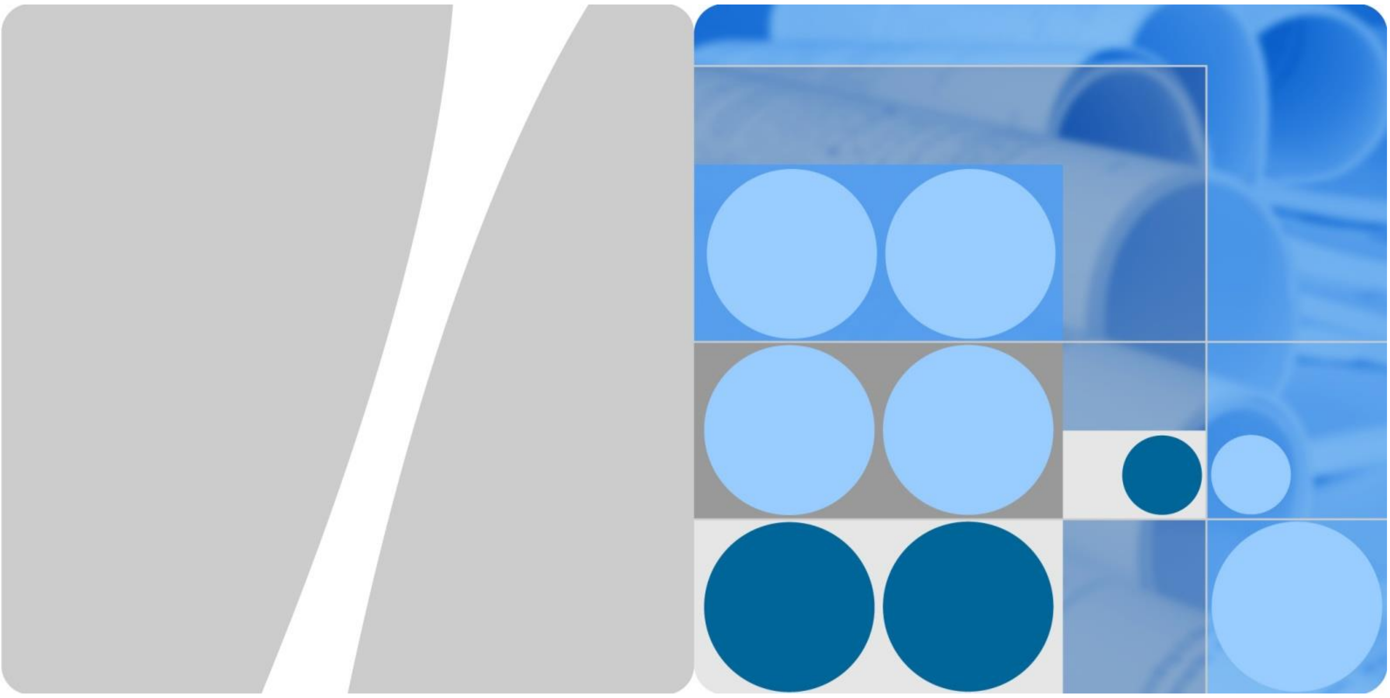


Huawei Anti-DDoS Solution

Technical White Paper

Issue	**5.5**
Date	**2017-01-10**

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

Contents

1 DDoS Attack Trend

1.1 Today's DDoS Attack

DDoS attacks are generally motivated by political ideology, malicious competition, extortion, and economic crimes. Politically motivated attacks are usually massive cyber attacks that target banks, government websites, or DNS servers. These attacks can easily lead to large-scale mass panic and are like "nuclear weapons" in cyber attacks. For example, in Dec. 2015, the hacker organization Anonymous declared cyber war on Turkey, accusing the country of supporting extremist organizations.

DNS servers in Turkey experienced massive cyber attacks, with 400,000 websites being forced offline. Attacks motivated by malicious competition and extortion target specific business systems, and are like "special forces" for the following reasons:(1) they directly attack real IP of websites that have purchased DNS traffic diversion-based mitigation services; (2) they launch continued slow attacks on game authentication servers; and (3) if such attacks do not work within 30 minutes, the attack methods will immediately be changed until the targets become inaccessible. Served as the "smokescreen", most attacks driven by economic crimes attract the attention of security personnel in order to mask the real intention of data theft.

DDoS attacks loosely fall into two categories: one uses reflection attacks or large packets flood to exhaust bandwidth, and the other contains slow attacks precisely target business systems such as e-finance or gaming.

In March 2013, The Spamhaus Project was hit by heavy DDoS attack traffic, peaking at up to 300 Gbit/s, launched using DNS amplification. In December 2013, the hacker organization DERP launched the first NTP amplification attack. Then in February 2014, the peak bandwidth of NTP amplification attack traffic was refreshed to 400 Gbit/s. Shortly thereafter, UDP amplification attacks were unleashed the world over. 2014 was marked by rampant UDP-based amplification attacks and large packet SYN flooding. With over 100Gbit/s DDoS attacks on nearly a monthly basis, attack traffic peak bandwidths were again refreshed.

Bandwidths in early 2014 were up to 400 Gbit/s, which rose to 500 Gbit/s by the end of the year (a DDoS attack was launched in December 20, 2014, targeted at specific Chinese cloud-based DCs hosting game servers; the attack which lasted 14 hours mainly consisted of ultra large packet SYN and UDP flooding from outside of China and some large DCs in China). Ultra-heavy traffic DDoS attacks already threaten operator gateways, and global Tier-1 operators have begun to seek the source of the attack to quickly filter out attack traffic through cloud mitigation solutions.

Due to the real-time online nature of routers, they have become a popular source of DDoS attacks. The hacker organization Lizard Squad, which is known worldwide for taking down multiple large game services, exploits botnets consisting of home routers to launch attacks.

IoT devices and router become new favorites of DDoS attack source.

With the rapid development of cloud computing, Internet services are becoming more centralized, exposing cloud-based DCs to severer DDoS attacks: (1) Cheap VMs and online tenant registration and payment make it hard to authenticate and manage real user identity. Attacks from rented VMs occur from time to time. (2) Tenants have little security awareness.

Accounts with weak passwords are easy to be brute-force cracked, and Trojan horses may be planted. Tenants may enable unnecessary services, which will threaten security of their own data and can be used to launch outbound attacks. (3) Even though cloud service providers can provide security services, targeted defense is difficult to implement due to the large number of cloud-based hosts, the wide variety of services, and vast differences among traffic patterns. (4) Attackers often launch various type and incremental size DDoS attacks to test the performance limit and robustness of cloud architecture.

Facing increasing new defense techniques, advanced botnets usually have a superior disguise capability. They can respond to challenge authentications of defense equipments, demonstrating a high evasion capability.

1.2 Development Trends

As CT shifts to IT-oriented developments, and enterprise IT becomes more cloud-based and centralized, DDoS attacks and defense will become much more complicated.

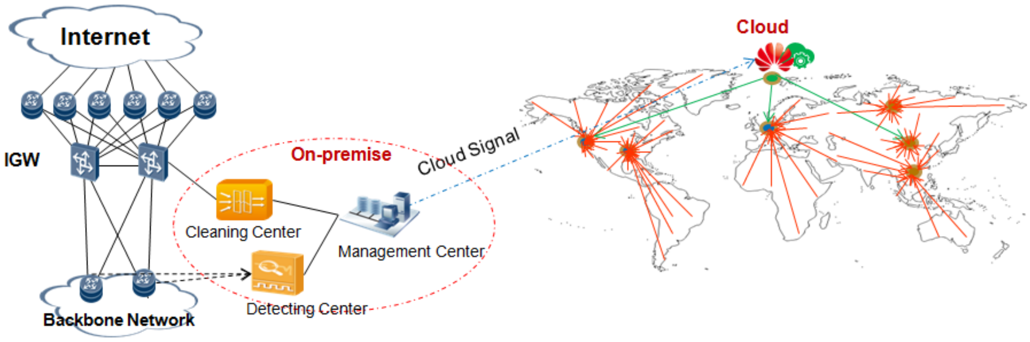
Hybrid reflection amplification attacks will become popular in the next few years and further boost the peak bandwidths of attack traffic. Major sources of attacks will still be a large number of poorly-managed UDP services and web servers, and rapidly-developed smart IoT devices without security mechanisms. As time goes by, more sources of reflection attacks will be discovered.

As ultra-heavy traffic DDoS attack frequency is increasing globally, carrier networks face direct threats. It is inevitable that Tier-2/3 carriers will seek for near-source cloud mitigation solutions that can filter ultra-heavy attack traffic from the attack source. As for enterprise network defense, single-point defense on enterprise network borders provides limited protection. Therefore, enterprises are in increasing need of layered defense solutions that combine cloud mitigation services (provided by upstream network providers) and on-premise defense (deployed on enterprise network borders). On-premise defense provides refined protection for each service, and cloud mitigation services protect enterprise network bandwidths by filtering heavy-traffic attacks. This rigid requirement, in turn, drives carriers to accelerate the deployment of on-premise defense systems on the IGW or Backbone to provide anti-DDoS services for enterprises.

2 Huawei multi-layer DDoS Defense Solution

2.1 Huawei multi-layer DDoS Defense Solution

Huawei delivers multi-layer protection against DDoS attacks by integrating on-premise defense with powerful cloud-based DDoS mitigation service. On-premise system defends against attacks in the bandwidth range of the customer’s network, and Huawei global near-source cloud mitigation service handles large DDoS attacks to protect the availability of customer’s network bandwidth. Huawei delivers automatic defense by integrating on-premise defense solution and global near-source cloud mitigation solution through the cloud signal.



2.1.1 On-Premise DDoS Defense

On-premise DDoS defense system deployed at the customer’s network edge serves as a first line of defense against attacks to the customer’s network. Huawei on-premise DDoS defense solution is designed to automatically detect and mitigate attacks for protecting application availability. On-premise DDoS defense system is purpose-built to filter multi-layered DDoS attacks, including:

- Volumetric attacks, such as SYN flood, UDP flood, UDP-based amplification attacks (DNS ,NTP, Chargen, SNMP, TFTP, NetBIOS, SSDP, QOTD, Quake, Steam, Portmapper), ACK flood, FIN/RST flood, ICMP flood, IP fragment flood, etc.
- Application-layer attacks, such as HTTP get/post flood, HTTP slow header attack, HTTP slow post attack, HTTPs flood, SSL-DoS/DDoS, DNS request flood, DNS reply flood, DNS cache poisoning attack, SIP Methods flood, etc.

- State exhausting attacks, such as TCP connection exhausting attack, TCP retransmission attack, Sockstress, etc.

In addition to the professional DDoS defense capabilities, Huawei on-premise defense solution supports comprehensive operation oriented functions that help carriers provide DDoS defense service to their enterprise customers.

2.1.2 On-demand, global near-source cloud Mitigation

Huawei global near-source cloud mitigation service provides global scrubbing capacity and can handle today’s largest and most complex attacks that threaten the availability of network bandwidth. Customer’s on-premise solution serves as a first line of defense. When the on-premise solution detects an attack which has risk of exceeding link bandwidth, it triggers an alert to the CCC using Huawei proprietary cloud signal. The CCC will dispatch cloud scheduling signal to CMA partners’ SOC to trigger scrubbing centers to divert traffic and filter attack traffic. After filtering attack traffic, scrubbing centers will re-inject normal traffic to customer’s network via GRE tunnels. Global near-source cloud mitigation service is purpose-built to filter large volumetric attacks, including: SYN flood, UDP flood, UDP-based amplification attacks (DNS ,NTP, Chargen, SNMP, TFTP, NetBIOS, SSDP, QOTD, Quake, Steam, Portmapper), ACK flood, FIN/RST flood, ICMP flood, IP fragment flood, etc.

