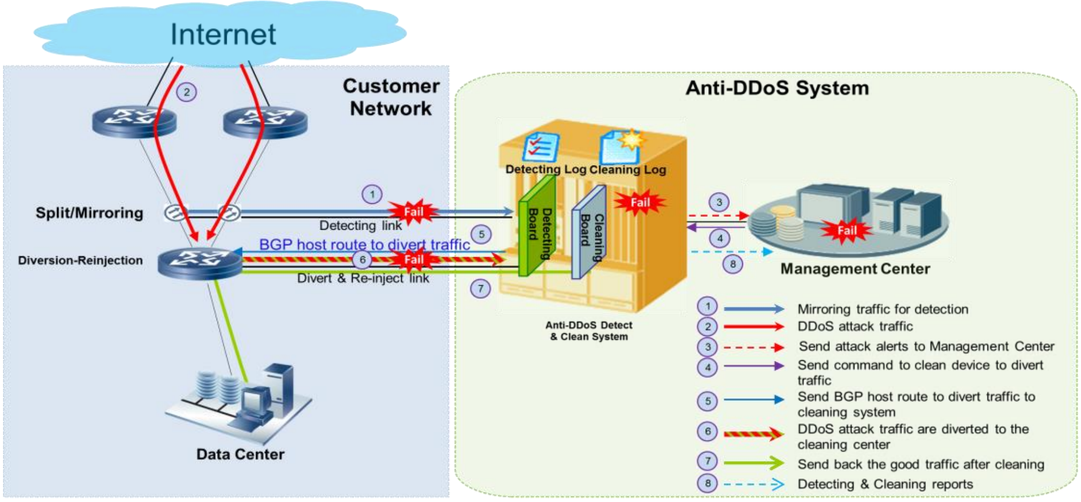

Internet
Customer Network
Anti-DDoS System
Split/Mirroring
Diversion-Reinjection
Detecting link
BGP host route to divert traffic
Divert & Re-inject link
Fail
Detecting Center
Cleaning Center
Management Center
Data Center
1 Mirroring traffic for detection
2 DDoS attack traffic
3 Send attack alerts to Management Center
4 Send command to clean device to divert traffic
5 Send BGP host route to divert traffic to cleaning system
6 DDoS attack traffic are diverted to the cleaning center
7 Send back the good traffic after cleaning
8 Detecting & Cleaning reports

Figure2: Detecting board and cleaning board are deployed within the same chassis


Internet
Customer Network
Anti-DDoS System
Split/Mirroring
Diversion-Reinjection
Detecting link
BGP host route to divert traffic
Divert & Re-inject link
Fail
Detecting Log
Cleaning Log
Detecting Board
Cleaning Board
Anti-DDoS Detect & Clean System
Management Center
Data Center
1 Mirroring traffic for detection
2 DDoS attack traffic
3 Send attack alerts to Management Center
4 Send command to clean device to divert traffic
5 Send BGP host route to divert traffic to cleaning system
6 DDoS attack traffic are diverted to the cleaning center
7 Send back the good traffic after cleaning
8 Detecting & Cleaning reports

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.

3.2.4 Easy to manage

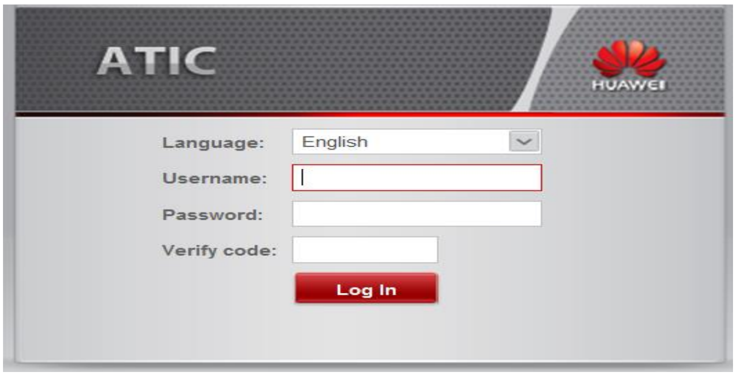
The AntiDDoS offers an intelligent traffic baseline learning system to free the administrator from configuring the threshold. To ease management and maintenance, Huawei proposes the easy-to-use GUIs as well as the excellent ATIC management system, which integrates device management, policy configuration,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

3.3 Management system

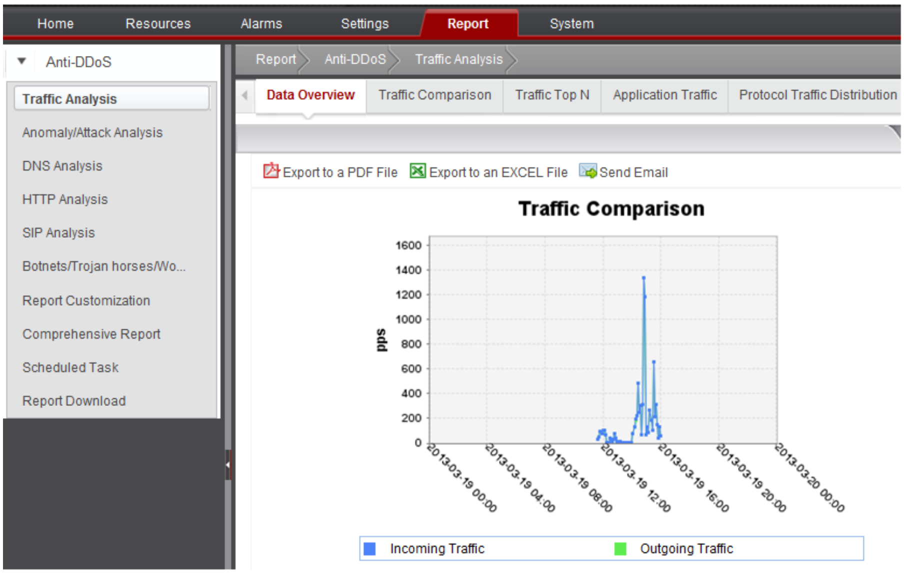
Huawei Anti-DDoS solution provides user friendly GUI management portal and powerful reports.

3.3.1 Management Portal

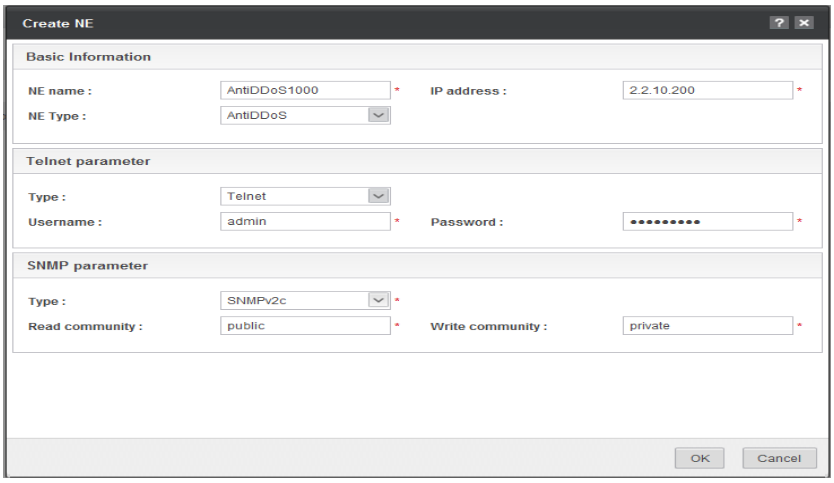
- **Login portal**



- **Home page**



- **System configuration**


Create NE

Basic Information

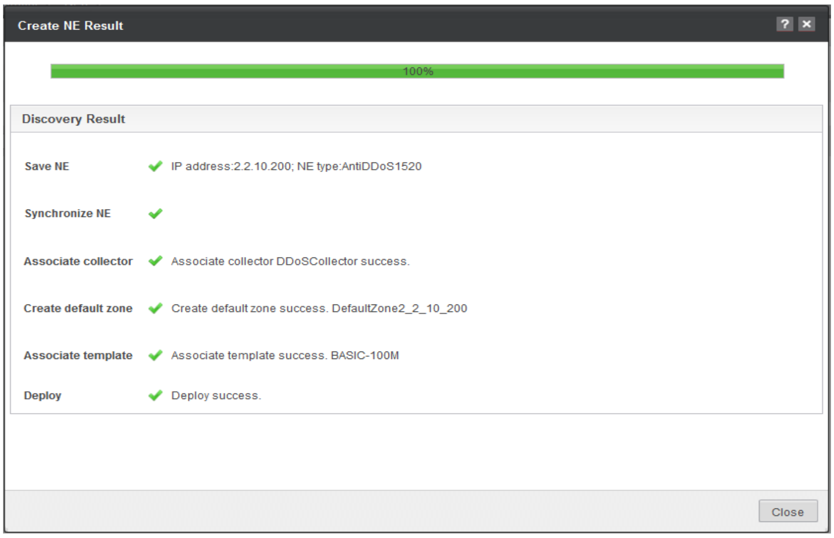
NE name : AntiDDoS1000 *
IP address : 2.2.10.200 *
NE Type : AntiDDoS

Telnet parameter

Type : Telnet
Username : admin *
Password : ●●●●●●●●●● *

SNMP parameter

Type : SNMPv2c *
Read community : public *
Write community : private *


Create NE Result

100%

Discovery Result

Save NE ✓ IP address:2.2.10.200; NE type:AntiDDoS1520

Synchronize NE ✓

Associate collector ✓ Associate collector DDoSCollector success.

