HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

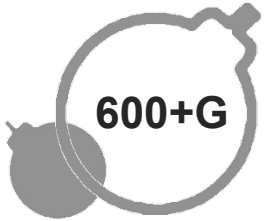
# Huawei Next-Generation Anti-DDoS Solution

enterprise.huawei.com
HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

# DDoS Attacks Trends

## Attacks Traffic Larger




2014-15

3X Growth in max. attack traffic volume

8X >20 Gbps attacks

6X Growth in average attack bandwidth

## More Mobile-Based Attacks

2014-15

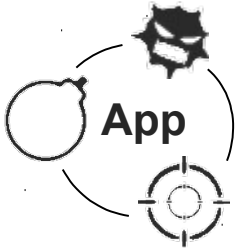
331 LTE commercial use networks

Smart terminal growth

46%

Increases in Mobile attack tools

## More Application Attacks



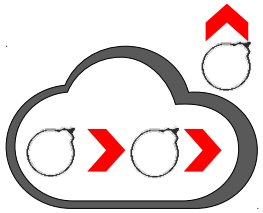

2014-15

42% Application level targeted attack growth

26% HTTP flood

40% Hybrid attack growth

## More Attacks launched from DCs



A growing number of attacks coming from Internet Data Centers.

Compromised DC servers being used as zombies.

IDCs have huge attack bandwidth capabilities.

Majority of large scale attacks are from IDCs.

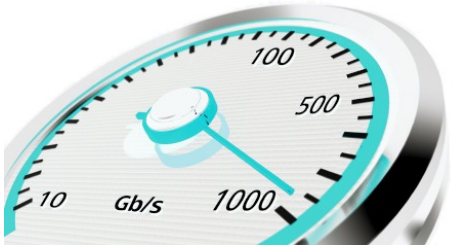


HUAWEI

# Anti-DDoS Solution You Need

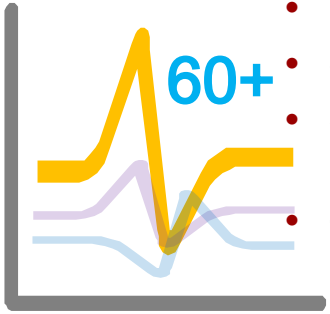
- ✓ **Excellent Capabilities** - to detect and defend wide range of attacks
- ✓ **Rich Knowledge** - large attack database with most up-to-date intelligence
- ✓ **Dynamic Solution** - scale from a small local attack to a large volumetric attacks

# Huawei Anti-DDoS Capabilities




- **T-grade defense performance**
  120G/240G LPU ， 160G SPU
  1.44Tbps defense performance
- **Attack response time: <5s**
- **Latency: 80us**

## T-grade Defense Performance




- **5 dimensions**
  qps, pps, bps, cps, and ratio
- **8 protocol families**
  IP, TCP, UDP, ICMP, HTTP, DNS, HTTPS, and SIP
- **38 protocol statuses**
  TCP Flags, TCP connections, TCP window size, UDP fragment, HTTP connections, HTTP URI, HTTP Host, SSL Renegotiating, DNS query, and DNS domain...
- **60+ traffic models**
  TCP SYN pps, UDP packet bps, DNS pps, HTTP get QPS, SIP pps, ICMP pps, TCP FIN pps, and TCP ACK pps...

## 60+ Traffic Models

- **Global botnet IP reputation**
  Reputation database with **5 million** IP addresses with dynamic updates on a daily basis.
- **Local real-time session reputation**
  **Tens of millions of sessions** guarantee authorized users' service access.
- **Proactive botnet defense feature library**
  **500+** active zombie, Trojan horse, and worm control packet feature library and C&C domains library.