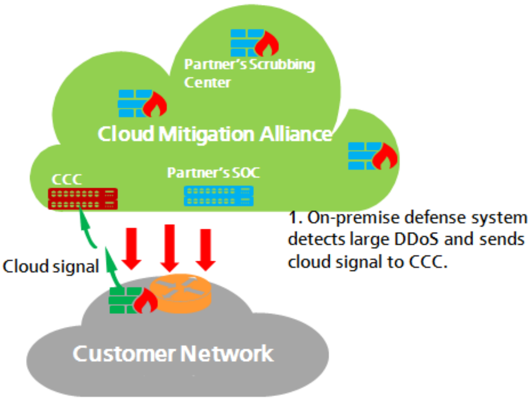
2.1.3 How Multi-Layered Protection Solution Works

Customer can preset the on-premise solution to automatically send cloud signal to Huawei’s CCC when a certain threshold is reached or customer can manually alert the CCC about the attack.

An automatic mitigation will work following below steps:

Step 1 On-premise solution detecting a large attack and triggering CCC

Customer’s on-premise defense solution serves as a first line of defense, when it detects an attack which has risk of exceeding link bandwidth; it triggers an alert to the Huawei’s CCC using Huawei unique Cloud Signal through Restful API.

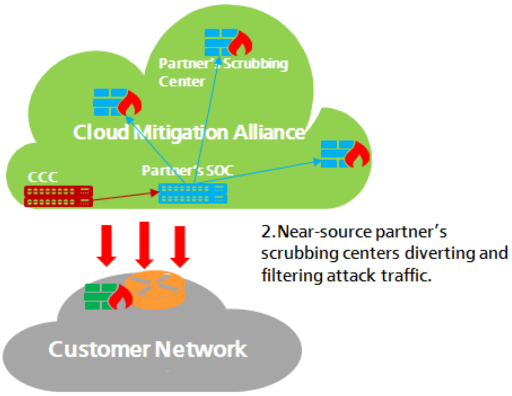


1. On-premise defense system detects large DDoS and sends cloud signal to CCC.

Step 2 CCC scheduling global scrubbing centers to mitigate

CCC sends an alert to CMA(Cloud Mitigation Alliance) partner’s SOC when CCC receiving cloud signal. And then customer’s inbound traffic will be rerouted to CMA’s global scrubbing centers to mitigate via BGP anycast after CMA partner’s SOC scheduling global cloud scrubbing centers. Huawei CMA’s global scrubbing centers with 2T+ defense capability located in:

- USA: San Jose, Miami, Los Angeles, Ashburn
- Europe: London, Amsterdam
- Asia: Singapore, Hong Kong
- China: Beijing, Shanghai, Guangzhou



2.Near-source partner's scrubbing centers diverting and filtering attack traffic.

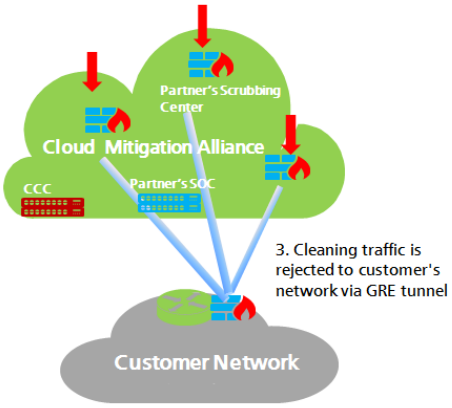
To use BGP anycast redirecting customer's inbound traffic to Huawei CMA scrubbing centers, customer must have a /24 prefix (Class C subnet) at a minimum.

Once a cloud signal is delivered to Huawei CCC:

- CMA partner's cloud SOC team initiates BGP announcements for the affected prefixes.
- Within minutes, customers inbound traffic of affected /24 prefixes network could be redirected to CMA global cloud scrubbing centers.
- Huawei CMA security experts work closely with customer to ensure that attack traffic against customer network would be filtered and customer's application availability.

Step 3 "clean" traffic forwarded via GRE tunnels

"Clean" traffic is forwarded to customer network via GRE tunnels after attack traffic is filtered in global scrubbing centers.



3. Cleaning traffic is rejected to customer's network via GRE tunnel

Step 4 Customized report and portal

CCC generates a customized report showing attack details. Customer can self-service reports via portal.

----End

3 Huawei On-premise Anti-DDoS Solution

3.1 Solution Architecture

Huawei on-premise Anti-DDoS solution includes management center, detecting center and cleaning center.

- Management center

  Management center mainly provides the following functions: the centralized management of the cleaning equipment, defense policies configuration and report display. Management also provides API for interconnection with the third-party Network Management System (NMS). The system, of which the management is based on zones, can be applied as the operational management platform for value-add DDoS defense service of ISP. Management center includes the management server and data collectors. Both the management server and data collectors run on the X86 platform. The adopted operating system is Windows 2008/2012, and the database is MySQL.

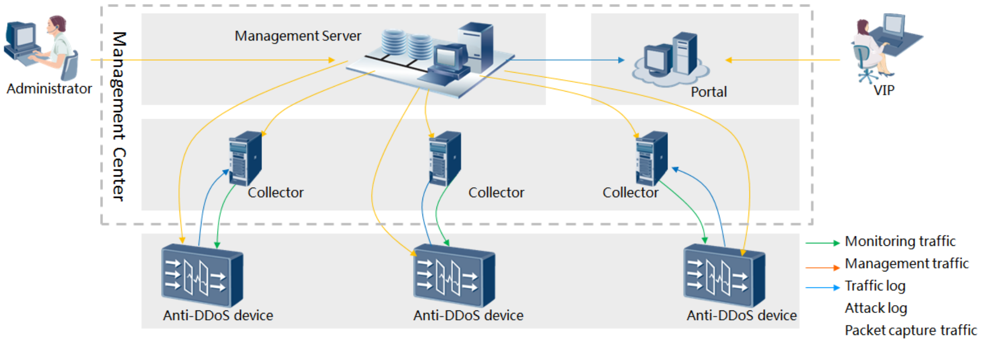
  B/S architecture: The management server provides the Web-based configuration, management and reports. Data collectors do not provide the interface.

  Data collector: One detecting or cleaning equipment corresponds to one data collector. The data collector is in charge of the collection, resolution, summarization, and warehousing of traffic logs and attack logs for data query and reports of the management server.

  Management server: The management server is in charge of the centralized management and defense policies of detecting and cleaning equipments and reports.

  Distributed deployment and centralized management: The management server and data collectors support both distributed deployment and centralized deployment. When deployed in distributed mode, the equipments have excellent scalability. The management server can manage 50 detecting and cleaning equipments and 50 data collectors at the same time.

  Based on SNMP, data collectors monitor the performance of and collector the logs from detecting and cleaning equipments. The management server delivers policies to detecting and cleaning equipments through SSH/Telnet, and sends traffic logs, exception logs, attack logs, or captured packets to data collectors through UDP.



- Detecting center

  According to detecting technology, detecting center has two kinds of equipments: flow-based detecting equipment and per-packet-based detecting equipment. Detecting center detects traffic, and notifies management center once identifying attacks. Then management center triggers cleaning center to divert the traffic to protected network for cleaning.

  Flow-based detecting technology fits large volume traffic analysis. However, it cannot detect small traffic attacks and application attacks because netflow logs are traffic sample and have no payload. It is always deployed on backbone network for clean-pipe solution.

  On the other hand, per-packet-based detecting technology fits refined detection for application layer attack. It is always deployed on the boundary of data center for service protection.

- Cleaning center

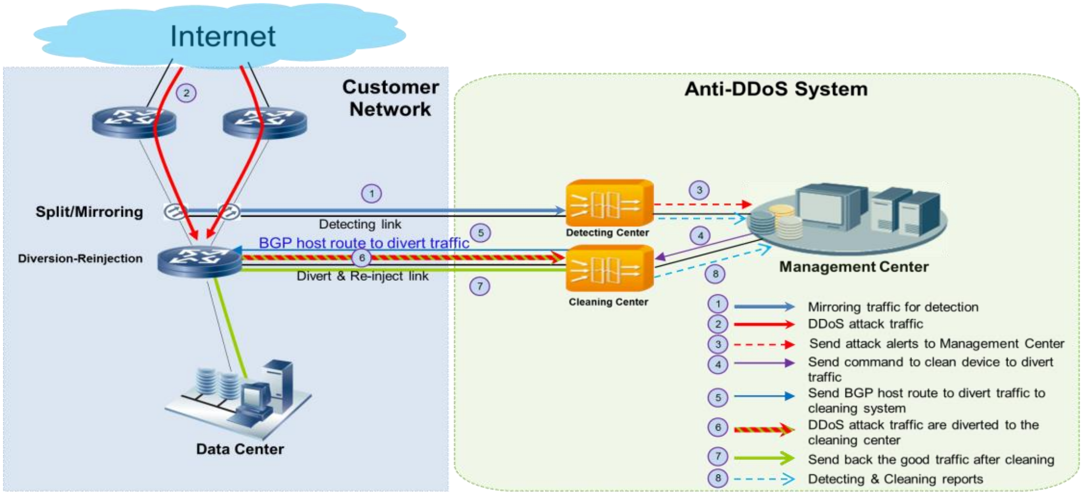
  Cleaning center diverts traffic, filters abnormal traffic, and injects normal traffic. Huawei cleaning center distinguishes between abnormal traffic and normal traffic based on the multi-layer filtering.

NOTE

Per-packet-based detecting equipment or cleaning equipment is AntiDDoS1000 series or AntiDDoS8000 series in Huawei Anti-DDoS solution. AntiDDoS1000 series is centralized equipment and AntiDDoS8000 is framed equipment. AntiDDoS8000 consist of cleaning card and detecting card. We can provide detecting device and cleaning device and hybrid device based on detecting card and cleaning card inserted in the same device. For hybrid device, you can assume it as independent cleaning equipment and detecting equipment.

3.2 Solution Working Principle

3.2.1 Per-packet based detect and dynamic diversion


Internet
Customer Network
Anti-DDoS System
Split/Mirroring
Diversion-Reinjection
Detecting link
BGP host route to divert traffic
Divert & Re-inject link
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

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

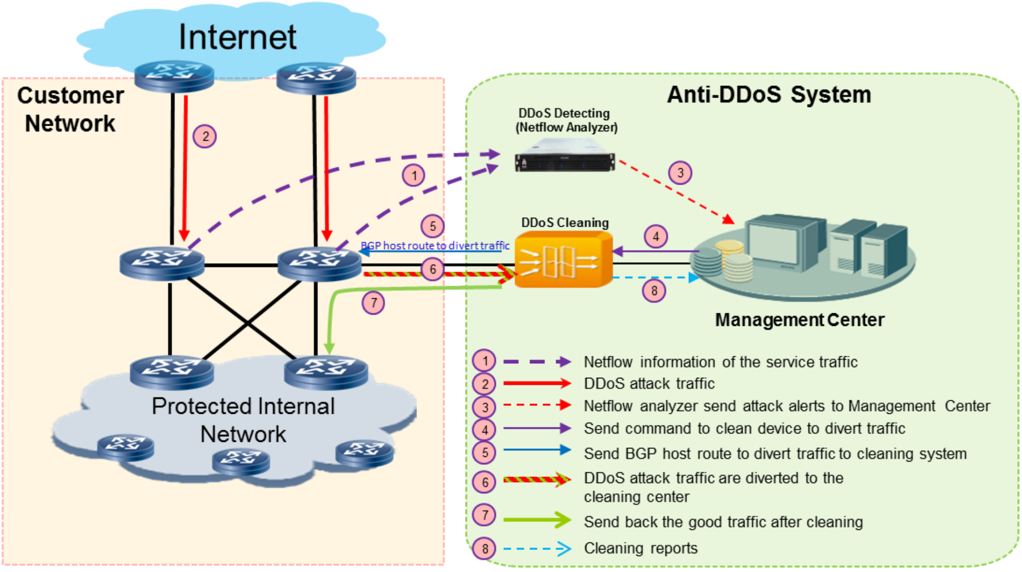
5) Cleaning center sends BGP divert route to the adjacent router, this route will divert all traffic that are going to the victim destination (including DDoS attack traffic and normal good traffic) to the cleaning center

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.