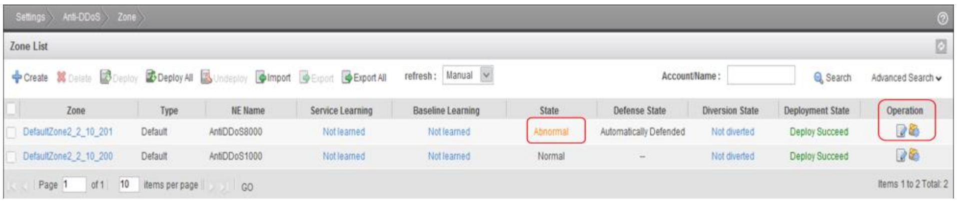
Create default zone ✓ Create default zone success. DefaultZone2_2_10_200

Associate template ✓ Associate template success. BASIC-100M

Deploy ✓ Deploy success.

- **Policy configuration**

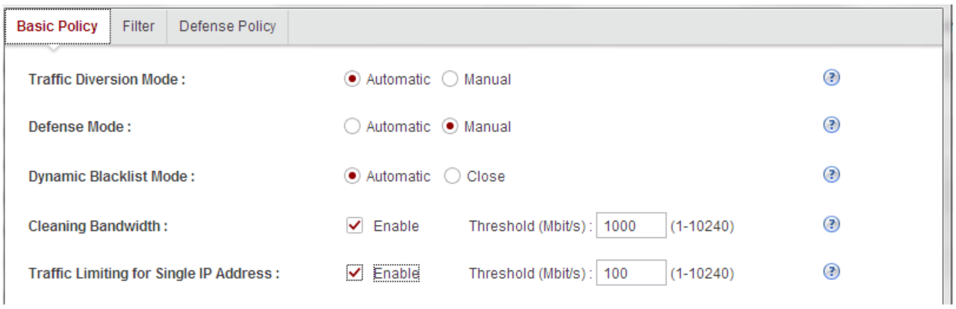
Step1: Auto Configure Zone



□	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	
□	DefaultZone2_2_10_200	Default	AntiDDoS1000	Not learned	Not learned	Normal	--	Not diverted	Deploy Succeed	

Page 1 of 1 10 items per page GO Items 1 to 2 Total: 2

Step2: Click Operation column item to see Policy



Traffic Diversion Mode : ● Automatic ○ Manual

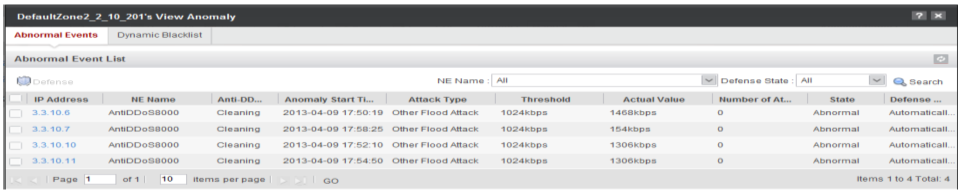
Defense Mode : ○ Automatic ● Manual

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)

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

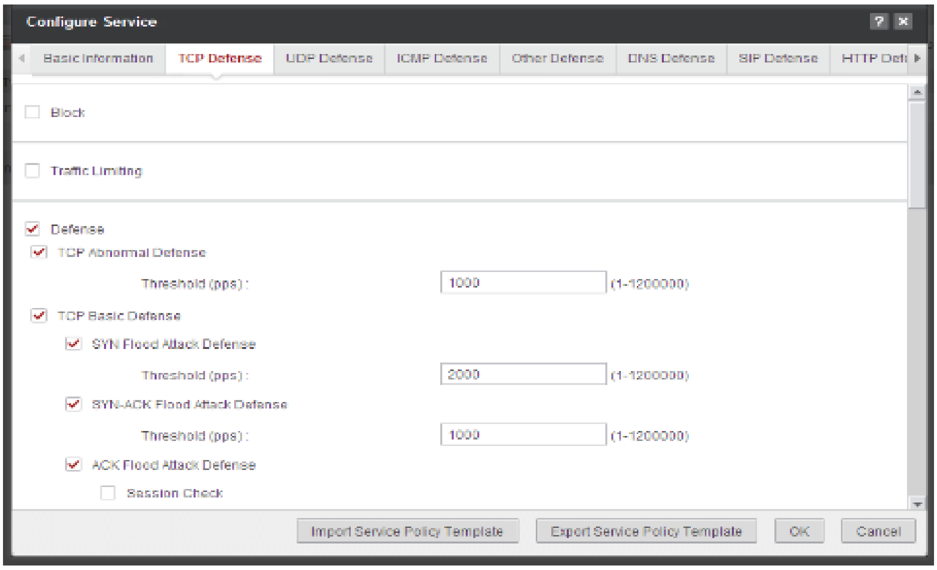


□	IP Address	NE Name	Anti-DD...	Anomaly Start Ti...	Attack Type	Threshold	Actual Value	Number of At...	State	Defense ...
□	3.3.10.6	AntiDDoS8000	Cleaning	2013-04-09 17:50:19	Other Flood Attack	1024kbps	1468kbps	0	Abnormal	Automaticall...
□	3.3.10.7	AntiDDoS8000	Cleaning	2013-04-09 17:58:25	Other Flood 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...

Page 1 of 1 10 items per page GO Items 1 to 4 Total: 4

Attack defense configuration example:

TCP attack defense configuration: Page1/4



□ Block

□ Traffic Limiting

☑ Defense

☑ TCP Abnormal Defense

Threshold (pps) : 1000 (1-1200000)

☑ TCP Basic Defense

☑ SYN Flood Attack Defense

Threshold (pps) : 2000 (1-1200000)

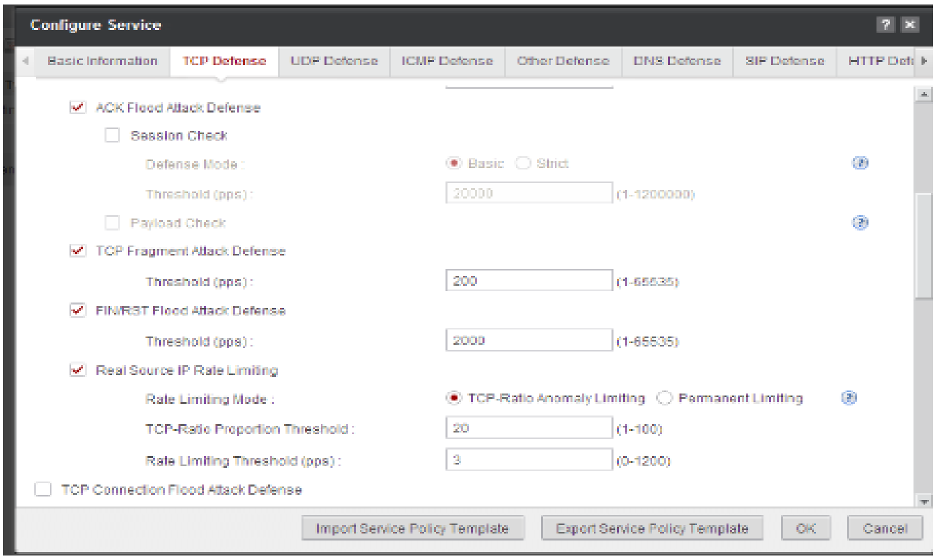
☑ SYN-ACK Flood Attack Defense

Threshold (pps) : 1000 (1-1200000)

☑ ACK Flood Attack Defense

□ Session Check

Page2/4



☑ ACK Flood Attack Defense

□ Session Check

Defense Mode : ● Basic ○ Strict

Threshold (pps) : 20000 (1-1200000)

□ Payload Check

☑ TCP Fragment Attack Defense

Threshold (pps) : 200 (1-65535)

☑ FIN/RST Flood Attack Defense

Threshold (pps) : 2000 (1-65535)

