AntiDDoS8000 DDoS Protection Systems

Background and Challenges

With the IT and network evolution, the Distributed Denial of Service (DDoS) attack has already broken away from original hacker behaviors. Instead, it forms an integral dark industry chain with overwhelming damages.

Severe DDoS attacks
At present, a single DDoS attack consumes more than 500 Gbit/s bandwidth. The number of DDoS attacks is 20 times of that in 2007, and over 30,000,000 zombie hosts flood the network. Moreover, attack tools become easily available. Large numbers of botnets break off the technical threshold for DDoS attacks. A DDoS attack is launched by only three steps, namely, downloading the attack tool, purchasing zombie hosts, and initiating the attack.

Traffic DDoS attacks evolve to application attacks
In the past, flood attacks were prevailing on the carrier network and infrastructure. In comparison, current DDoS attacks are specific to applications and services, such as enterprise portal applications, online shopping, online videos, online games, Domain Name Service (DNS), and email. The targets of attacks become more extensive. A single attack consumes less traffic and fewer costs. The attack behavior becomes more complex and difficult to distinguish. This brings difficulty in detecting and defending against DDoS attacks.

Service interruption adversely affects enterprise operation
DDoS attacks frequently intrude into the service systems of enterprises, and severely interrupt the normal service operation. On the one hand, service interruption damages enterprises' brand images, takes away their customers, and reduces their profits, especially for small Internet enterprises on e-business, online games, and portals. On the other hand, constructing an anti-DDoS system brings intensive investment and maintenance pressure on these enterprises and deteriorates their normal service operation.

DDoS attacks cause IDC customer loss
If a service system suffers from DDoS attacks, the attack traffic occupies the entire Internet Data Center (IDC) bandwidth, affecting the service systems of other leasers. As a result, IDC leasers quit, competitiveness lowers, and operation costs rise. These side impacts severely deteriorate the service operation and profits.
Solution Highlights

Overview
Designed for carriers, enterprises, data centers, and ICP service providers (including providers for web portals, online games, online videos, and DNS services), Huawei AntiDDoS8000 series incorporates extensive experience in network security and full understanding of customer demands.

Huawei AntiDDoS8000 series enhances defense against application-layer attacks, IPv4-IPv6 attack defense, and defense against zombies, Trojan horses, and worms. This fully ensures network security and service continuity.

Huawei AntiDDoS8000 series uses the leaser-specific service design for management configuration, which implements a series of functions, including leaser service model learning, leaser configuration, and report self-service. Moreover, IDC operators can provide the anti-DDoS solution for their leasers as a SaaS service to increase the leaser viscosity, improve IDC competitiveness, and add IDC operation profits.

Functions

Service-based defense policy
Huawei AntiDDoS8000 series supports continuously periodic learning and analysis on the service traffic of the Zone, draws the outline of normal service traffic, and enables differentiated defense types and policies for various services or one service in different time ranges, therefore implementing refined defense.

Accurate abnormal traffic cleaning
Huawei AntiDDoS8000 series uses Big Data analyticstechnology to detect and defend against DDoS attacks, learning traffic models from over 60 dimensions and building traffic models. Once abnormal traffic occurs in a certain dimension, the corresponding defense policy is triggered and enabled immediately. This solution applies multiple technologies, including seven-layer filtering, behavior analysis, and session monitoring, to accurately defend against various flood attacks, Web application attacks, DNS attacks, SSL DoS/DDoS attacks, and protocol stack vulnerability attacks. In this way, application servers are protected.

Intelligently caching DNS traffic
Besides accurately defending against various attacks on the DNS server, Huawei Anti-DDoS Solution supports DNS cache for improved performance under heavy DNS server traffic.

Defense against prevailing zombies/Trojan horses/worms
By spreading Trojan horses and worms to large numbers of hosts, hackers control the hosts hierarchically and form the botnet to launch attacks. Therefore, botnets breed DDoS attacks. Huawei Anti-DDoS Solution identifies and blocks over 200 common zombies/Trojan horses/worms worldwide, therefore smashing botnets.

Perfect IPv4-IPv6 defense
In February 2011, Internet Assigned Numbers Authority (IANA) declared that IPv4 addresses were exhausted. Enterprises have no new IPv4 addresses and begin to put IPv6 network construction into agenda. The particular IPv4-IPv6 technology of Huawei Anti-DDoS Solution supports concurrent defense against DDoS attacks on both IPv4 and IPv6 networks. The solution addresses the DDoS attack defense requirements in dual stack and helps users transit to the next generation network.

Flexible networking
The anti-DDoS solution must be adaptive to various network environments and address different grades of service requirements.

On this basis, Huawei AntiDDoS8000 series provides multiple in-line and off-line deployments, which enable...
customers to select flexibly by their services and networks.

In-line deployment: serially connects the detecting and cleaning modules to the network to be protected for direct traffic detecting and cleaning. The high-performance and multi-core hardware platform in use not only ensures the detecting and cleaning accuracy, but also minimizes the processing delay.