3.2.2 Netflow based detect and dynamic diversion


Internet
Customer Network
Anti-DDoS System
DDoS Detecting (Netflow Analyzer)
DDoS Cleaning
BGP host route to divert traffic
Management Center
Protected Internal Network
1 2 3 4 5 6 7 8
1 Netflow information of the service traffic
2 DDoS attack traffic
3 Netflow analyzer 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 Cleaning reports

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

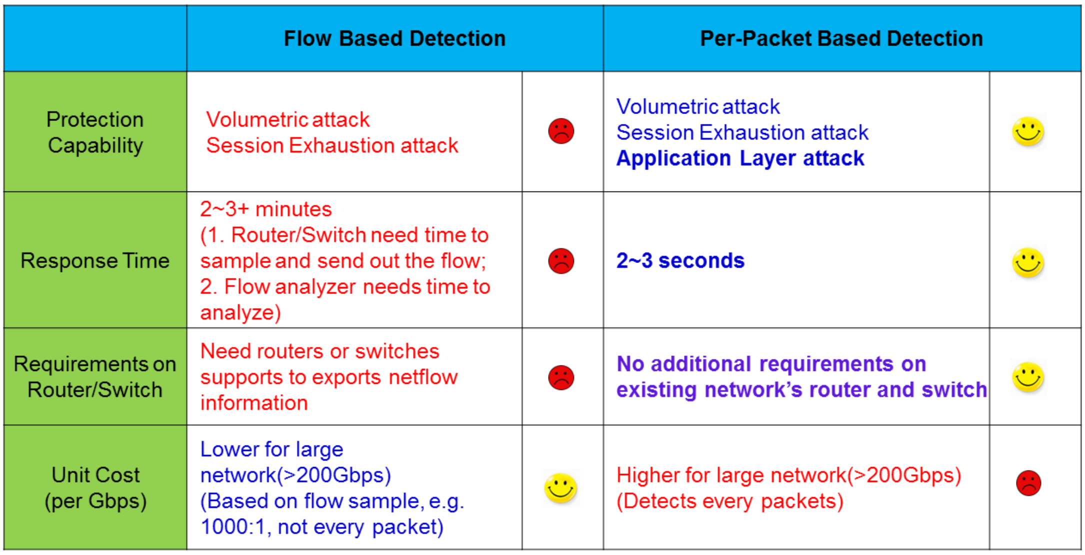
5) Cleaning center sends BGP divert route to the adjacent router, this route will divert all traffic that are going to the victim destination (including DDoS attack traffic and normal good traffic) to the cleaning center

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.

- Comparison between Per-packet based and flow based method

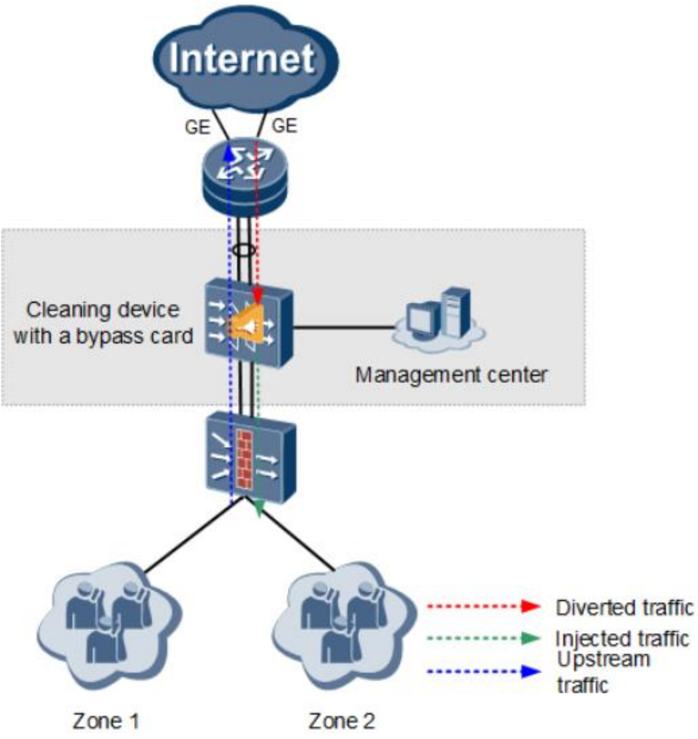


	Flow Based Detection		Per-Packet Based Detection	
Protection Capability	Volumetric attack Session Exhaustion attack	☹	Volumetric attack Session Exhaustion attack **Application Layer attack**	☺
Response Time	2~3+ minutes (1. Router/Switch need time to sample and send out the flow; 2. Flow analyzer needs time to analyze)	☹	**2~3 seconds**	☺
Requirements on Router/Switch	Need routers or switches supports to exports netflow information	☹	**No additional requirements on existing network's router and switch**	☺
Unit Cost (per Gbps)	Lower for large network(>200Gbps) (Based on flow sample, e.g. 1000:1, not every packet)	☺	Higher for large network(>200Gbps) (Detects every packets)	☹

For enterprise customers, the traffic bandwidth is generally not large, require application layer DDoS protection and quick response capability, per-packet detect solution is more suitable for enterprise scenario.

For carriers/ISPs, the bandwidth is generally large, the cost of per-packet will be high, carriers/ISPs are not sensitive to application layer attacks, also can endure minutes DDoS attacks, so flow based detect solution is more attractive for carriers/ISPs.

3.2.3 Inline deployment real-time protecting



For small bandwidth scenario (for example small or middle enterprise network edge, DNS server/Web server/other online service servers）, to simplify the network design, reduce cost for product and maintenance, inline deployment mode is a good choice.

Inline deployment mode only deploy cleaning device (also supports DDoS detecting), when traffic go through Anti-DDoS cleaning device, it will detect DDoS in real-time, if there is no DDoS attack, the traffic will be forwarded directly; if there is DDoS attack, will start cleaning.

Inline deployment mode includes physical inline deployment and logical inline deployment, the logical inline deployment means the physical deploy is still offline mode, but configure static route/policy route on Anti-DDoS cleaning device’s adjacent routers, redirect the protected zone's traffic to the Anti-DDoS cleaning system.

Inline deployment mode can detect traffic in real-time, fast response to DDoS attack.

In order to prevent single point of failure, can deploy internal bypass card for AntiDDoS1600 series or external bypass for AntiDDoS8000 series.

3.3 Managed DDoS Protection Service

The system supports zone-based defense policies and reports and customized portal for self-service reports. Zone is a group of protected IP addresses that can be multiple IP addresses or the IP address segments defined by the mask. To realize the refined defense for the services externally, you can customize defense policies for each zone.

3.4 Flexible Traffic Diversion Modes

Management center provides three traffic diversion modes including static traffic diversion, dynamic traffic diversion, and interactive traffic diversion.

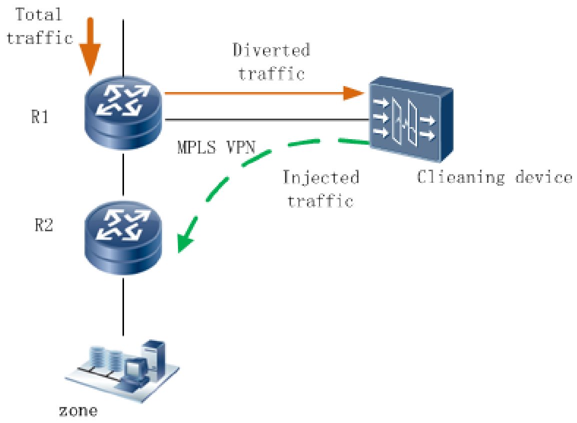
- Static Traffic Diversion: You need to manually create and deliver traffic diversion policies to the detecting equipment to trigger the traffic diversion. The system does not cancel the traffic diversion automatically. When the protectd network traffic passes through the cleaning equipment in real time, the static defense is performed.
- Dynamic Traffic Diversion: The detecting equipment reports the anomalies to management center. Management center generates traffic diversion policies automatically and delivers the policies to the cleaning equipment. When attacks end, management center cancels the delivery of traffic diversion policies to the cleaning equipment.
- Interactive Traffic Diversion: The detecting equipment reports the anomalies to management center. Management center generates the traffic diversion policies automatically and delivers the policies to the cleaning equipment after the administrator confirms the policies manually. When attacks end, the administrator needs to determine whether to delete the traffic diversion policies or not.

3.5 Flexible Traffic Injection

In off-line mode, the cleaning equipment adopts multiple modes to inject cleaned traffic.

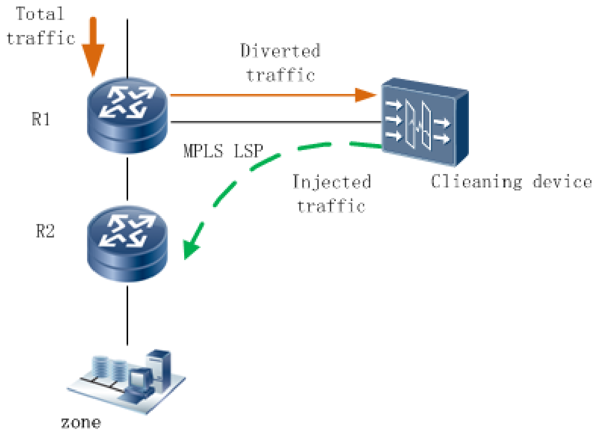
3.5.1 MPLS VPN injection

As shown in the following figure, the VPN is configured on both the DDoS cleaning equipment and R2. On the traffic-injection link, both the DDoS cleaning equipment and R2 serve as Provider Edge (PE) equipments, and R1 serves as the core router. Cleaned traffic is tagged with two layers of labels and outer labels are stripped after the traffic passes through R1. Then R2 searches the corresponding private routing table based on inner private labels and forwards the traffic.



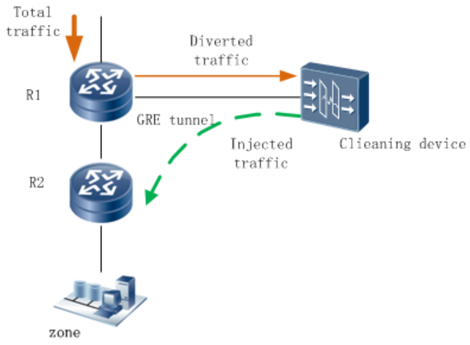
3.5.2 MPLS LSP injection

As shown in the following figure, MPLS and LDP are configured on the DDoS cleaning equipment, R1, and R2 respectively. MPLS labels are delivered to and MPLS LSP is established on these equipments. After tagged with single layer labels on the DDoS cleaning equipment, cleaned traffic is sent to the zone based on the pre-established LSP.