☑ Real Source IP Rate Limiting

Rate Limiting Mode : ● TCP-Ratio Anomaly Limiting ○ Permanent Limiting

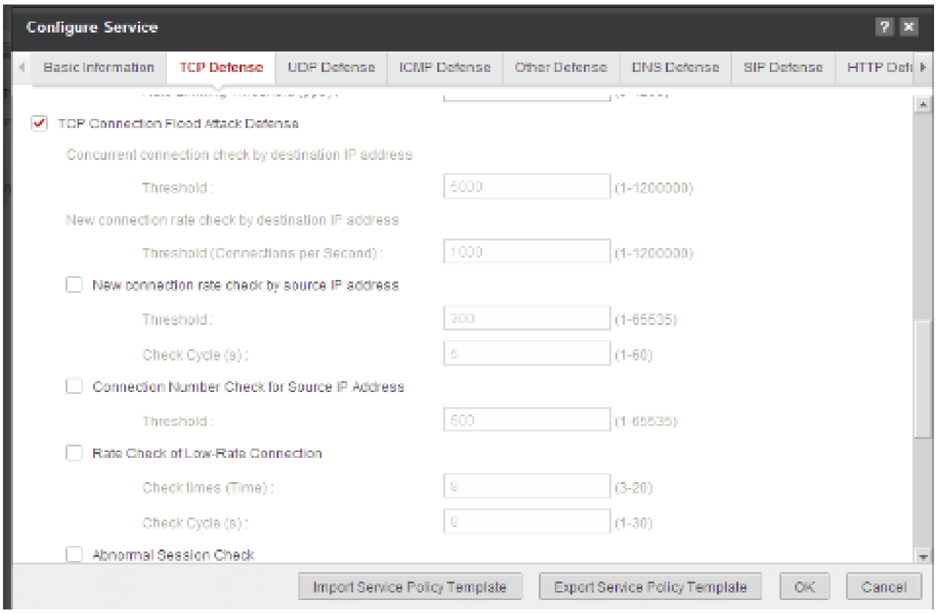
TCP-Ratio Proportion Threshold : 20 (1-100)

Rate Limiting Threshold (pps) : 3 (0-1200)

□ TCP Connection Flood Attack Defense

Import Service Policy Template
Export Service Policy Template
OK
Cancel

Page3/4



☑ TCP Connection Flood Attack Defense

Concurrent connection check by destination IP address

Threshold : 5000 (1-1200000)

New connection rate check by destination IP address

Threshold (Connections per Second) : 1000 (1-1200000)

□ New connection rate check by source IP address

Threshold : 200 (1-65535)

Check Cycle (s) : 5 (1-60)

□ Connection Number Check for Source IP Address

Threshold : 500 (1-65535)

□ Rate Check of Low-Rate Connection

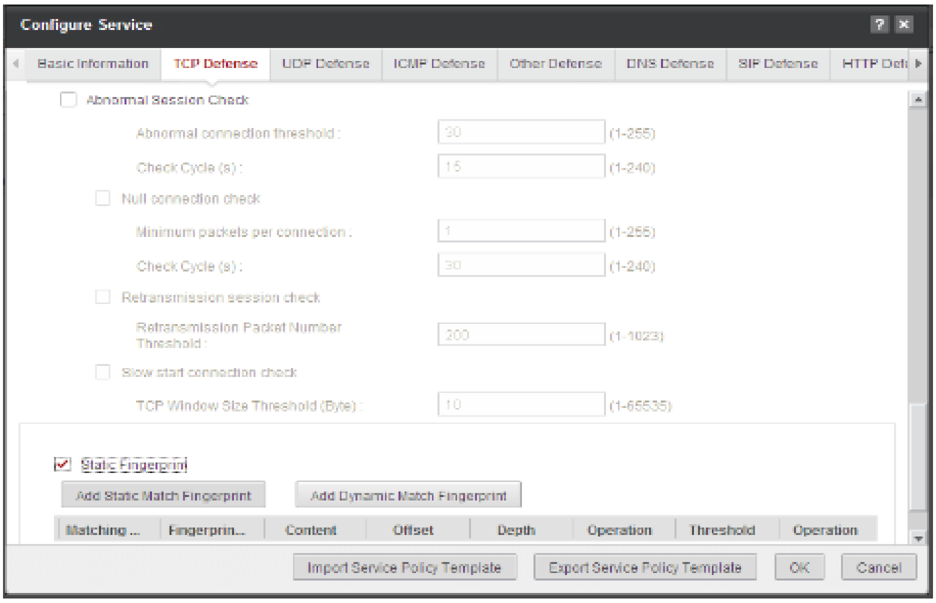
Check times (Time) : 8 (3-20)

Check Cycle (s) : 8 (1-30)

□ Abnormal Session Check

Import Service Policy Template
Export Service Policy Template
OK
Cancel

Page4/4



□ Abnormal Session Check

Abnormal connection threshold : 30 (1-255)

Check Cycle (s) : 15 (1-240)

□ Null connection check

Minimum packets per connection : 1 (1-255)

Check Cycle (s) : 30 (1-240)

□ Retransmission session check

Retransmission Packet Number Threshold : 200 (1-1023)

□ Slow start connection check

TCP Window Size Threshold (Byte) : 10 (1-65535)

☑ Static Fingerprint

Matching ...	Fingerprin...	Content	Offset	Depth	Operation	Threshold	Operation

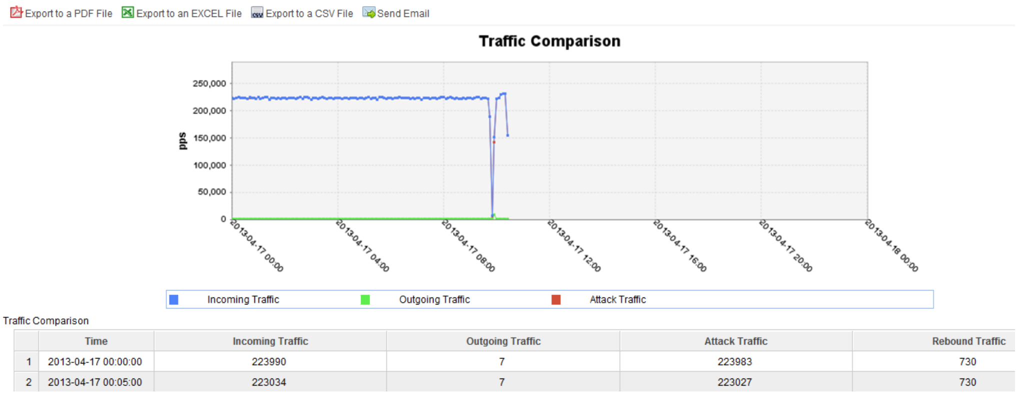
3.3.2 Reports

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**

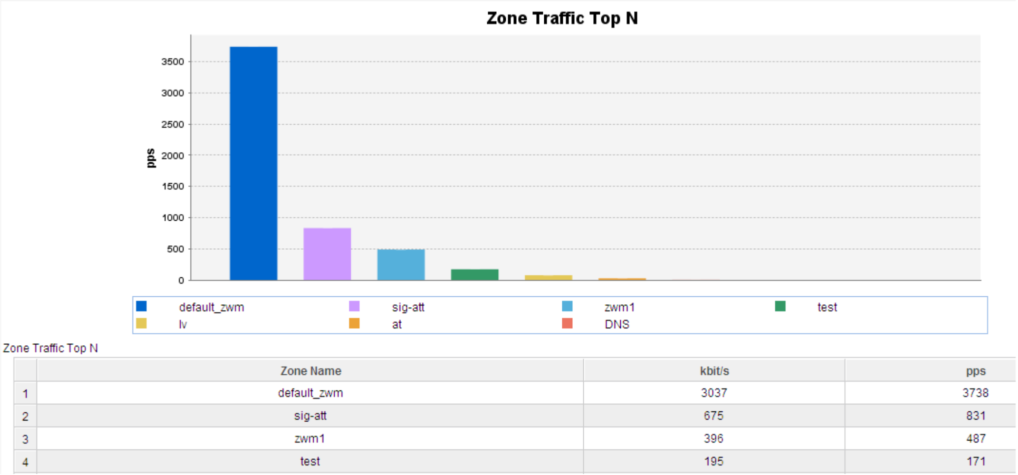


Traffic Comparison

	Time	Incoming Traffic	Outgoing Traffic	Attack Traffic	Rebound Traffic
1	2013-04-17 00:00:00	223990	7	223983	730
2	2013-04-17 00:05:00	223034	7	223027	730

