1.1 Introduction

The modern world is witnessing exponential growth of network attacks. For example, in 2010 alone the rate of distributed denial-of-service (DDoS) traffic attacks on bandwidth was 100 Gbit/s, a 1000% increase compared with that in 2005. These emerging attacks target specific application-layer protocols, such as HTTP, HTTPS, SIP, and DNS. These new malicious attacks render conventional flow devices ineffective. Consequently, customers are faced with the following problems:
- How to withstand massive flooding and application-layer attacks while securing the network
- How to maximize investments on DDoS defense while reducing maintenance costs

Based on long-accumulated security technologies and deep understanding on customer requirements, Huawei has devised a traffic cleaning solution able to secure customers’ networks while simplifying their management needs. The solution is specifically tailored for:
- Large and medium-sized enterprises
- Internet data centers (IDCs)
- Internet service providers (ISPs), including web portals, game service providers, and DNS service providers

1.2 Solution

The Huawei traffic cleaning solution can be divided into three centers, as shown in the following figure.

1.3 Hardware

The following figure shows detecting and cleaning devices involved in the solution.
1.4 Features

1.4.1 Industry’s Highest Performance to Secure the Network

- **High Performance**
  - With an industry-leading processing capacity of 160 Gbit/s per chassis, the solution can withstand large-scale attacks.
  - Advanced architecture
  - Built on the network processor (NP), multicore CPU, and distributed architecture, the detecting and cleaning centers provide linear capacity expansion capability to overcome bottlenecks in processing performance.
  - High capacity
  - The solution provides fine-grained protection for 2000 VIP customers and 10,000 IP addresses and provides coarse-grained protection for 1 million IP addresses.

- **Highest Detection Rate**
  - With DPI technology and a solid 7-layer defense structure, the solution can efficiently prevent various attacks from occurring.
  - Deep Packet Inspection (DPI)
  - Unlike conventional Netflow-based devices, Huawei’s detecting devices use DPI technology to analyze every byte inside packets, and use the 7-layer defense structure to effectively identify attack types, including traffic, application-layer, scanning and snooping, and malformed packet attacks.

- **High Reliability**
  - Reliable platform
    - Hardware platform:
      - ≥ 1+1 main processing engines
      - ≥ 3+1 switching boards
      - Key component (power module and fan) redundancy
      - Core router-class service stability
    - Versatile Routing Platform (VRP):
      - ≥ Independent modules with little impact on each other
      - ≥ 4 million devices on live networks
  - Reliable system
    - The solution ensures 500,000 hours of mean time between failures (MTBF) and 99.9999% reliability through:
      - Inter-board load balancing
      - Cross-board interface binding
    - Two-node cluster hot backup
    - The solution provides a flexible graphical user interface which simplifies configuration and maintenance and reduces operating expenses (OPEX).
    - Flexible evidence collection methods
      - The solution collects evidences in either of the following ways:
        - Packet capture based on access control lists (ACLs)
        - Automatic packet capture based on the types of attack events
    - Centralized management
      - The solution manages distributed peripheral devices in a centralized and simplified mode, which decreases management servers and significantly reduces maintenance costs.

- **Easy Management and Low OPEX**
  - Graphical management
    - The solution provides a flexible graphical user interface which simplifies configuration and maintenance and reduces operating expenses (OPEX).
  - Easy Management and Low Expansion Cost
    - Software license upgrade
      - The E1000E supports software license upgrades to expand the cleaning capacity without adding hardware, which thereby greatly reduces costs.
    - Smooth upgrade
      - The E1000E supports smooth capacity expansion.
    - Linear expansion
      - The E1000E supports a maximum of eight service boards per chassis. Users can add service boards to expand the capacity. The expansion mode improves investment efficiency and reduces capacity expansion.
1.5 Application Scenarios

1.5.1 IDC Security

- **Customer Challenges**
The service-rich IDC with egress bandwidth is vulnerable to flooding attacks and application-layer attacks.

- **Solution Benefits**
  - Provides a processing capacity of 160 Gbit/s per chassis and quick response (within seconds).
  - Withstands over 30 types of DDoS attacks, including e.g.:
    - UDP Flood attacks
    - CC attacks
    - HTTP Flood attacks
    - HTTPS Flood attacks
    - DNS attacks
    - Slow attacks

1.5.2 Web Portal or Game Server Security

- **Customer Challenges**
Web portals or game servers with egress bandwidth are vulnerable to flooding attacks and application-layer attacks.