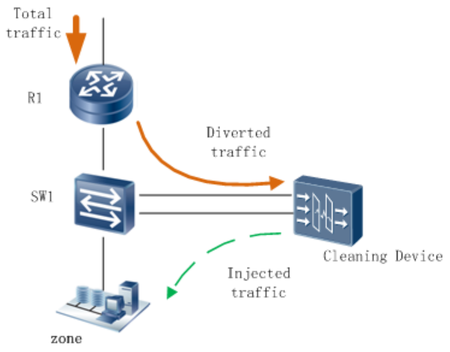
3.5.3 GRE tunnel injection

As shown in the following figure, a GRE tunnel is established between the DDoS cleaning equipment and R2. Cleaned traffic travels through the GRE tunnel from the DDoS cleaning equipment to R2.



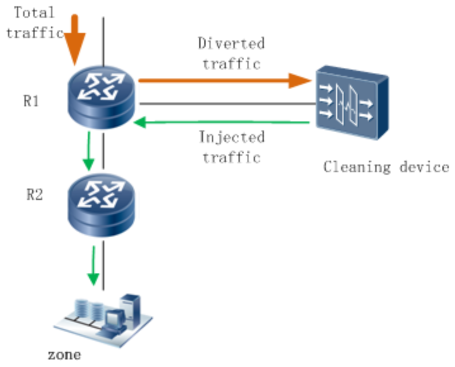
3.5.4 Layer 2 injection

As shown in the following figure, the IP address of the egress on the DDoS cleaning equipment and the zone are on the same network segment. After cleaning the diverted traffic, the cleaning equipment sends ARP packets to request MAC addresses from IP addresses in the zone. Then the cleaning equipment receives ARP reply packets and sends cleaned normal traffic to the zone through switch1.



3.5.5 PBR injection

The cleaning equipment sends cleaned traffic to R1, and then R1 (PBR is enabled on the interface receiving injected traffic) injects the traffic to R2.



3.6 Attack Traffic Analysis

The system supports packet capture based on abnormal or attack events. That is, when an abnormal or attack event occurs, packets are captured automatically (the number of captured packets can be specified). Additionally, the system supports the sampling and unattended packet capture. Moreover, the equipment supports the packet capture based on ACLs and the discarding of packet capture.

Packets captured by the equipment are sent as UDP packets to data collectors. Then the packets are saved on data collectors as the .pacp file. The system supports managing the captured packets, downloading captured files, and analyzing the defense details via ATIC.

Management center extracts attack features from the captured packet file, and delivers these features to the cleaning equipment for filtering attack traffic.

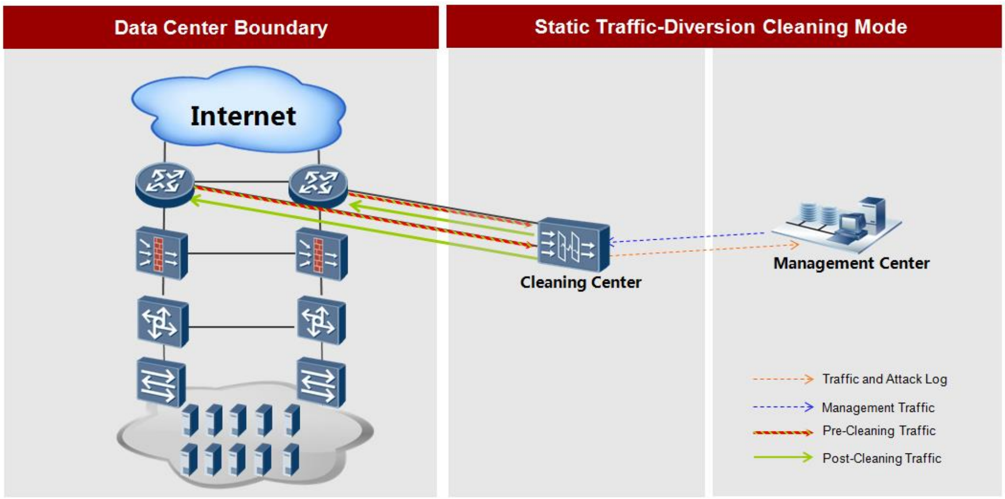
The system supports extracting attack sources from attack events. Meanwhile, dynamic blacklist can be sent to management center as an importance data source for attack tracing.

3.7 Comprehensive Reports

The system supports zone-based traffic statistic, attack analysis and application layer report via ATIC. ATIC supports daily, weekly, monthly and yearly reports and can be exported as .xls and .pdf.

3.8 Deployment Scenarios

3.8.1 Static Traffic-Diversion Defense (In-line)



- Deployment Description

  The off-line mode statically defends the specified traffic. The cleaning equipment can dynamically learn the network traffic baseline and detect DDoS attacks. Meanwhile, the cleaning equipment filters abnormal traffic, injects the normal traffic, and reports the traffic logs and attack logs to management center. Management center is in charge of monitoring and managing the cleaning equipment, configuring policies, and displaying reports.

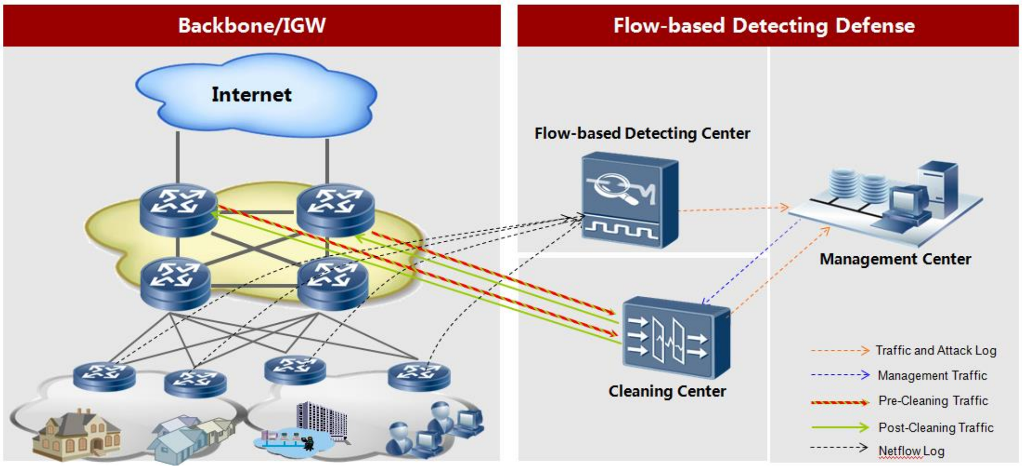
- Deployment Advantages

  The deployment applies to for small-medium data center perimeter protection. The static defense mode provides accurate and always-on detection and cleaning for the specifically protected users with little defense delay.

3.8.2 Dynamic Traffic-Diversion Defense (Off-line)

According to detecting technology, dynamic traffic-diversion defense has two kinds of solutions: flow-based defense solution and per-packet-based defense solution.

Flow-based Defense



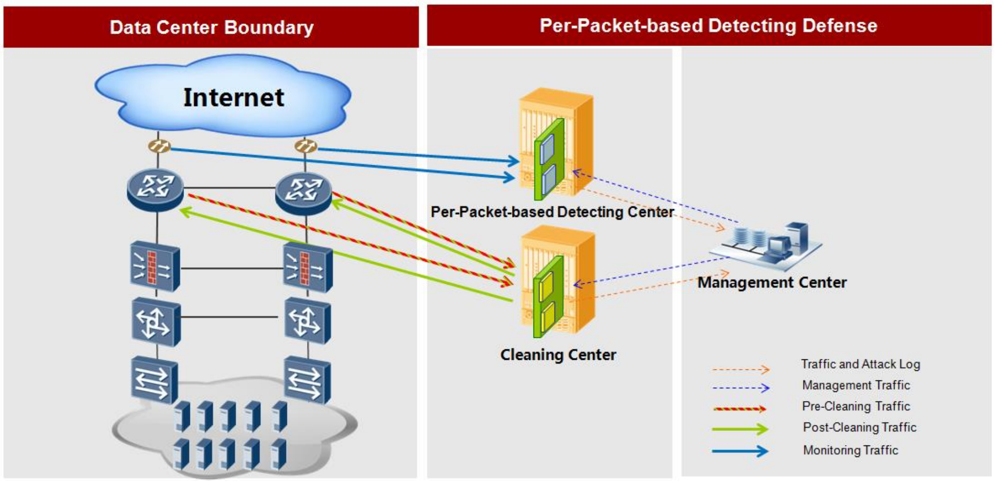
- Deployment description

  The off-line deployment of the flow-based detecting equipment analyzes network anomalies through netflow packets, and notifies management center of anomalies. Then management center delivers the traffic-diversion policy to cleaning center. Cleaning center advertises traffic-diversion routes to divert the traffic for cleaning and injects the cleaned traffic back to the customer's network.

- Deployment advantages

  The deployment mainly applies to backbone network. The deployment has high cost-effective for clean-pipe solution.

Per-packet-based Defense



- Deployment description

  The detecting equipment and cleaning equipment are deployed in off-line mode. The detecting equipment detects mirroring or optical splitting traffic, and notifies management center of anomalies. Then management center delivers the traffic-diversion policy to cleaning center. Cleaning center advertises traffic-diversion routes to divert the traffic for cleaning and injects the cleaned traffic back to the original link.

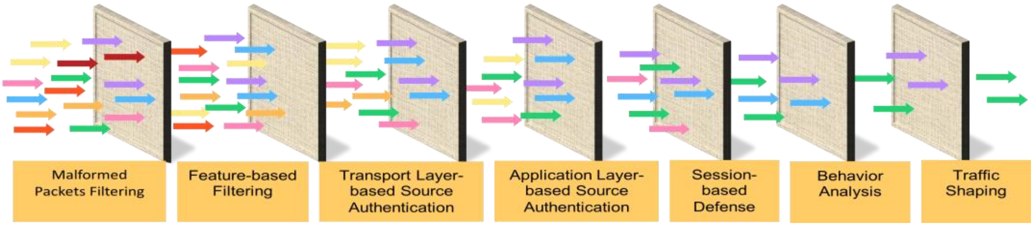
- Deployment advantages

This solution provides accurate and always-on defense for customer’s services. This solution can provide flexible customer strategy for value-add DDoS defense service. This solution is more suitable for data center perimeter protection and MSS scenario.

4 Introduction to the Principles of Defense

4.1 Multi-layered Filtering

Figure 4-1 Multi-layered Filtering Model


Malformed Packets Filtering
Feature-based Filtering
Transport Layer-based Source Authentication
Application Layer-based Source Authentication
Session-based Defense
Behavior Analysis
Traffic Shaping

The cleaning procedures of Huawei Anti-DDoS solution are based on the multi-layer filtering. The main filtering procedure of each layer is as follows:

Step 1 **Malformed Packets Filtering:** Filtering malformed packets according to protocol valid checking.

Step 2 **Feature-based Filtering:** First, packet content-based static filtering is performed for defending against connectionless attacks, such as UDP flooding, UDP-based amplification attacks, DNS flooding, and ICMP flooding. Then static filtering is performed based on blacklists and whitelists.

Step 3 **Transport Layer-based Source Authentication:** This layer can defend against spoofed source attacks. Such as SYN flooding.

Step 4 **Application Layer-based Source Authentication:** This layer can defend against spoofed source attacks and the botnet attacks. Such as DNS Query flooding, HTTP Get/Post flooding, HTTPS flooding, SIP flooding.

Step 5 **Session-based Defense:** This layer can defend against ACK flooding, RST flooding, FIN flooding, TCP connection flooding, Sockstress, TCP Retransmission attack, TCP NULL connection attack, DNS cache poisoning, SSL-DoS/DDoS, HTTP slow headers/post attack. The system collections TCP session information, such as TCP window size, the number of TCP concurrent sessions, the number of TCP new connections per second, the number of TCP retransmission sessions. And blocking those source IPs with abnormal sessions.