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

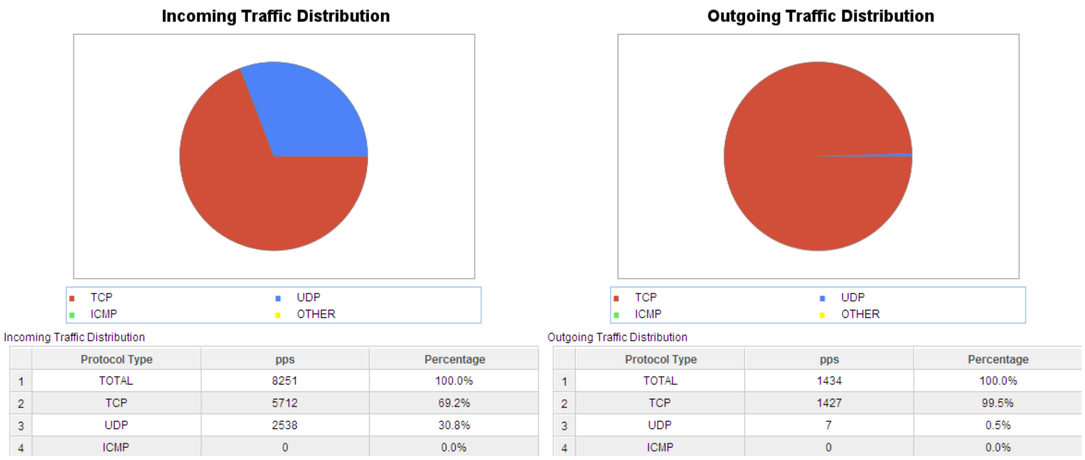


Zone Traffic Top N

	Zone Name	kbit/s	pps
1	default_zwm	3037	3738
2	sig-att	675	831
3	zwm1	396	487
4	test	195	171

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



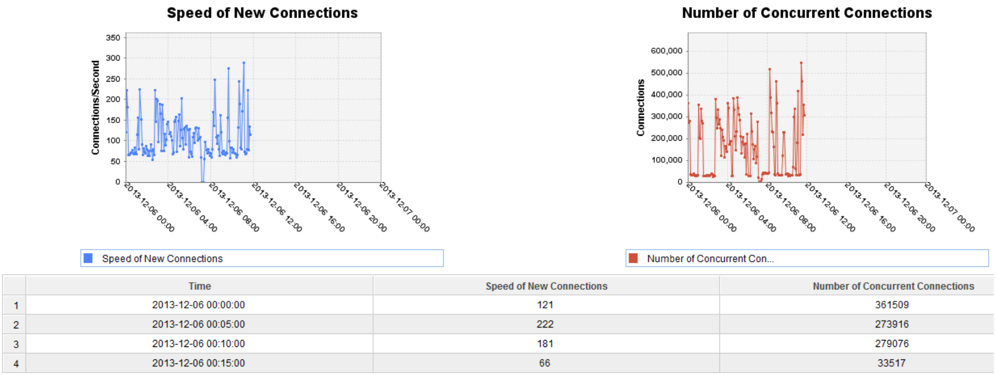
Incoming Traffic Distribution

	Protocol Type	pps	Percentage
1	TOTAL	8251	100.0%
2	TCP	5712	69.2%
3	UDP	2538	30.8%
4	ICMP	0	0.0%

Outgoing Traffic Distribution

	Protocol Type	pps	Percentage
1	TOTAL	1434	100.0%
2	TCP	1427	99.5%
3	UDP	7	0.5%
4	ICMP	0	0.0%

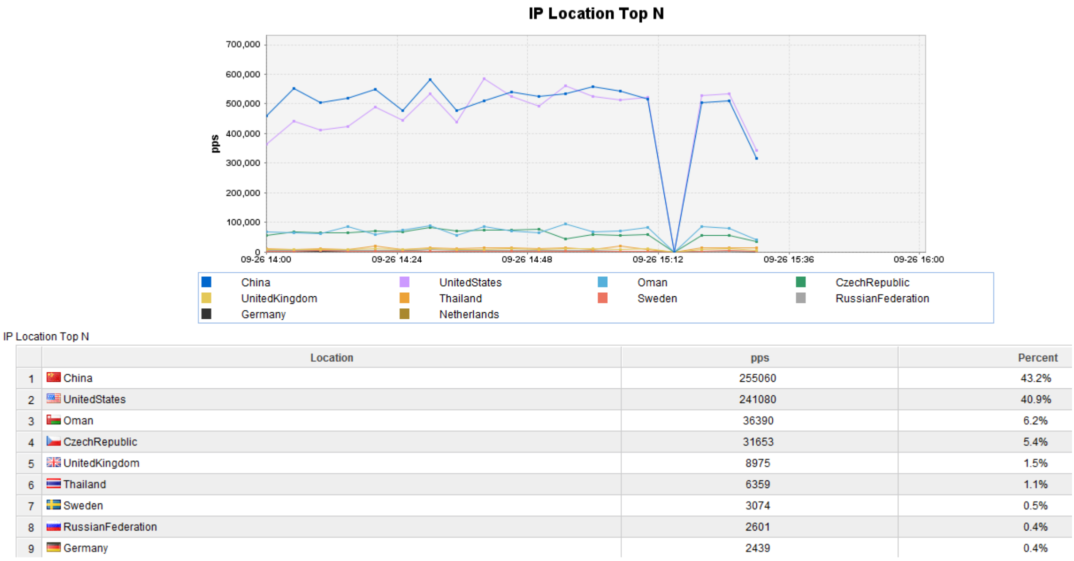
4) Number of new connections and concurrent connections by destination IP address



	Time	Speed of New Connections	Number of Concurrent Connections
1	2013-12-06 00:00:00	121	361509
2	2013-12-06 00:05:00	222	273916
3	2013-12-06 00:10:00	181	279076
4	2013-12-06 00:15:00	66	33517

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



IP Location Top N

	Location	pps	Percent
1	China	255060	43.2%
2	UnitedStates	241080	40.9%
3	Oman	36390	6.2%
4	CzechRepublic	31653	5.4%
5	UnitedKingdom	8975	1.5%
6	Thailand	6359	1.1%
7	Sweden	3074	0.5%
8	RussianFederation	2601	0.4%
9	Germany	2439	0.4%

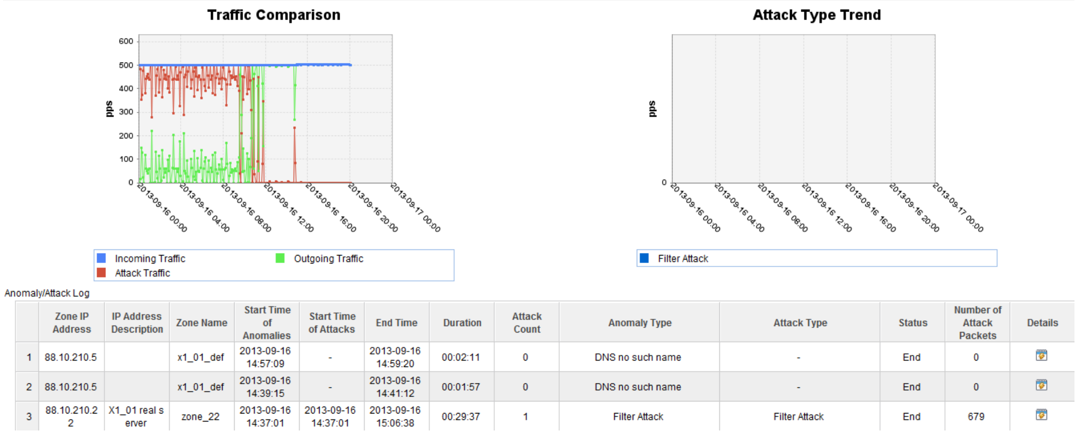
The IP Location Top N report provides visibility into the Top N IP locations that have the maximum volume of incoming or attack traffic.

- **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.