Off-line traffic-diversion deployment: deploys the cleaning module on the network in off-line mode. Once detecting DDoS attack traffic, the detecting and cleaning centers perform actions based on the policies configured in the management center.

**Highlights**

Highlights of Huawei AntiDDoS8000 series:

**Anti-Large-DDoS, Heavy Traffic DDoS Attack Defense**
- Multi-core, distributed hardware architecture and Big Data-based Intelligent Defense Engine provide T-bit defense performance.
- Instant attack response within seconds protects link availability.

**Anti-App-DDoS, Application DDoS Attack Defense**
- Performs all traffic collection and 3/4/7-layer packet-by-packet analysis, create traffics models from over 60 dimensions, and provides the most precise and comprehensive attack detection.
- Fine-grained reputation system consisting of local session behavior-based reputation, service access behavior-based reputation, geographical location-based reputation, and botnet cloud-based reputation precisely guards against various lightweight, slow application-layer DDoS attacks launched by botnets.
- Full-scale defense against over 100 attacks guarantees continuous operations of key service systems that encompass enterprise web applications and DNS, DHCP, and VoIP services.

**Anti-Mobile-DDoS, Mobile DDoS Attack Defense**
- Dynamic, real-time upgrade of 20,000 fingerprints and filtering of mobile terminal botnet tool features effectively defend DDoS attacks launched by botnets and mobile terminals and guarantees authorized access to mobile gateways.
- Protects availability of mobile data service systems such as mobile payment, mobile store, mobile social networking, and mobile game.

**Anti-Outbound-DDoS: Inbound-to-Outbound DDoS Attack Defense**
- Blocks the global most active zombie, Trojan horse, and worm controlling traffic.
- Blocks C&C DNS request traffic.
- Prevents DDoS attacks at the source.

**Managed-Anti-DDoS, DDoS Attack Defense Operations**
- Provides tenant/service-based automatic and manual defense policies and complete defense methods.
- Tenant/service-based independent statistics reports and email sending simplify defense management.
- Increases tenants’ service stickiness by providing Portal-based self-service functions for tenants.
- Supports large-scale operations, for example, 100,000 tenants/services, and protects 200,000 IP addresses of each tenant/service simultaneously.
Solution Components

As shown in the following figure, Huawei Anti-DDoS Solution comprises the detecting center, cleaning center, and ATIC management center. By means of policy interworking and control interworking, the three centers provide a professional anti-DDoS solution with easy management and flexible deployment for customers.

- Detecting center: As the “antenna” of the entire solution, the detecting center receives detecting policies delivered by the ATIC management center, identities and detects DDoS traffic, and gives detecting results back to the ATIC management center.
- Cleaning center: As the “executor” of the entire solution, the cleaning center cleans DDoS traffic on the network based on the control signals delivered by the ATIC management center.
- ATIC management center: As the “brain” of the solution, the ATIC management center allows the user to customize detecting and cleaning policies and delivers the policies to the detecting center and cleaning center to control the detecting and cleaning process. Meanwhile, the user can also generate and view attack reports and cleaning records in the ATIC management center.

Typical Application Scenarios

IDC Secure and Profitable Operation

Huawei AntiDDoS8000 series deployed at the IDC egress delivers the following functions:

- Defends against attacks on the DNS server, for example, DNS protocol stack vulnerability attacks, DNS reflection attacks, DNS flood attacks, and DNS CacheMiss attacks, and supports DNS cache for improved DNS server performance under heavy traffic.
- Defends against attacks on Web servers, for example, SYN flood attacks, HTTP flood attacks, CC attacks, and low-rate connection attacks.
- Defends against attacks on online games, for example, UDP flood attacks, SYN flood attacks, and TCP attacks.
- Defends against SSL DoS/DDoS attacks on HTTPS servers.
- Provides customers with self-service policy configuration and report by operating anti-DDoS as a security service.
Customer Challenges

Tencent IDC processes huge services and suffers from various DDoS attacks from the Internet every day, especially those attacks on online games and DNS servers. Defending devices, such as traditional firewalls and IPS devices, are not sharp in DDoS attack defense. When DDoS attacks are launched, these devices may exhaust connections and resources. Enabling attack defense may interrupt normal services. Therefore, Tencent is confronted with big security challenges.

Solution

Deploy an AntiDDoS8000 series as cleaning device at the Tencent IDC egress in off-line mode to defend against DDoS attacks on the IDC service system.

This deployment requires high performance, reliability, and scalability of the anti-DDoS device. Then, the device must be able to restore services rapidly after an incident occurs. Next, all the deployed AntiDDoS8000 series devices can be managed in a global way.

Huawei Anti-DDoS Solution, applying to multiple Tencent IDCs, features high performance, sound reliability, and fine defense effects, and meets with a favorable reception in Tencent.
**Customer Benefits**

Huawei device displays normal status during IDC attack defense and successfully defends against continuous DNS flood attacks. The protected services operate stably, and no user complaint is received. Therefore, Huawei device is highly regarded by the personnel in the service line.