Step 6 **Behavior Analysis:** The botnet attacks always have fixed frequency and fixed target. For example, when HTTP Get flooding, the system can learn the fingerprints of URI attacked, and block the source IP who accessing these URI attacked.

Step 7 **Traffic Shaping:** If the traffic is still heavy and exceeds the actual bandwidth of users after previous steps, traffic shaping is used to ensure available network bandwidths.

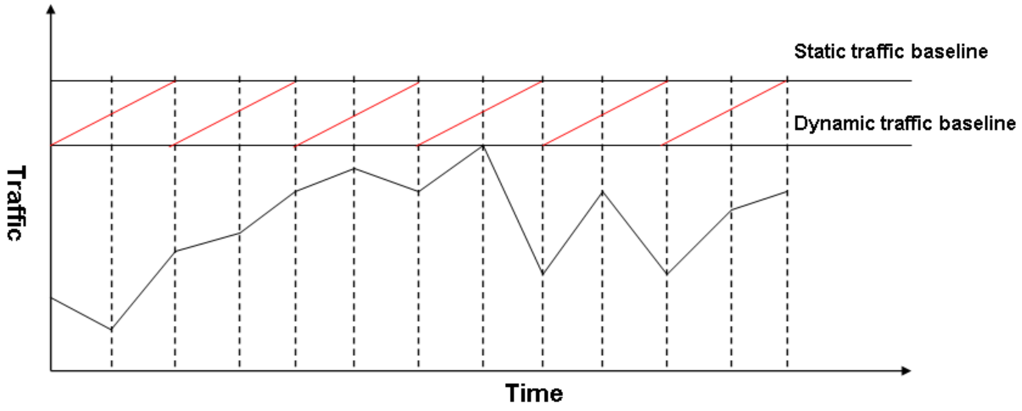
----End

4.2 Introduction to Major Detecting Technologies

4.2.1 Static Threshold Comparison

The detecting equipment collects the statistics on traffic, and then compares the traffic with the pre-defined threshold. If the traffic exceeds the threshold, abnormal traffic occurs. Then management center delivers the traffic diversion policy. Therefore, the accuracy of attack detecting depends on whether the predefined threshold is proper, which in turn is relevant to the experience of configuration personnel. In this case, the detecting threshold is hard to configure for various applications on different networks and differentiated bandwidths. Since the detecting threshold is crucial but the manual configuration is difficult, and the detecting equipment is online permanently, the dynamic traffic baseline is proposed to allow the equipment to dynamically learn various traffic thresholds on networks.

4.2.2 Dynamic Traffic Baseline



Huawei Anti-DDoS solution learns the protected network traffic models. The detecting threshold is specified based on the peak traffic within the learning period and tolerance (avoiding mistaken identification cased by sudden traffic jitter). When the traffic model changes, the Anti-DDoS system re-learns the traffic to obtain a proper detecting threshold.

Huawei per-packet-based detecting system supports 60+ traffic models learning for fast and accurate attack detection.

- 5 statistics dimensions: qps, pps, bps, cps, and ratio
- 8 protocol families: IP, TCP, UDP, ICMP, HTTP, HTTPS, DNS and SIP
- 38 protocol states: TCP Flags, TCP connections, TCP window size, HTTP connections, HTTP URI, HTTP Host, SSL Renegotiating, DNS query, DNS domain, etc.

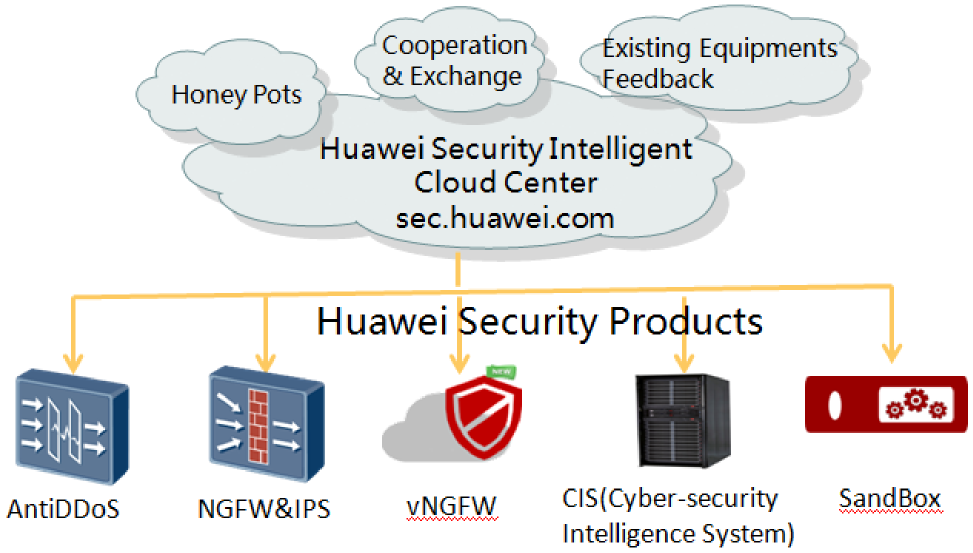
4.3 Introduction to Major Cleaning Technologies

4.3.1 Filtering Based on Signature Database

Huawei security intelligent cloud center supports multiple security knowledge databases which can be updated automatically via a subscription over a secured connection arming them with the latest threat intelligence to thwart modern day attacks or advanced threats. It enables customers to directly benefit from the depth and breadth of Huawei's security research capability.

Huawei security intelligence is from Huawei WeiRan Lab which focuses on developing core security techniques and building an advanced security reputation system and cloud security architecture.

WeiRan Lab are dedicated to discovering and analyzing emerging Internet threats and developing targeted defenses, and uses a sophisticated combination of attack data collection, partner information and analysis tools to create security intelligence that provide detection and defense of advanced threats.


Honey Pots
Cooperation & Exchange
Existing Equipments Feedback
Huawei Security Intelligent Cloud Center
sec.huawei.com
Huawei Security Products
AntiDDoS
NGFW&IPS
vNGFW
CIS(Cyber-security Intelligence System)
SandBox

IP Reputation

Huawei Anti-DDoS solution supports two kinds of IP reputation: global botnet IP reputation and local real-time session reputation.

There are 5 million IP addresses in global botnet IP reputation database with daily updating from Huawei security intelligent cloud center via ATIC. Functions of global botnet IP reputation are as follows:

- An alarm will be triggered when detecting center monitors traffic increasing from botnet IP addresses.
- Cleaning center filters attack traffic from botnet IP addresses.

Tens of millions of local real-time session reputation is generated through normal TCP session-checking as whitelists to avoid negative influence on legal access.

Attacks Tools Signature

Huawei DDoS cleaning center supports signature database to filter attacks. Signature database can be updated from Huawei security intelligent cloud center. Signature database includes r.u.d.y., slowhttptest, slowloris, L.O.I.C., AnonCannon, RefRef, ApacheKill, ApacheBench, etc.

Customer can also delivery attack capture packets or attack tools to Huawei to extract attack signature when 0-day attack occurs.

Geo-IP

Huawei DDoS cleaning center supports Geo-IP location filtering through identifying location by country for sources of traffic to filter traffic from some large DDoS source country.

4.3.2 Static Filtering

Most attacks have obvious signatures. Huawei Anti-DDoS solution supports flexible filters including 3/4-layer and 7-layer packet header and payload. Customers can define the filters via ATIC.

4.3.3 Transport Layer Protocol-based Source Authentication

Cleaning center sends a challenge authentication packet with a cookie to the source IP address when SYN flooding. If the source IP address exists, client responds to the challenge authentication packet with the cookie. Cleaning center can determine whether the source IP address exists by checking the cookie. This technology can effectively defend against the SYN flooding initiated by forged source IP addresses. No session in cleaning center before successful authentication.

4.3.4 Application Layer Protocol-based Source Authentication

HTTP flooding defense as an example, based on HTTP protocol to do challenge authentication, cleaning center checks whether the source IP address is that of the real client. If yes, the source IP address will be put into white-lists, and subsequent access traffic is allowed through. Application layer protocol-based source authentication can effectively defend against the attacks launched by most zombie tools; however, advanced zombie tools launch attacks through the HTTP proxy or directly function as the browser. For the attacks of this type, Huawei cleaning center delivers an advanced HTTP source authentication technology, that is, when an attack occurs, cleaning center prompts the user to enter the check code. Only if the check code is correct, the user can pass identity authentication and continue its access. Since the check code changes randomly, the advanced HTTP source authentication technology can effectively defend against the attacks launched by most zombie tools.

4.3.5 Session Defense

Session-based flooding attack or vulnerability exploit attacks is one of the attacks that occur frequently on current networks and their harms are obvious. By monitoring sessions, Huawei Anti-DDoS cleaning center can identify abnormal sessions and abnormal source IP addresses which continuously establish abnormal sessions with servers in time. This layer can defend against RST flooding, FIN flooding, ACK flooding, TCP connection flooding, sockstress, TCP retransmission attack, TCP NULL connection attack, DNS cache poisoning, SSL-DoS, SSL-DDoS, HTTP slow header/post attack.

4.3.6 Behavior Analysis

Attack behaviors of botnet differ greatly from the access of normal users. The latter features unexpectedness and disorder; however, the former, also called the robot attack, features constant frequency, and stable accessible resources or unchangeable packet loads. Huawei Anti-DDoS cleaning center can use fingerprint learning or TCP packets ratio statistics or access frequency behavior learning to defend against such attacks. By using the behavior analysis, cleaning center can effectively defend against slow SYN flooding, UDP flooding with payload signature, HTTP get flooding with fixed URL and so on.

4.4 Introduction to the Attack Defense Technology

4.4.1 Defense Against Malformed Packet Attacks

Smurf

Attack Principle

A simple Smurf attack is employed to attack a network. The attacker sends an ICMP response request. In this request packet, the destination IP address is set to be the broadcast address of the victim network, so that all hosts on the network reply to this ICMP response request, and thus the network is congested. The traffic of this attack is one or two amplitude levels higher than the traffic of a large ping packet. An advanced Smurf attack is employed to attack the target host. The attacker changes the source IP address of the ICMP response request packet to the IP address of the victim host. As a result, the victim host crashes. Launching an attack requires certain traffic and duration of attack packets. Theoretically, the more hosts that exist on the network, the more obvious the attack effects are.

Defense Principle

Cleaning center checks whether the destination IP address of the ICMP response request packet is the broadcast address or network address of the subnet. If so, directly deny the packet and log the attack.

Land

Attack Principle

The attack sends a packet whose source IP address is the same as the destination IP address, or is a loopback IP address to the target host (the source port is the same as the destination port), so that the target host establishes a connection with itself. In this way, the system resources are greatly occupied, or even the resources are exhausted and the system slows down, crashes or restarts.

Defense Principle

Cleaning center directly discards the SYN packets whose source IP addresses are the same as the destination IP addresses and the SYN packets whose source IP addresses are loopback IP addresses.

Fraggle

Attack Principle

When a UDP port (usually Port 19) on which the Chargen service runs receives a data packet, the UDP port generates a character string as the response. When a UDP port (usually Port 7) on which the echo service runs receives a data packet, it simply returns the data content of this packet as the response. These two types of services may be used by attackers to launch Fraggle attacks. As a result, the victim systems are busy and the links are congested.

Defense Principle

Cleaning center filters the specific types of packets and disables unnecessary services.

Ping Of Death

Attack Principle

When the length field of an IP packet is 16 bits, it means that the maximum length of this IP packet is 65535 bytes. If the data length of an ICMP echo request packet is more than 65508 bytes, the sum of ICMP data length, IP header length (20 bytes), and ICMP header length (8 bytes) is more than 65535 bytes. After receiving such a packet, certain routers or systems crash, stop responding, or restart due to the improper processing of the packet. The so-called Ping of Death is an attack on the system launched through certain oversized ICMP packets.