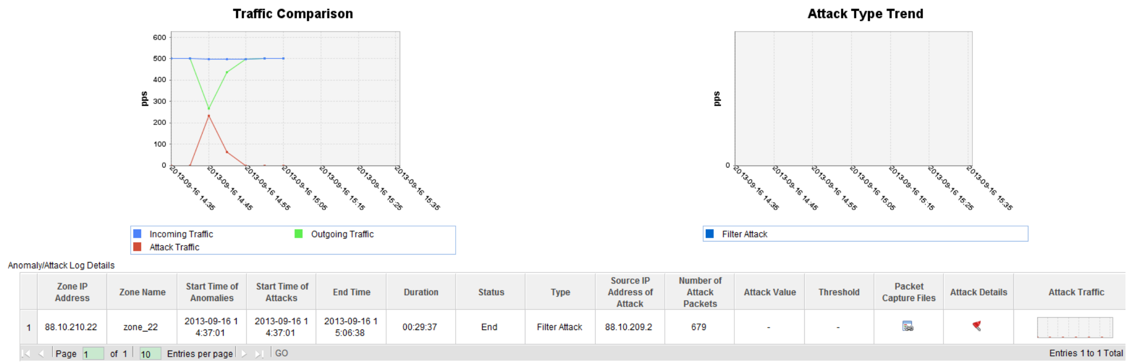
Anomaly/attack Details



Anomaly/Attack Log

	Zone IP Address	IP Address Description	Zone Name	Start Time of Anomalies	Start Time of Attacks	End Time	Duration	Attack Count	Anomaly Type	Attack Type	Status	Number of Attack Packets	Details
1	88.10.210.5		x1_01_def	2013-09-16 14:57:09	-	2013-09-16 14:59:20	00:02:11	0	DNS no such name	-	End	0	
2	88.10.210.5		x1_01_def	2013-09-16 14:39:15	-	2013-09-16 14:41:12	00:01:57	0	DNS no such name	-	End	0	
3	88.10.210.2 2	X1_01 real s erver	zone_22	2013-09-16 14:37:01	2013-09-16 14:37:01	2013-09-16 15:06:38	00:29:37	1	Filter Attack	Filter Attack	End	679	

Anomaly/attack Logs Details

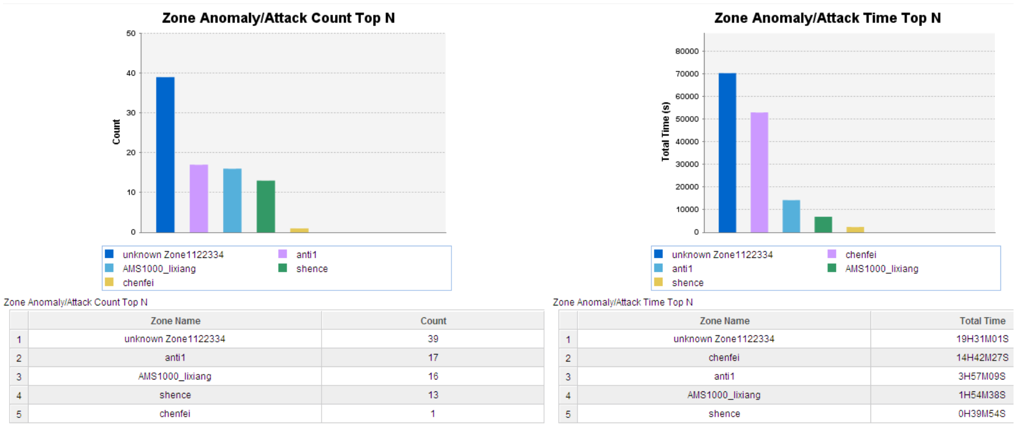


Anomaly/Attack Log Details

	Zone IP Address	Zone Name	Start Time of Anomalies	Start Time of Attacks	End Time	Duration	Status	Type	Source IP Address of Attack	Number of Attack Packets	Attack Value	Threshold	Packet Capture Files	Attack Details	Attack Traffic
1	88.10.210.22	zone_22	2013-09-16 14:37:01	2013-09-16 14:37:01	2013-09-16 15:06:38	00:29:37	End	Filter Attack	88.10.209.2	679	-	-			

2) Anomaly/Attack top N

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



Zone Anomaly/Attack Count Top N

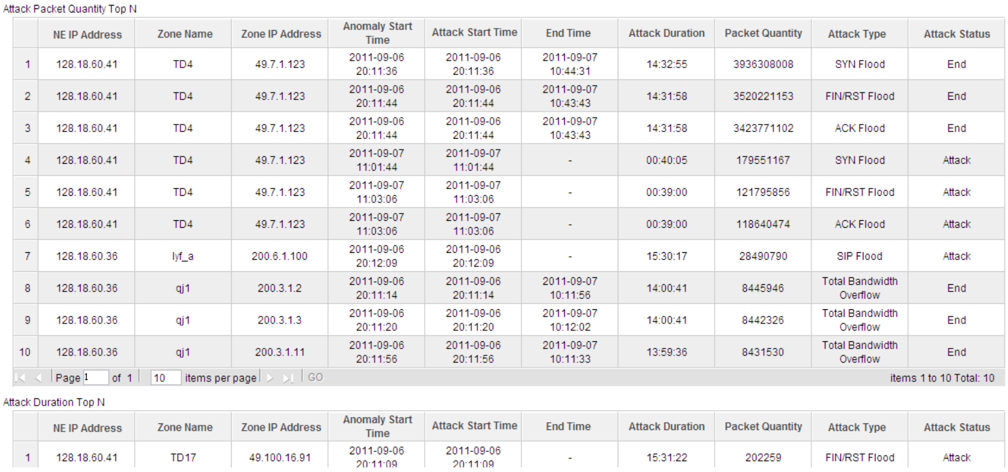
	Zone Name	Count
1	unknown Zone1122334	39
2	anti1	17
3	AMS1000_lixiang	16
4	shence	13
5	chenfei	1

Zone Anomaly/Attack Time Top N

	Zone Name	Total Time
1	unknown Zone1122334	19H31M01S
2	chenfei	14H42M27S
3	anti1	3H57M09S
4	AMS1000_lixiang	1H54M38S
5	shence	0H39M54S

3) Attacks Top N logs

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



Attack Packet Quantity Top N

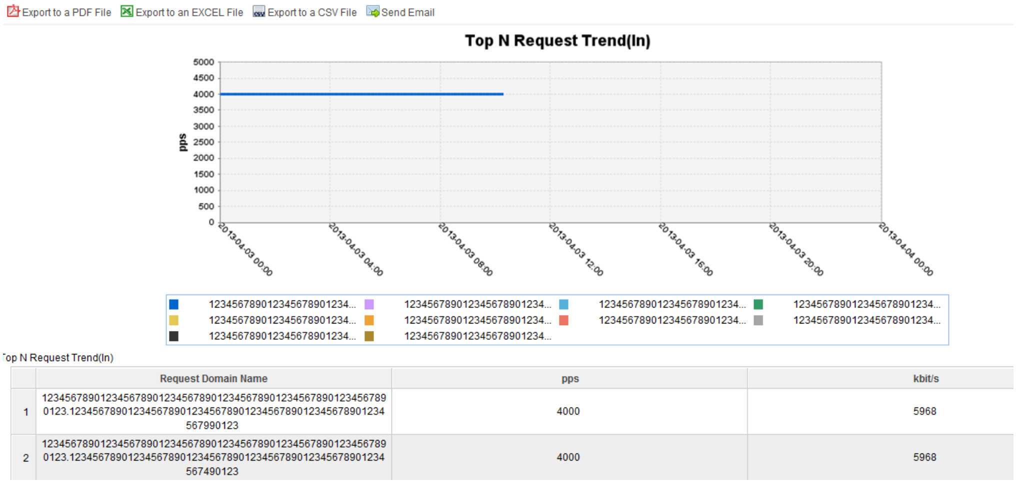
	NE IP Address	Zone Name	Zone IP Address	Anomaly Start Time	Attack Start Time	End Time	Attack Duration	Packet Quantity	Attack Type	Attack Status
1	128.18.60.41	TD4	49.7.1.123	2011-09-06 20:11:36	2011-09-06 20:11:36	2011-09-07 10:44:31	14:32:55	3936308008	SYN Flood	End
2	128.18.60.41	TD4	49.7.1.123	2011-09-06 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

Attack Duration 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

- **DNS Analysis**

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

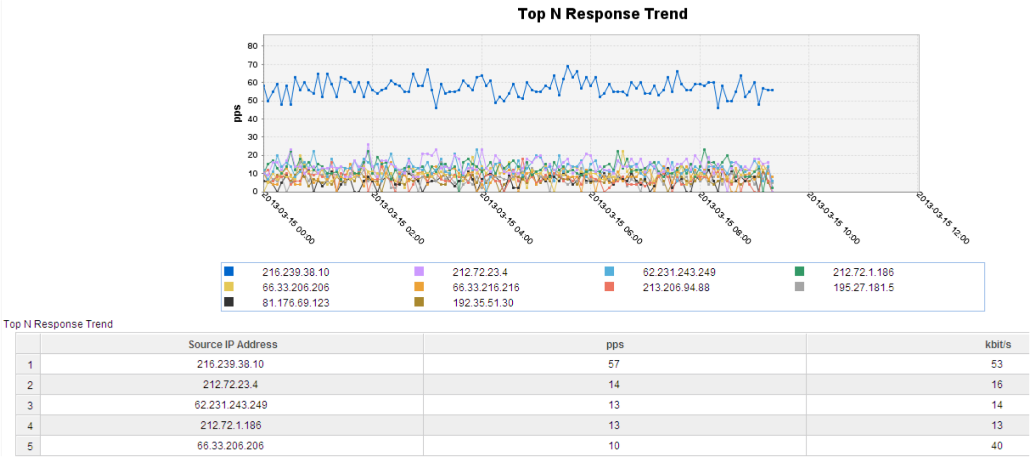


'op N Request Trend(In)