- **Solution Benefits**
  - Provides a processing capacity of 160 Gbit/s per chassis and quick response (within seconds).
  - Withstands over 30 types of DDoS attacks, including e.g.:
    - UDP Flood attacks
    - CC attacks
    - HTTP Flood attacks
    - TCP Flood attacks

The following figure shows the anti-DDoS network of a web portal or game website.

1.5.3 Enterprise Network Egress Security

- **Customer Challenges**
Large and medium-sized enterprises build networks or rent links (about 10 GB) to enable office automation (OA) and internal communication, which is vulnerable to DDoS attacks.

- **Solution Benefits**
Withstands over 30 types of DDoS attacks, particularly those attacks aimed at OA networks, including:
  - UDP Flood attacks
  - HTTP Flood attacks
  - TCP Flood attacks

The following figure shows the anti-DDoS network of an enterprise.
1.5.4 Online Service Security

- **Customer Challenges**
  Online services are vulnerable to DDoS attacks. These attacks severely compromise a service provider’s customer base, financial security, and reputation.

- **Solution Benefits**
  Withstands over 30 types of DDoS attacks, particularly those aimed at online transaction systems, including:
  - HTTP Flood attacks
  - HTTPS Flood attacks
  - CC attacks
  - Slow link attacks
  - DNS attacks (DNS Query and Reply Flood)

The following figure shows the anti-DDoS network of online services.

1.5.5 DNS Security

- **Customer Challenges**
  DNS servers, a vital part of the Internet infrastructure, are often subject to DDoS attacks, which brings serious consequences onto its customers whom have shown vested interests in securing their DNS services.

- **Solution Benefits**
  - Withstands over 30 types of DDoS attacks, particularly those attacks aimed at DNS services, including:
    - DNS attacks (DNS Query and Reply Flood)
    - DNS cache poisoning
    - UDP Flood attacks
  - Provides the Top N DNS cache function to alleviate the DNS server’s pressure in coping with attacks.

The following figure shows the anti-DDoS network of a DNS sever.
1.6 Product Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>E1000E-I/D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of slots</td>
<td>For a 1 U device: 4 pairs of GE optical/electrical (mutually exclusive) interfaces, 2 USB 2.0 interfaces</td>
</tr>
<tr>
<td>Detecting and cleaning capacity</td>
<td>4G</td>
</tr>
<tr>
<td>Protected destination IP addresses</td>
<td>√ Protected targets: 400, IP addresses (fine-grained protection): 2048</td>
</tr>
</tbody>
</table>

### Preventable DDoS attacks (Applicable to IPv4, IPv6, and IPv4-IPv6 networks)

- **Traffic-type attacks**
  - SYN Flood
  - ACK Flood
  - FIN/RST Flood
  - IP Fragment Flood
  - UDP Flood
  - ICMP Flood
  - Smurf attack

- **Application-layer attacks**
  - Connection Flood
  - DNS Query Flood
  - DNS Reply Flood
  - HTTP Get/Post Flood
  - CC attack
  - SIP Flood
  - HTTPS Flood

- **Scanning and snooping attacks**
  - Port scanning
  - Address scanning
  - Tracert packet
  - IP source routing option attack
  - IP timestamp option attack
  - IP routing record option attack

- **Malformed packet attacks**
  - IP Spoofing
  - LAND attack
  - Fraggle attack
  - Wnnuke
  - Ping of Death
  - Tear Drop
  - IP Option control
  - IP fragment control packet
  - Invalid TCP flag attack
  - Super large ICMP control packet
  - ICMP redirect packet
  - ICMP unreachable packet

### Reliability
- Dual power modules and fans
- Module/Component hot swap, two-node cluster hot backup, link aggregation, and 1+1 main processing engines