**Specifications**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Abuse Attack Defense, Defense against IP spoofing, LAND, Fraggle, Smurf, Winnuke, Ping of Death, Tear Drop, IP Option, IP Fragment Control Packet, TCP Label Validity Check, Large ICMP Control Packet, ICMP Redirect Control Packet, and ICMP Unreachable Control Packet attacks, etc.</td>
<td>Web application attacks defense: HTTP Get Flood attacks, HTTP Post Flood attacks, HTTP Head Flood attacks, HTTP Slow Header attacks, HTTP Slow Post attacks, HTTPS Flood attacks, SSL DoS/DDoS attacks, etc.</td>
<td>Defense against DNS Query Flood attacks from real or spoofed source IP addresses, DNS Reply Flood attacks, DNS Cache Poisoning attacks, DNS Protocol Vulnerability Exploits, and DNS Reflection attacks.</td>
<td>SIP Methods Flood; Register Flood; Deregistration Flood; Authentication Flood; Call Flooding, etc.</td>
<td>UDP Flood Attacks, UDP Fragment Flood Attacks, etc.</td>
<td>DHCP Flood</td>
<td>Defensible DDoS attacks launched by mobile botnets, for example, AnDOSid/WebLOIC/Android. DDoS.1.origin</td>
</tr>
<tr>
<td>Scanning and Sniffing Attack Defense: Defense against Port Scanning, IP Scanning, Tracert Control Packet, IP Option, IP Timestamp, and IP Routing Record attacks, etc.</td>
<td>Web application intrusion filter functions: SQL injection attacks filter; XSS cross site attacks, etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network-layer Attack Defense: SYN Flood Attacks, ACK Flood Attacks, FIN/RST Flood Attacks, TCP fragment Flood Attacks, ICMP Flood, TCP Connection Flood, Sockstress Attacks, TCP Retransmission, and TCP Null Connection attacks, IPv6 Attacks, etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reflection And Amplification Attacks Defense: NTP Reflection and Amplification attacks, SNMP Reflection and Amplification attacks, TFTP Reflection and Amplification attacks, NetBIOS Reflection and Amplification attacks, SSDP Reflection and Amplification attacks, QOTD Reflection and Amplification attacks, Quake Reflection and Amplification attacks, Steam Reflection and Amplification attacks, etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zombie, Trojan horse, Worm and Tools Traffic Blocking: Blocking of controlling traffic of active zombies, Trojan horses, worms, and tools, such as LOIC, HOIC, Slowloris, Pyloris, HttpDosTool, Slowhttptest, Thc-ssl-dos, YoyoDDOS, IMDDOS, Puppet, Storm, fengyun, AladinDDoS, And so on C&amp;C DNS request traffic blocking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature-based Filtering Blacklist, HTTP/DNS/SIP/DHCP field-based filtering, and IP/TCP/UDP/ICMP/Other Protocol field-based and load feature-based filtering.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Reputation Database 12 data centers across the globe process 12 billion query analysis requests on a daily basis and tracks the global most active 5 million zombie hosts with a daily update.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Management and Reports:

Supports account management and rights allocation; supports 10,000 defense objects; supports import of defense policies in batches; supports device performance monitoring; supports source tracking through packet capture and fingerprint extraction; supports SMS/Voice/Email alarming; supports log dumping; supports network traffic model learning; supports multidimensional reports including attack traffic analysis, attack event analysis, and attack trend analysis; supports download of reports in multiple formats such as HTML, PDF, Excel, and CSV; supports report push through emails; and supports Portal-based operations.

Networking and Traffic Diversion Policies

Deployment Modes:
Supports inline and bypass deployment.

Traffic Diversion and Rejection Policies:


Rejection Functions: Support MPLS Rejection, MPLS LSP Rejection, GRE Tunnel Rejection, Layer-2 Rejection and policy Routing Rejection, etc.

Interface and Hardware Parameters

<table>
<thead>
<tr>
<th>AntiDDoS8000系列</th>
<th>Max Performance</th>
<th>Max Performance/Slot</th>
<th>slot</th>
<th>Interface Card Type</th>
<th>Power Supply Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntiDDoS8030 (4 U Height)</td>
<td>120Gbps</td>
<td>120Gbps</td>
<td>3</td>
<td>LPUF-40 interface card</td>
<td>Supports both DC and AC power supply.</td>
</tr>
<tr>
<td>AntiDDoS8080 (14 U Height)</td>
<td>720Gbps</td>
<td>160Gbps</td>
<td>8</td>
<td>LPUF-120 interface card</td>
<td></td>
</tr>
<tr>
<td>AntiDDoS8160 (32 U Height)</td>
<td>1.44Tbps</td>
<td>160Gbps</td>
<td>16</td>
<td>LPUF-240 interface card</td>
<td></td>
</tr>
</tbody>
</table>

Reliability

Supports dual MPUs and achieves a five-nine carrier-grade reliability (99.999%).