	Request Domain Name	pps	kbit/s
1	12345678901234567890123456789012345678901234567890123456789 0123.123456789012345678901234567890123456789012345678901234 567990123	4000	5968
2	12345678901234567890123456789012345678901234567890123456789 0123.123456789012345678901234567890123456789012345678901234 567490123	4000	5968

2) Top N Response Trend

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



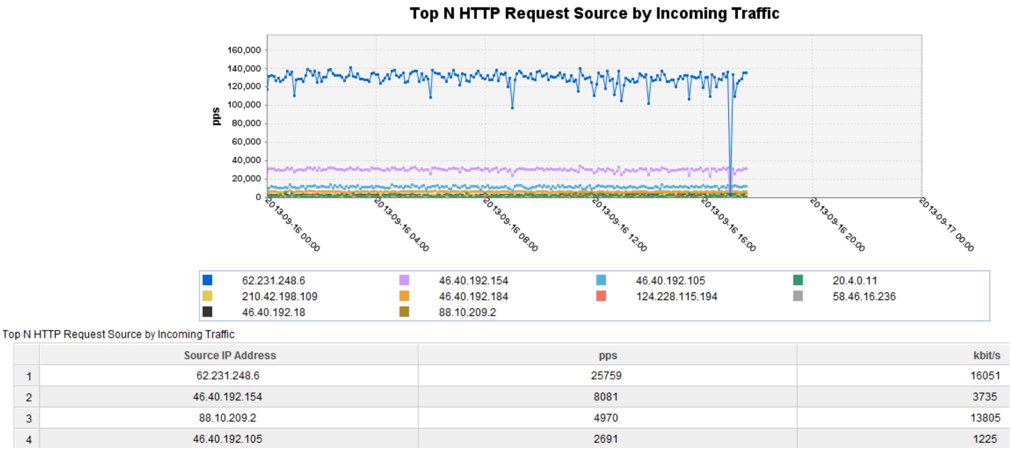
Top N Response Trend

	Source IP Address	pps	kbit/s
1	216.239.38.10	57	53
2	212.72.23.4	14	16
3	62.231.243.249	13	14
4	212.72.1.186	13	13
5	66.33.206.206	10	40

- **HTTP(S) Analysis**

1) Top N HTTP Request Sources by Traffic

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

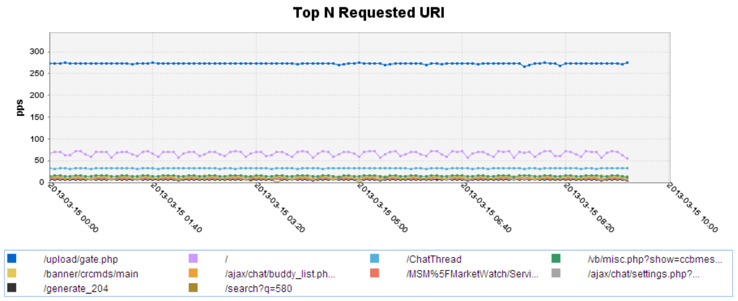


Top N HTTP Request Source by Incoming Traffic

	Source IP Address	pps	kbit/s
1	62.231.248.6	25759	16051
2	46.40.192.154	8081	3735
3	88.10.209.2	4970	13805
4	46.40.192.105	2691	1225

2) Top N Requested URI

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

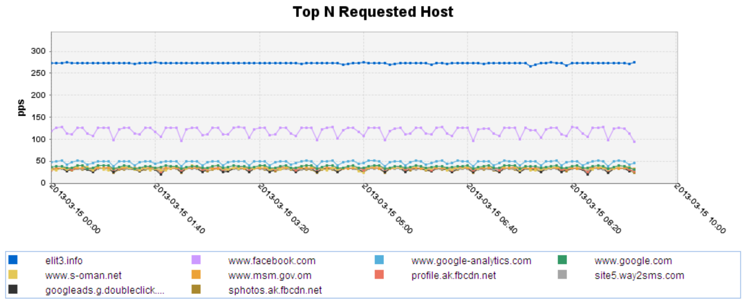


Top N Requested URI

	URI	pps	kbit/s
1	/upload/gate.php	273	2982
2	/	66	453
3	/ChatThread	32	289
4	/vb/misc.php?show=ccbmessages	14	127
5	/banner/crcmds/main	14	37
6	/ajax/chat/buddy_list.php?__a=1	11	143
7	/MSM%5FMarketWatch/Service/Process.aspx?Op=MD&MDC=	10	71

3) Top N Requested Host

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

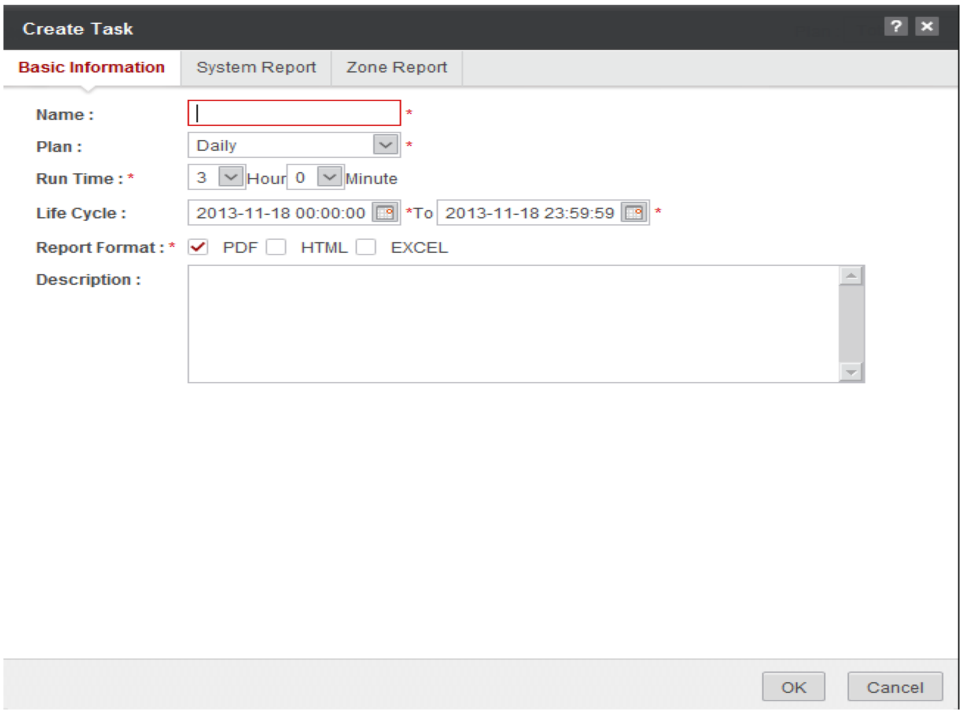


Top N Requested Host

	Host	pps	kbit/s
1	elit3.info	273	2982
2	www.facebook.com	118	1177
3	www.google-analytics.com	47	437
4	www.google.com	37	321
5	www.s-oman.net	34	284
6	www.msm.gov.om	33	204
7	profile.ak.fbcdn.net	33	145

- **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

Name : *

Plan : Daily *

Run Time : * 3 Hour 0 Minute

Life Cycle : 2013-11-18 00:00:00 *To 2013-11-18 23:59:59 *

Report Format : * ☑ PDF □ HTML □ EXCEL

Description :

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.