Defense Principle

Cleaning center detects if the length of the ICMP echo request packet is more than 65535 bytes. If so, discard the packet and log the attack.

Tear Drop

Attack Principle

1 Small fragment attack: The attacker uses the information contained in the packet header of trusted IP fragments in TCP/IP protocol stack implementation to launch an attack evading filtering by cleaning center.

2 Overlapping fragment attack: The attacker uses the vulnerabilities in IP fragment processing by Windows 95/NT/3.1 or the earlier versions of Linux to send UDP data packet fragments with overlapping offset addresses to the victim hosts. As a result, errors occur when the target equipment reassembles the fragments and the target system crashes or restarts.

Defense Principle

Cleaning center buffers the information about the first fragment and subsequent fragments, and performs valid check on the fragments.

WinNuke

Attack Principle

WinNuke attack is also called out-of-band transmission attack. The attacker uses out-of-band data to attack the target port; thus, abnormalities occur when the victim system processes the data. As a result, the victim system stops responding and its screen turns blue. The attacked target ports are usually port 139, 138, 137, 113, and 53, and the URG flag bit is 1.

3 TCP WinNuke: The hacker sends an OOB data packet to the NetBIOS port (139) of the target host (Windows system). As a result, the NetBIOS fragment overlap occurs and the target host crashes.

4 IGMP WinNuke: The hacker sends IGMP fragments to the target host. If the system cannot properly process the IGMP fragments, it crashes.

Defense Principle

A. Cleaning center detects whether the destination port of the TCP packet is Port 139 or any of the above, and whether the TCP URG flag bit is specified.

B. Cleaning center detects whether the IGMP packet is fragmented.

TCP Error Flag

Attack Principle

The TCP flag consists of six bits, namely, URG, ACK, PSH, RST, SYN, and FIN. The attacker sends large numbers of packets with the invalid combinations of TCP flag bits. The victim host has to judge and identify these flag bits; thus, the performance of the victim host is degraded, or even certain operating systems cannot properly process the TCP flag packets, and the host crashes.

Defense Principle

Huawei cleaning center directly discards invalid TCP packets that TCP flag is one of the following:

- All 6 flag bits are set to 1.
- All 6 flag bits are set to 0.
- The SYN bit and the FIN bit are set to 1.
- The SYN bit and the RST bit are set to 1.
- The FIN bit and the RST bit are set to 1.
- The PSH, FIN, and URG bits are set to 1.
- Only the FIN bit is set to 1.
- Only the URG bit is set to 1.
- Only the PSH bit it set to 1.

4.4.2 Defense Against 3/4-layer Attacks

SYN flooding

Attack Principle

The TCP/IP protocol stack only permits a limited number of TCP connections due to resource restriction. The SYN flooding attack utilizes this feature. The attacker forges a SYN packet whose source IP address is forged and initiates a connection to the server. After receiving this packet, the server replies with a SYN/ACK packet. After the response packet is sent, no SYN ACK packet is received, a semi-connection is established. If the attacker sends large numbers of such packets through botnet, a lot of semi-connections are established on the attacked host and the resources of the attacked host are exhausted; therefore, normal users cannot access the host until the semi-connections time out.

Defense Principle

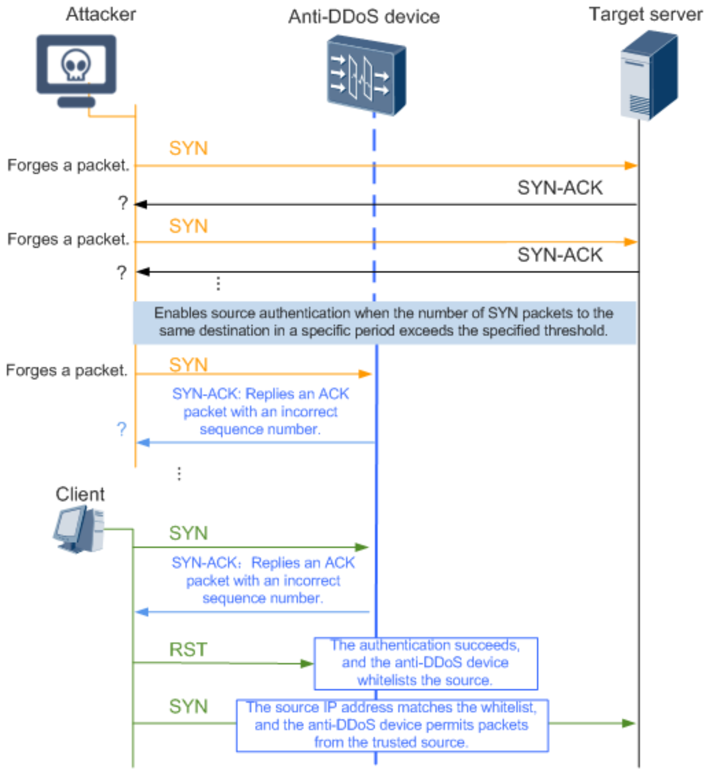
When it detects that SYN packets rate exceeds the specified threshold, detecting center triggers cleaning center to validate the source IP address via challenge authentication based on transmission protocols. The defense procedure is as follows:

Step 1 Cleaning center receives the access packet for the first time and sends the challenge packets with the cookie to the source IP address.

Step 2 The validity of the source IP address is authenticated through the response packets. Thus, the attacks of the forged source IP address are prevented.

Step 3 If the source authentication passed, source IP will be add into whitelists and subsequent TCP packets will directly go into the following process.

----End


Attacker
Anti-DDoS device
Target server
Forges a packet.
SYN
SYN-ACK
?
Forges a packet.
SYN
SYN-ACK
?
Enables source authentication when the number of SYN packets to the same destination in a specific period exceeds the specified threshold.
Forges a packet.
SYN
SYN-ACK: Replies an ACK packet with an incorrect sequence number.
?
Client
SYN
SYN-ACK: Replies an ACK packet with an incorrect sequence number.
RST
The authentication succeeds, and the anti-DDoS device whitelists the source.
SYN
The source IP address matches the whitelist, and the anti-DDoS device permits packets from the trusted source.

TCP flooding

Attack Principle

An attacker uses the botnet to launch the TCP flooding (include ACK flooding, FIN flooding, RST flooding, TCP fragment flooding) to consume the network bandwidth. Meanwhile, after receiving attack packets, the attacked server needs to check whether they belong to a certain session. If there are a large number of attacked packets, the processing performance of the server is consumed up and DDoS attacks occur.

Defense Principle

White-lists, black-lists, IP reputation and session checking are used to defend against TCP subsequent packets flooding.

UDP flooding

Attack Principle

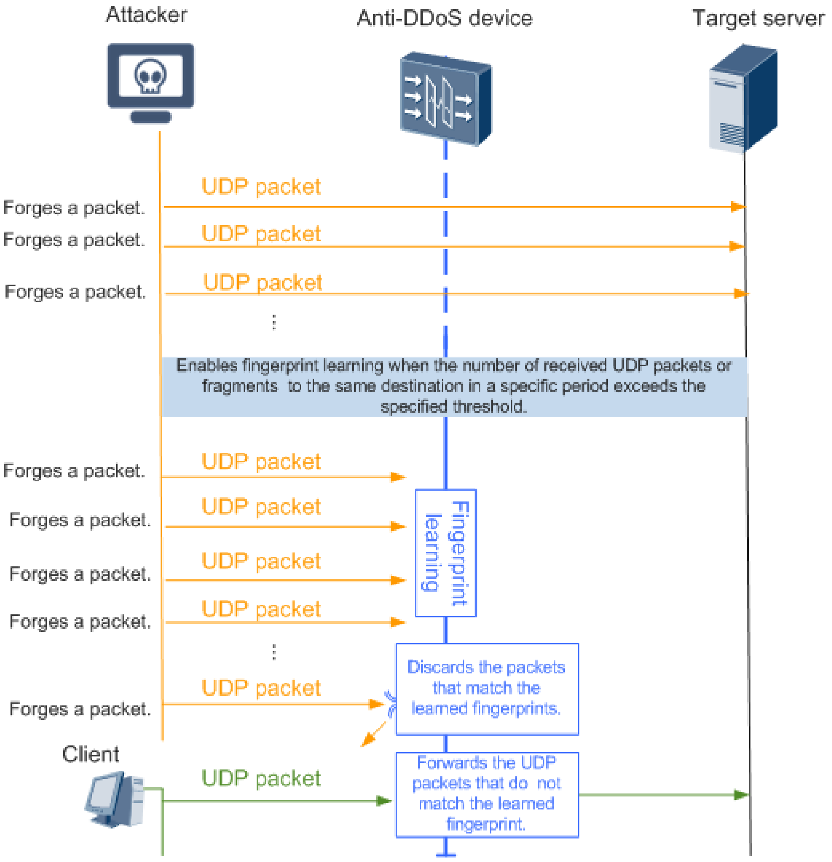
The attacker sends large numbers of large UDP packets or UDP fragments to the target server through botnets. UDP-based reflection amplification attacks increase DDoS attack peak bandwidth. As a result, bandwidth is congested.

Defense Principle

Depending on whether it has fingerprints, UDP flooding can be distinguished as two types. Static signature filtering is the most effective method to defend against UDP flooding with fingerprints. Dynamic fingerprint learning can help customer to extract signature. Only rate-limiting can be used to defend against UDP flooding without fingerprints.

UDP rate limiting can be used as the default defense policy for non-UDP service server.

Dynamic fingerprint learning principle is as follows:


Attacker
Anti-DDoS device
Target server
Forges a packet.
UDP packet
Forges a packet.
UDP packet
Forges a packet.
UDP packet
Enables fingerprint learning when the number of received UDP packets or fragments to the same destination in a specific period exceeds the specified threshold.
Forges a packet.
UDP packet
Forges a packet.
UDP packet
Forges a packet.
UDP packet
Forges a packet.
UDP packet
Fingerprint learning
Forges a packet.
UDP packet
Discards the packets that match the learned fingerprints.
Client
UDP packet
Forwards the UDP packets that do not match the learned fingerprint.

ICMP flooding

Attack Principle

An attacker sends massive ICMP packets to the specific target within a short time period, causing the target system over burdened and hence cannot process legitimate transmission or even the links are congested.

Defense Principle

Rate limiting is the most effective defense technology.

TCP Connection flooding

Attack Principle

For the TCP connection flooding, an attacker initiates large numbers of TCP connections to the server through botnet, and thus consumes the TCP connection resources of the server. Generally, connection flooding attacks include the following attack types:

- Attack type 1: After the three-way handshake, no packet is sent, and these TCP connections are maintained.
- Attack type 2: After the three-way handshake, ACK/PSH packets with random payload are sent ceaselessly.
- Attack type 3: During the connection, server connection resources are consumed through sockstress attacks.
- Attack type 4: Lots of TCP retransmission requests result in uplink congestion.

Defense Principle

Defending against connection flooding attacks is implemented through the collection of the statistics on the new connections, concurrent connections, and abnormal connections of source IP addresses. The source IP addresses that exceed any statistics threshold are blacklisted.

4.4.3 Defense Against 7-layer Attacks

HTTP Get/Post flooding

Attack Principle

The attacker sends large numbers of HTTP Get/Post packets to the target server through zombie hosts. The requests contain the URLs operated by the database or other URLs that consume system resources. As a result, the server resources are exhausted and the server cannot respond to normal requests.

Defense Principle

Collect the HTTP packet statistics on the destination IP addresses. If the packet rate exceeds the threshold, enable the cleaning.