### Interface board type
- Ethernet interface card: 1 x 10GE, 12 x 1G (optical/electrical)
- POS interface card: 1 x 10G

### Dimensions (W x D x H)
- 436 x 560 x 44.2 mm

### Weight
- 10 kg

### Power
- 100 W

### Mean time between failures (MTBF)
- 37.54 years

---

Model | Eudemon8080E | Eudemon8160E
---|---|---
Number of slots | 8 slots, a maximum of 4 detecting/cleaning boards and 4 interface boards | 16 slots, a maximum of 8 detecting/cleaning boards and 8 interface boards
Detecting and cleaning capacity | 80G | 160G
Protected IP addresses | Protected targets: 2000, IP addresses (fine-grained protection): 10,000, IP addresses (coarse-grained protection): 1 million | Protected targets: 4000, IP addresses (fine-grained protection): 2048, IP addresses (coarse-grained protection): 2048
Application-layer attacks | Connection Flood, DNS Query Flood, DNS Reply Flood, HTTP Get/Post Flood, CC attack, SIP Flood, HTTPS Flood | LAND attack, Fraggle attack, Wnnuke, Ping of Death, Tear Drop, IP Option control, IP fragment control packet, Invalid TCP flag attack, Super large ICMP control packet, ICMP redirect packet, ICMP unreachable packet
Reliability | Module/Component hot swap, two-node cluster hot backup, link aggregation, and 1+1 main processing engines | Module/Component hot swap, two-node cluster hot backup, link aggregation, and 1+1 main processing engines
Interface board type | Ethernet interface card: 1 x 10GE, 12 x 1G (optical/electrical) | POS interface card: 1 x 10G
Maximum interfaces | Ethernet interface 8 x 12 x 1GE, 8 x 10GE | POS interface 8 x 10G, 16 x 10G
### Traffic cleaning service board

<table>
<thead>
<tr>
<th>Model</th>
<th>Eudemon8080E</th>
<th>Eudemon8160E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (W x D x H)</td>
<td>442 x 669 x 886 mm</td>
<td>442 x 669 x 1600 mm</td>
</tr>
<tr>
<td>Weight</td>
<td>100 kg</td>
<td>150 kg</td>
</tr>
<tr>
<td>Power</td>
<td>700 W</td>
<td>900 W</td>
</tr>
<tr>
<td>MTBF</td>
<td>57 years</td>
<td>57 years</td>
</tr>
</tbody>
</table>

#### DDoS Attack Defense

- **Defense against attacks based on protection targets**: Supported
- **SYN Flood defense**: Supported
- **SYN-ACK Flood defense**: Supported
- **ACK Flood defense**: Supported
- **HTTP Flood defense**: Supported
- **HTTPS Flood defense**: Supported
- **DNS Request Flood defense**: Supported
- **DNS Reply Flood defense**: Supported
- **SIP Flood defense**: Supported
- **RST Flood/FIN Flood defense**: Supported
- **UDP Flood defense**: Supported
- **IP Fragment Flood defense**: Supported
- **Non-TCP/UDP/ICMP protocol packet flood defense**: Supported
- **CC attack defense**: Supported
- **Connection flood defense**: Supported