4 Anti-DDoS Products Introduction

4.1 Anti-DDoS8000 Series

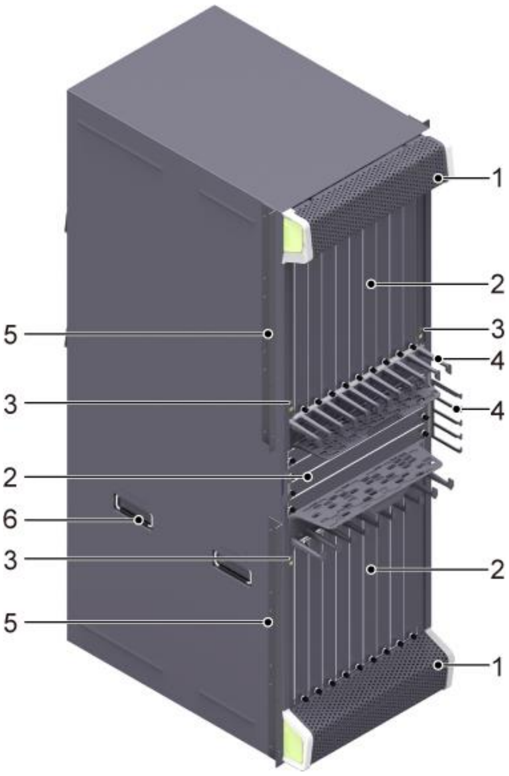
4.1.1 Anti-DDoS8000 Hardware

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

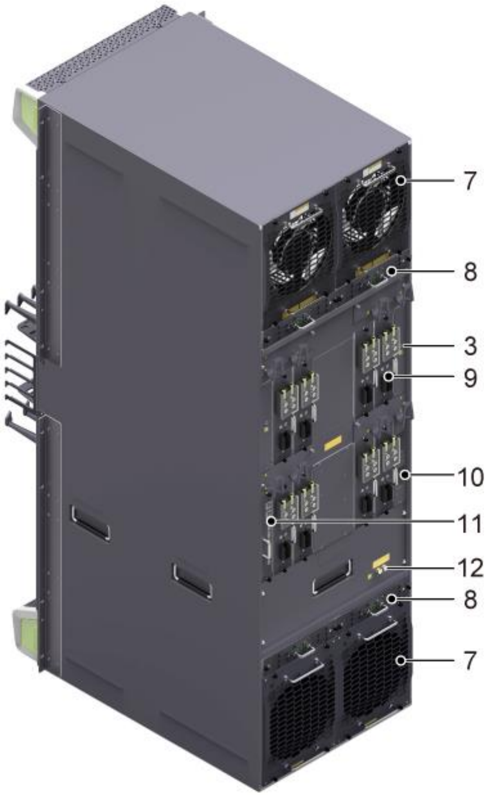
//Please choose Anti-DDoS8160/8080/8030 based on the project.

//Anti-DDoS8160

- **Front View**

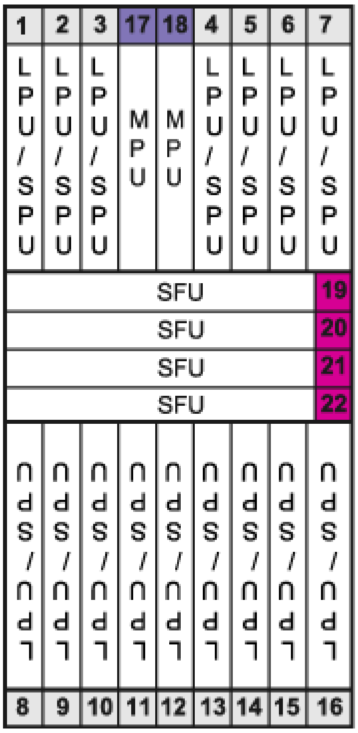


- **Rear View**



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**



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 chassises
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 ℃ to 45 ℃
	Short-term	-5 ℃ to 50 ℃
	Remarks	Limit of the temperature change rate: 30 ℃/hour
Storage temperature		-40 ℃ to 70 ℃
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.

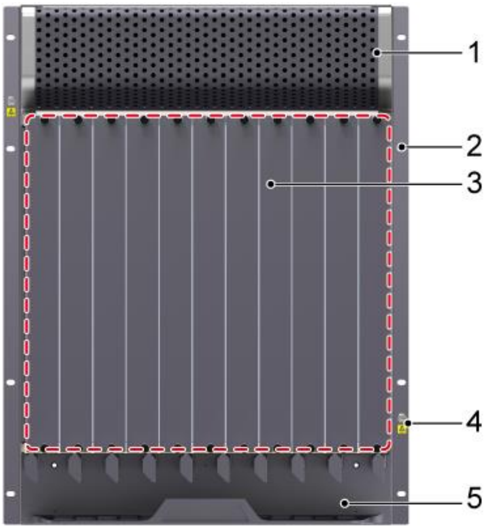
b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards.

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.

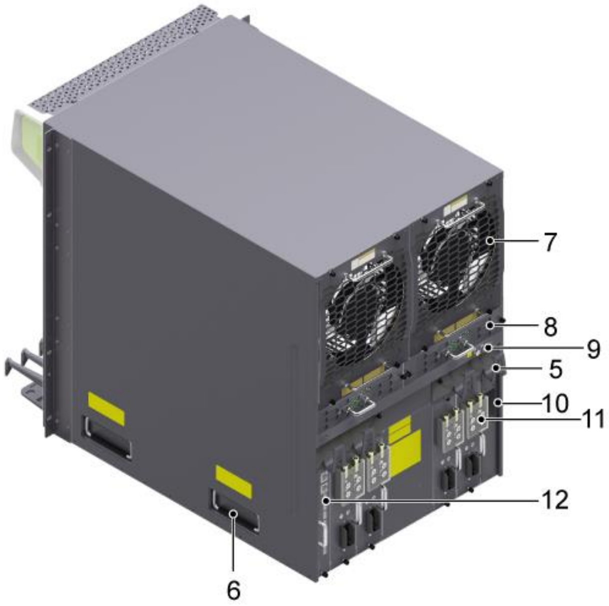
d . Short-term operation means that the continuous operation time does not exceed 96 hours and the accumulated operation time per year does not exceed 15 days. Otherwise, it is called long-term operation.

//Anti-DDoS8080

- **Front View**

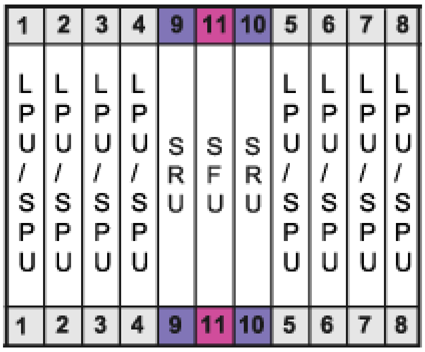


- **Rear View**



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
LPU/SPU	LPU/SPU	LPU/SPU	LPU/SPU	SRU	SFU	SRU	LPU/SPU	LPU/SPU	LPU/SPU	LPU/SPU
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 ℃ to 45 ℃
	Short-term	-5 ℃ to 50 ℃
	Remarks	Limit of the temperature change rate: 30 ℃/hour
Storage temperature		-40 ℃ to 70 ℃
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.

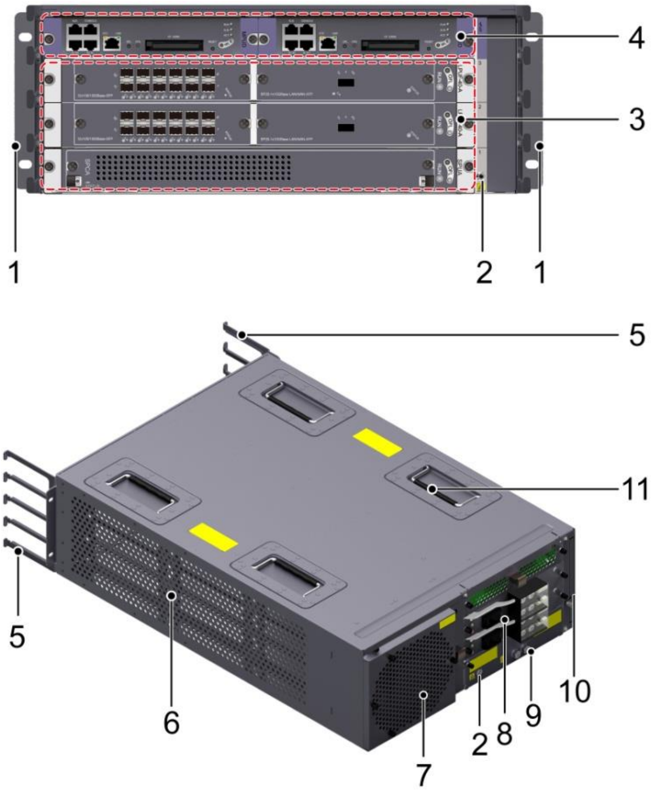
b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards.

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.