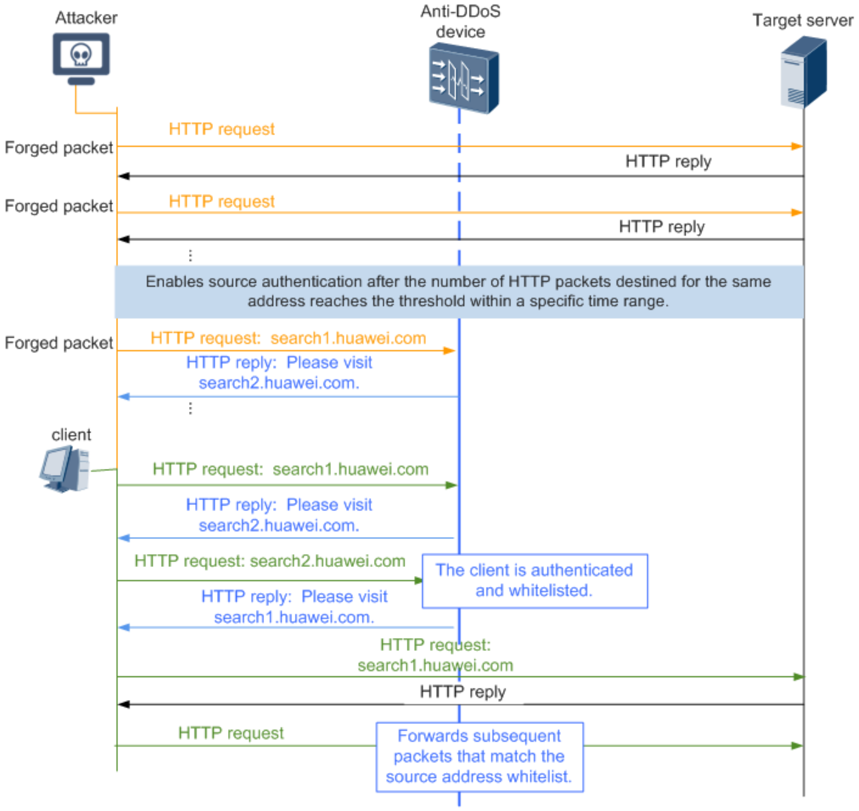
Source authentication defense HTTP Get flooding based on HTTP 302 redirection

The procedure for the source authentication defense based on application protocols is as follows:

Step 1 Cleaning equipment receives HTTP packets. Cleaning center sends the challenge authentication packets with the cookie to the source IP address.

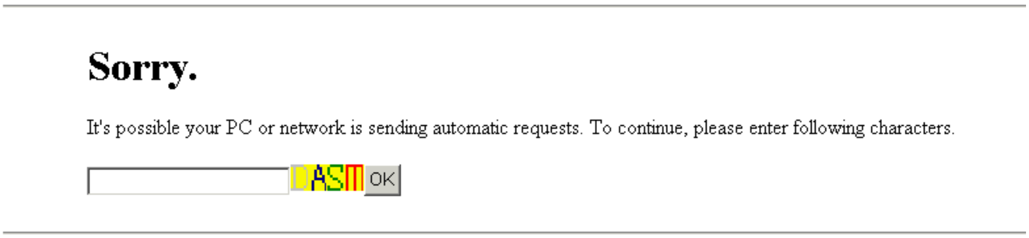
Step 2 The real client responds to the authentication packets. Cleaning center authenticates the validity of the response packets.

Step 3 The source subsequent HTTP packets verified by the authentication directly pass the authentication.


Attacker
Anti-DDoS device
Target server
Forged packet
HTTP request
HTTP reply
Forged packet
HTTP request
HTTP reply
Enables source authentication after the number of HTTP packets destined for the same address reaches the threshold within a specific time range.
Forged packet
HTTP request: search1.huawei.com
HTTP reply: Please visit search2.huawei.com.
client
HTTP request: search1.huawei.com
HTTP reply: Please visit search2.huawei.com.
HTTP request: search2.huawei.com
The client is authenticated and whitelisted.
HTTP reply: Please visit search1.huawei.com.
HTTP request: search1.huawei.com
HTTP reply
HTTP request
Forwards subsequent packets that match the source address whitelist.

Redirection check code input authentication technology

The check code that changes randomly is added to the redirection page. The user can pass authentication and enter the subsequent session after entering the correct check code. Although zombie tools can stimulate the access to the Internet through the proxy, they are non-attendant and thus the randomly-changeable check code becomes unavailable. Therefore, the defense method is effective for the HTTP Get flooding launched by botnet.



Sorry.

It's possible your PC or network is sending automatic requests. To continue, please enter following characters.

----End

DNS Query flooding

Attack Principle

The attacker sends large numbers of the DNS requests of the non-existent domain names to the DNS server through botnet. As a result, the DNS server is overloaded, and cannot continue to respond to the DNS requests of normal users, thus achieving the attack purposes.

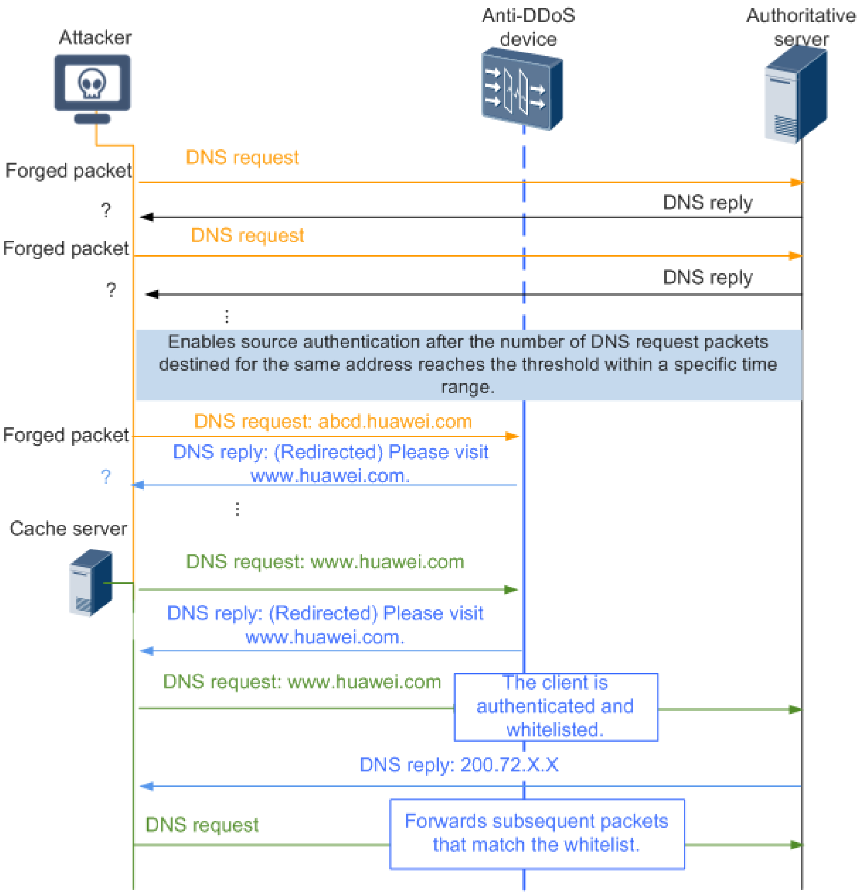
The source IP addresses of the attacks of this type are generally forged. To achieve large-scale attack effect, the attack sets the recursive query field. As a result, the server cannot find the domain record in cache and send request to the recursive DNS server, thus leading to the chain response of massive DNS servers. Attacks target DNS servers can easily lead to large-scale mass panic and are like "nuclear weapons" in cyber attacks. So DNS server is the primary target in politically motivated attacks event.

Defense Principle

Defense against DNS Query flooding Based on Application Layer-based Source Authentication

Application layer-based source authentication is used to defend against DNS query flooding and the follow packets from the source authenticated is forwarded directly.

Defense against DNS Query flooding for DNS authoritative server based on CNAME.


Attacker
Anti-DDoS device
Authoritative server
Forged packet
DNS request
DNS reply
?
Forged packet
DNS request
DNS reply
?
Enables source authentication after the number of DNS request packets destined for the same address reaches the threshold within a specific time range.
Forged packet
DNS request: abcd.huawei.com
DNS reply: (Redirected) Please visit www.huawei.com.
?
Cache server
DNS request: www.huawei.com
DNS reply: (Redirected) Please visit www.huawei.com.
DNS request: www.huawei.com
The client is authenticated and whitelisted.
DNS reply: 200.72.X.X
DNS request
Forwards subsequent packets that match the whitelist.

For DNS cache server protection, the Anti-DDoS system defense against DNS Query flooding through passive defense based on DNS packet retransmission.

HTTP Slow Attacks

Attack Principle

HTTP slow attacks are used to attack HTTP servers by keep the connections to the HTTP servers alive as long as possible. Slow POST and slow Headers are common slow HTTP attacks:

- Slow POST: An attacker sends POST packets with the content-length field being set to a large value. However, subsequent packets are small. The server keeps waiting for the attacker to complete packet sending.
- Slow Header: An attacker initiates a connection to the server using GET or POST packets, but does not send the ending character during the transmission of HTTP header. Then the attacker sends other fields to keep the connection alive. The server keeps waiting for a terminator.

Defense Principle

If the number of new HTTP connections per second reaches a specified value, cleaning center starts HTTP session check. If either of the following types of packets are detected, cleaning center considers them as slow HTTP attack packets, adds the source IP address to the dynamic blacklist, and disconnect the IP address from the HTTP server.

- The lengths of consecutive HTTP POST packets are large, but the payload lengths are small.
- The header of consecutive HTTP GET/POST packet does not contain any terminator.

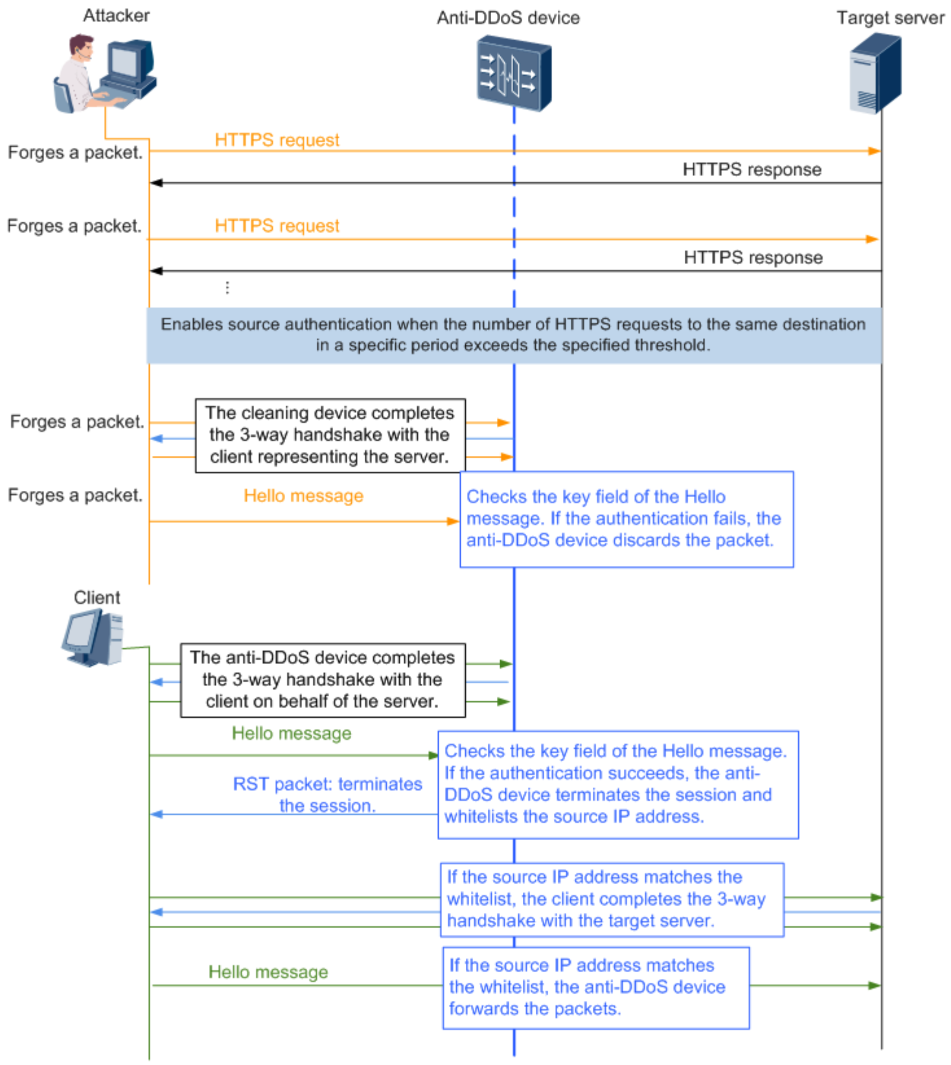
HTTPS flooding

Attack Principle

An attacker sends a large number of HTTPS flooding packets to the target server directly or through proxies or botnet. As a result, server resources are exhausted and cannot respond to normal requests.