#### Traffic statistics and limit

- Supported

#### Global packet capture

- Supported

#### Abnormal event packet capture

- Supported

#### Static fingerprint

- Supported

#### Global feature filtering

- Supported

#### Attack logs

- Supported

#### Abnormal logs

- Supported

### 1.7 Order Information

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1000E-VD</td>
<td>E1000E anti-DDoS cleaning host, AC, 2G license HS universal security platform software</td>
</tr>
<tr>
<td>SU4Z1ADGD01</td>
<td>E1000E anti-DDoS cleaning host, AC, 2G license HS universal security platform software</td>
</tr>
<tr>
<td>SU4Z2ADGD01</td>
<td>E1000E anti-DDoS cleaning host, DC, 2G license HS universal security platform software</td>
</tr>
<tr>
<td>SU4Z1ADGI01</td>
<td>E1000E anti-DDoS detecting host, AC HS universal security platform software</td>
</tr>
<tr>
<td>SU4Z2ADGI01</td>
<td>E1000E anti-DDoS detecting host, DC HS universal security platform software</td>
</tr>
<tr>
<td>FWEM0004FE02</td>
<td>4-port 100 M Ethernet electrical interface module (RJ45)</td>
</tr>
<tr>
<td>FWBM12GE</td>
<td>2-port 1000 M Ethernet electrical interface module (RJ45 and SFP)</td>
</tr>
<tr>
<td>L5UADGD01</td>
<td>License used to expand the anti-DDoS cleaning capacity of the E1000E to 4G HS universal security platform software</td>
</tr>
<tr>
<td>ATIC3-WINDOWS</td>
<td>Software suite, ATIC management system installation package, DVD</td>
</tr>
<tr>
<td>E8000E Anti-DDoS</td>
<td>Eudemon8080E AC: 1 chassis, 2 power modules, 2 SRUs, 2 switch boards, 4 1G memory modules, 4 CF cards</td>
</tr>
<tr>
<td>E8008E-BUNDLE-AC</td>
<td>Eudemon8080E AC: 1 chassis, 2 power modules, 2 SRUs, 2 switch boards, 4 1G memory modules, 4 CF cards</td>
</tr>
<tr>
<td>E8008E-BUNDLE-DC</td>
<td>Eudemon8080E DC: 1 chassis, 2 power modules, 2 SRUs, 2 switch boards, 4 1G memory modules, 4 CF cards</td>
</tr>
<tr>
<td>Model</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FWCD10GD0D01</td>
<td>Service processing unit, 10G detecting capacity</td>
</tr>
<tr>
<td></td>
<td>HS universal security platform software</td>
</tr>
<tr>
<td>FWCD10GD0C01</td>
<td>Service processing unit, 10G cleaning capacity</td>
</tr>
<tr>
<td></td>
<td>HS universal security platform software</td>
</tr>
<tr>
<td>FWCD20GD0D01</td>
<td>Service processing unit, 20G detecting capacity</td>
</tr>
<tr>
<td></td>
<td>HS universal security platform software</td>
</tr>
<tr>
<td>FWCD20GD0C01</td>
<td>Service processing unit, 20G cleaning capacity</td>
</tr>
<tr>
<td></td>
<td>HS universal security platform software</td>
</tr>
<tr>
<td>FWCD10GDOU01</td>
<td>Plug-in board used to expand the anti-DDoS detecting capacity from 10G to 20G</td>
</tr>
<tr>
<td>FWCD10GDOU01</td>
<td>Plug-in board used to expand the anti-DDoS cleaning capacity from 10G to 20G</td>
</tr>
<tr>
<td>FWC2L0PK01</td>
<td>Flexible card line processing unit (LPKF-21, two sub-slots)</td>
</tr>
<tr>
<td>FWC2L1XX01</td>
<td>1-port 10GBase WAN/LAN-XFP flexible sub-card</td>
</tr>
<tr>
<td>FWC2E8G01</td>
<td>12-port 10GBase-X-SFP flexible sub-card</td>
</tr>
<tr>
<td>FWC2E8G01</td>
<td>12-port 10GBase-X-SFP flexible sub-card</td>
</tr>
<tr>
<td>FWC2P1XXB20</td>
<td>1-port OC-192c/STM-64c POS-XFP flexible sub-card</td>
</tr>
<tr>
<td>FWC500NOFA00</td>
<td>DDoS management center, a collection of functions for non-carrier customers</td>
</tr>
<tr>
<td>FWC500DOFA00</td>
<td>DDoS management center, a collection of functions for carriers</td>
</tr>
<tr>
<td>FWC500IC00</td>
<td>Data collector</td>
</tr>
<tr>
<td>FWC500BM00</td>
<td>DDoS management center-basic modules</td>
</tr>
<tr>
<td>FWC500ST00</td>
<td>DDoS management center-statistical report management</td>
</tr>
<tr>
<td>FWC500AL00</td>
<td>DDoS management center-alarm management</td>
</tr>
<tr>
<td>FWC501PC00</td>
<td>DDoS management center-packet capture analysis management</td>
</tr>
<tr>
<td>FWC501SH00</td>
<td>DDoS management center-self-service query</td>
</tr>
<tr>
<td>FWC505DM00</td>
<td>DDoS management center license (to add 5 control devices)</td>
</tr>
<tr>
<td>FWC510DM00</td>
<td>DDoS management center license (to add 10 control devices)</td>
</tr>
<tr>
<td>FWC525DM00</td>
<td>DDoS management center license (to add 25 control devices)</td>
</tr>
<tr>
<td>FWC550DM00</td>
<td>DDoS management center license (to add 50 control devices)</td>
</tr>
</tbody>
</table>