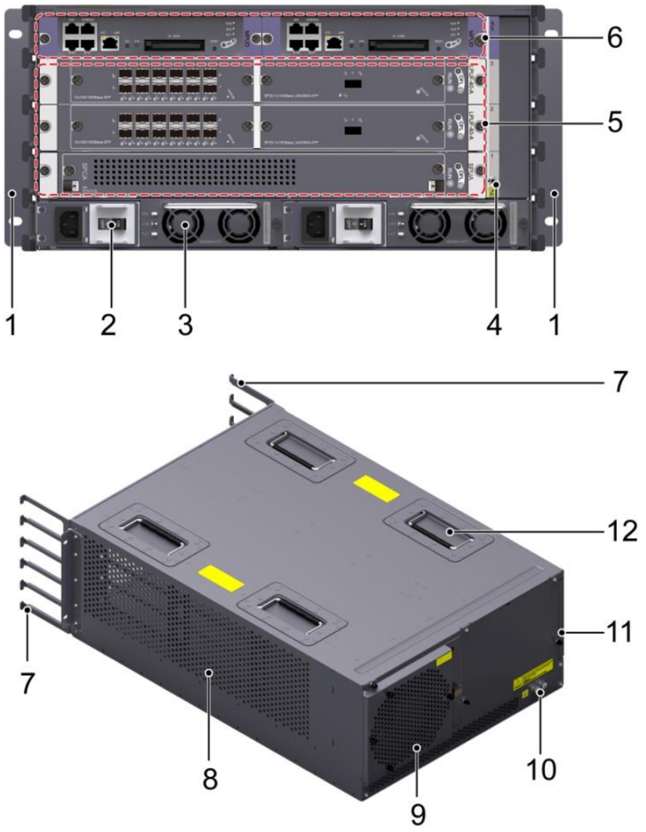
//Anti-DDoS8030

- **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 SPUs or

Slot Name	Slot Number	Quantity	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 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 ℃ to 45 ℃
	Short-term	-5 ℃ to 50 ℃
	Remarks	Limit of the temperature change rate: 30 ℃/hour
Storage temperature		-40 ℃ to 70 ℃
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.

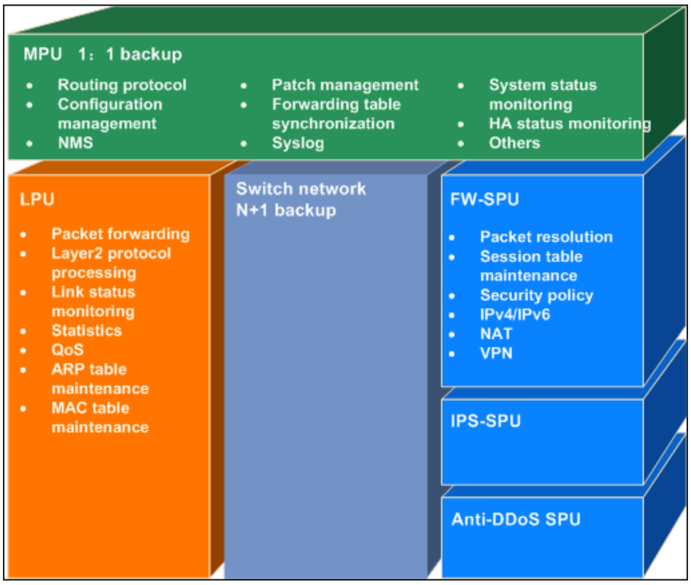
4.1.2 Anti-DDoS8000 Software

- **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.

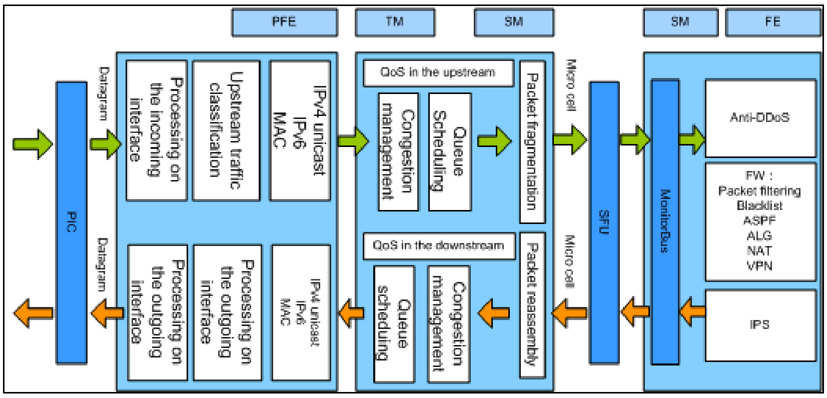
  Figure 1 Diagram of the logical software architecture



- **Data Forwarding Process**

  Following figure shows the flowchart of Anti-DDoS8000 forwarding data process:

  Figure 1 Flowchart of forwarding data



- **Anti-DDoS Detect and Clean Specification**

Category		**Query per second**		**Rate Statistics (pps)**		**Traffic Statistics (bit/s)**		**Session Statistics**	
		Destination IP	**Source IP**	**Destination IP**	**Source IP**	**Destination IP**	**Source IP**	**Destination IP**	**Source IP**
TCP	SYN			Yes					
	FIN/RST			√					
	TCP fragment			√		√			
	TCP			√		√			
UDP	UDP fragment					√			
	UDP			√		√			
HTTP	HTTP	√	√	√	√				
	Number of new HTTP connections							√	√
	Number of concurrent HTTP connections							√	√
	Access rate of the URLs in the URL list			√					√
	fingerprin			√	√				

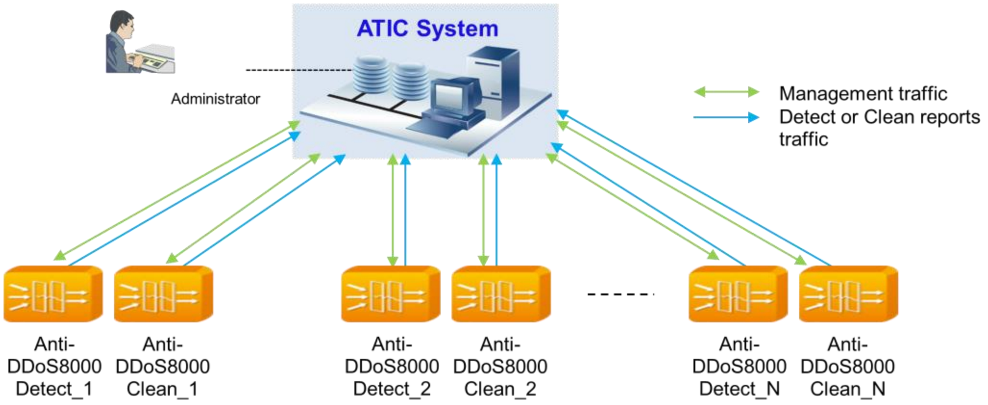
	t of URL								
	TOPN URI	√							
	TOPN HOST	√							
HTTPS	HTTPS			√	√				
	SSL Renegotiating rate							√	√
DNS	UDP DNS query			√	√				
	DNS Nxdomain			√					
	DNS domain attacked	√							
	UDP DNS reply			√	√				
	TOPN domain	√							
	TOPN Source IP			√	√				
SIP	SIP			√					
	TOPN Source IP				√				
	TOPN Caller			√					
	TOPN Callee			√					

4.2 ATIC System

4.2.1 ATIC System Architecture

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

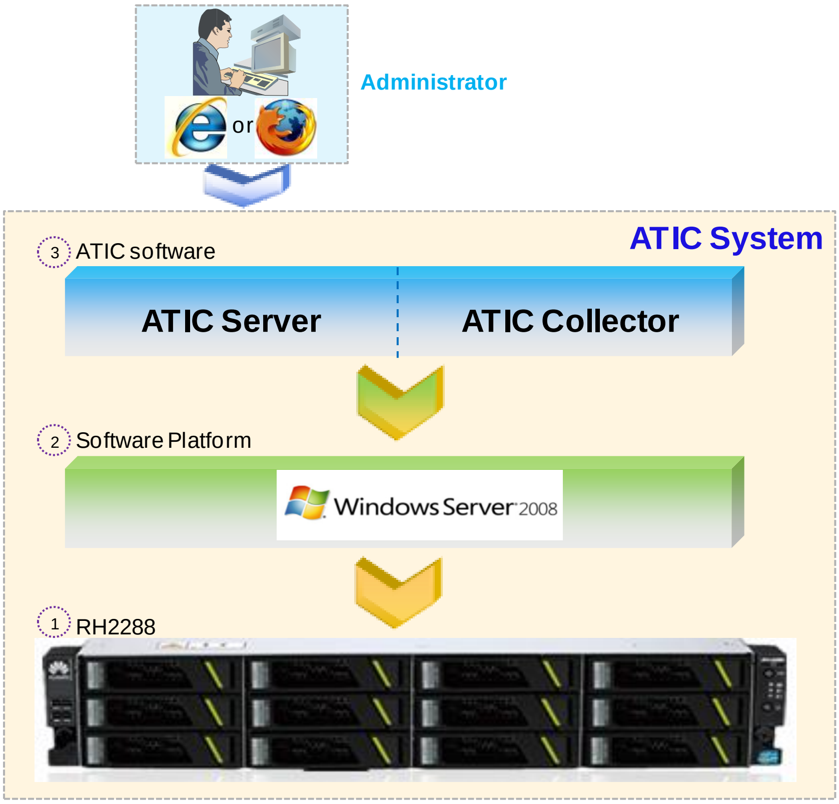
- **ATIC System Network Architecture**



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

4.2.2 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

4.2.3 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