Defense Principle

When identifying that the packet rate of the destination IP address exceeds the pre-defined threshold, cleaning center enables the authentication for the source IP addresses of packets, and allows authenticated packets through.


Attacker
Anti-DDoS device
Target server
Forges a packet.
HTTPS request
HTTPS response
Forges a packet.
HTTPS request
HTTPS response
Enables source authentication when the number of HTTPS requests to the same destination in a specific period exceeds the specified threshold.
Forges a packet.
The cleaning device completes the 3-way handshake with the client representing the server.
Forges a packet.
Hello message
Checks the key field of the Hello message. If the authentication fails, the anti-DDoS device discards the packet.
Client
The anti-DDoS device completes the 3-way handshake with the client on behalf of the server.
Hello message
Checks the key field of the Hello message. If the authentication succeeds, the anti-DDoS device terminates the session and whitelists the source IP address.
RST packet: terminates the session.
If the source IP address matches the whitelist, the client completes the 3-way handshake with the target server.
Hello message
If the source IP address matches the whitelist, the anti-DDoS device forwards the packets.

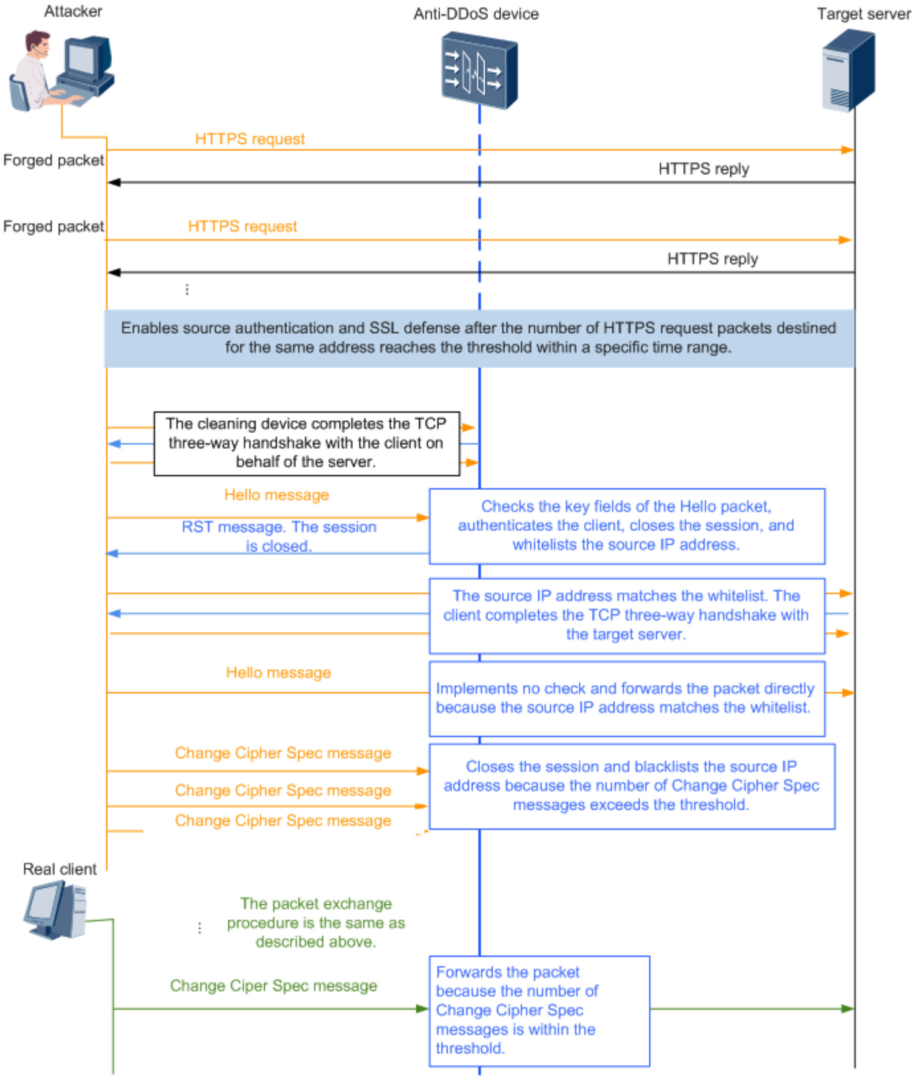
SSL-DoS/DDoS

Attack Principle

In SSL handshakes, the CPU usage on the server is about 15 times that on the client during encryption algorithm negotiation. An attacker may take advantage of this feature to initiate rapid and continuous renegotiations (allowed by SSL) in a TCP connection to exhaust CPU resources on a server. This attack is called SSL-DoS. In SSL-DDoS attacks, multiple zombie hosts are used to launch SSL-DoS attacks to the server.

Defense Principle

In a negotiation check cycle, if the number of renegotiations in one session from a source address to the destination address exceeds the threshold, cleaning center marks the session as abnormal. In a session anomaly check cycle, if the number of abnormal sessions exceeds the threshold, cleaning center blacklists the source address.


Attacker
Anti-DDoS device
Target server
Forged packet
HTTPS request
HTTPS reply
Forged packet
HTTPS request
HTTPS reply
Enables source authentication and SSL defense after the number of HTTPS request packets destined for the same address reaches the threshold within a specific time range.
The cleaning device completes the TCP three-way handshake with the client on behalf of the server.
Hello message
RST message. The session is closed.
Checks the key fields of the Hello packet, authenticates the client, closes the session, and whitelists the source IP address.
The source IP address matches the whitelist. The client completes the TCP three-way handshake with the target server.
Hello message
Implements no check and forwards the packet directly because the source IP address matches the whitelist.
Change Cipher Spec message
Change Cipher Spec message
Change Cipher Spec message
Closes the session and blacklists the source IP address because the number of Change Cipher Spec messages exceeds the threshold.
Real client
The packet exchange procedure is the same as described above.
Change Ciper Spec message
Forwards the packet because the number of Change Cipher Spec messages is within the threshold.

A Acronyms and Abbreviations

Acronym and Abbreviation	Full Spelling	Description
BGP	Border Gateway Protocol	Border gateway routing protocol
DoS	Denial of Service	Denial of Service
DDoS	Distributed Denial of Service	Distributed Denial of Service
Huawei Anti-DDoS Solution	Huawei Anti-DDoS Solution	Huawei delivers multi-layer protection against DDoS attacks by integrating on-premise defense with powerful cloud-based DDoS mitigation service. On-premise system defends against attacks in the bandwidth range of the customer's network, and Huawei global near-source cloud mitigation service handles large DDoS attacks to protect the availability of customer's network bandwidth. Huawei delivers automatic defense by integrating on-premise defense solution and global near-source cloud mitigation solution through the cloud signal. Huawei on-premise defense solution includes detecting center, cleaning center, and management center. Generally, detecting center detects optical splitting or mirroring traffic and delivers alarms to management center when detecting center finds attacks against protected network. After that, management center triggers cleaning center to divert traffic. Traffic to the protected network is redirected to cleaning center by BGP announce. Cleaning center filters abnormal traffic and injects the normal traffic to the protected network. At the same time, cleaning center reports cleaning logs to management center. At last, management center displays reports.

Acronym and Abbreviation	Full Spelling	Description
Detecting Center	Detecting Center	According to detecting technology, detecting center has two kinds of equipments: flow-based detecting equipment and per-packet-based detecting equipment. The per-packet-based detecting equipment processes mirroring or optical splitting traffic. When the per-packet-based equipment identifies the abnormal traffic to protected network, it reports management center to trigger traffic-diversion. The flow-based detecting equipment receives netflow logs (such as netflow, sflow, netstream, and cflow packets, etc.) from routers. Based on netflow logs, the flow-based detecting equipment counts and detects the traffic of protected network. When the flow-based detecting equipment identifies the abnormal traffic to protected network, it reports management center to trigger traffic-diversion.
Cleaning Center	Cleaning Center	Cleaning center is in charge of differentiating the normal traffic and abnormal traffic via layer-to-layer cleaning, discarding abnormal traffic, and injecting normal traffic.
Management Center	Management Center	Management center based on the B/S architecture is in charge of the centralized management of detecting and cleaning equipments of Huawei Anti-DDoS solution, defense policy configuration, and reports. In Huawei Anti-DDoS solution, management center includes the management server and data collector, which can either be deployed on one server of the X86 platform or be deployed independently. The operating system adopted by both the management server and data collectors is Windows 2008/2012 Server. When management center is deployed in distributed mode, a management server can manage a maximum of 50 data collectors. The data collector receives and resolves the traffic logs and exception or attack logs from the detecting or cleaning equipment, and summarizes and stores these logs for the management server to manage and query them. For better performance, it is recommended that one data collector corresponds to one detecting or cleaning equipment in the solution.

Acronym and Abbreviation	Full Spelling	Description
Data Collector	Data Collector	Management center of Huawei Anti-DDoS solution supports the distributed deployment. The data collector not only collects, resolves, and stores service data, but also summarizes the data for the management server to manage and query them. The data collector saves the packets captured by the detecting and cleaning equipments into the .pcap files, and then the management server can manage them. The management server can monitor the performance of the data collector.
Zone	Zone	A group of protected IP addresses can be multiple IP addresses or the IP address segments defined by the mask. To realize the refined defense for the services externally, you can configure the defense policy for each service of zone and set the proper detecting threshold and select appropriate defense policy. In MSS scenario, Zone and customer can be corresponded in order to provide customized defense policies and reports.
Exception Log	Exception Log	If detecting center or the detecting module of cleaning center identifies that the traffic statistics exceed the traffic threshold, it reports exception logs to management center.
Attack Log	Attack Log	After abnormal traffic occurs, the cleaning function is enabled. Cleaning center reports attack logs to management center.
MSS	Managed Security Service	The system supports zone-based defense policies and reports and customized portal for self-service reports.
On-premise defense system	On-premise defense system	On-premise DDoS defense system deployed at the customer's network edge serves as a first line of defense against attacks to the customer's network. Huawei on-premise DDoS defense solution is designed to automatically detect and mitigate attacks for protecting application availability.
Cloud-based mitigation	Cloud-based mitigation	Huawei global near-source cloud mitigation service provides global scrubbing capacity and can handle today's largest and most complex attacks that threaten the availability of customer network bandwidth.