## Full-Scale Reputation System

- **Dynamic fingerprint learning**
  Over 20,000 dynamic fingerprint features with real-time updates to find out attacks.
- **Static fingerprints**
  **10+** global active zombie tools fingerprints
- **Web intrusion fingerprints**
  **400+** SQL injection and XSS fingerprints

## Fingerprint Protection

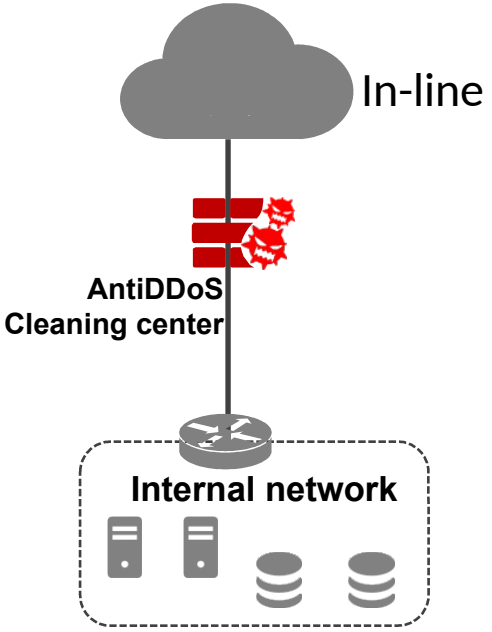


HUAWEI

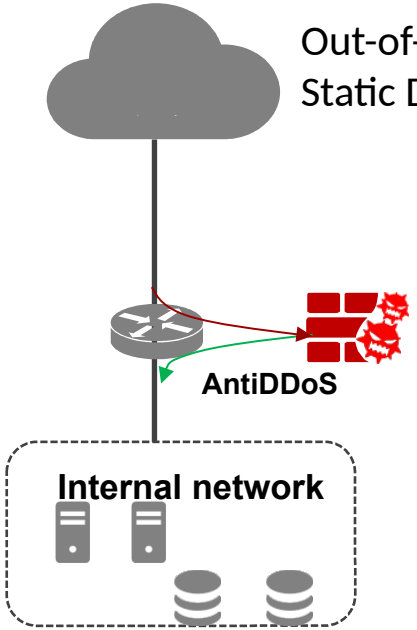
# Huawei Knowledge in Threat Intelligences

| | IP Reputation Signature | DDoS Tools Signature | Web Intrusion Signature | Malware Traffic Signature |
|---|---|---|---|---|
| **Function** | Identify the Botnet DDoS attack by IP Reputation database | Identify the DDoS attack by DDoS attack tools database | Identify the DDoS attack by web intrusion database | Botnet detecting and blocking |
| **Capacity** | 5M | 10+ category | 1) 200+ SQL intrusion<br>2) 200+ XSS | 1) 60+ Trojan<br>2) 150+ worm<br>3) 280+ backdoor |
| **Source** | 1. Buy from Cyren<br>2. Honeynet(China, HK)<br>3. Open sources*<br>4. Partnership: Tencent, Baidu, Nexusguard<br>5. DNS-based detection botnet(2016Q4) | Huawei Self-developed (Huawei Security Research Center) | Huawei Self-developed (Huawei Security Research Center) | Huawei Self-developed (Huawei Security Research Center) |
| **Update interval** | Daily | Weekly | Weekly | Weekly |

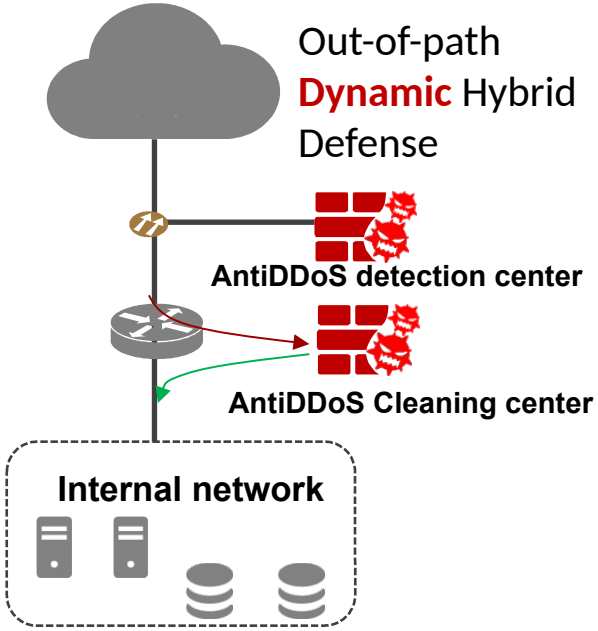
# Deployment Scenarios




- Transparent/Router Mode
- Support bypass
- Middle-Size deployment
- Simple deployment




- Suit for IDC scenario
- High Reliability
- Lower cost deployment

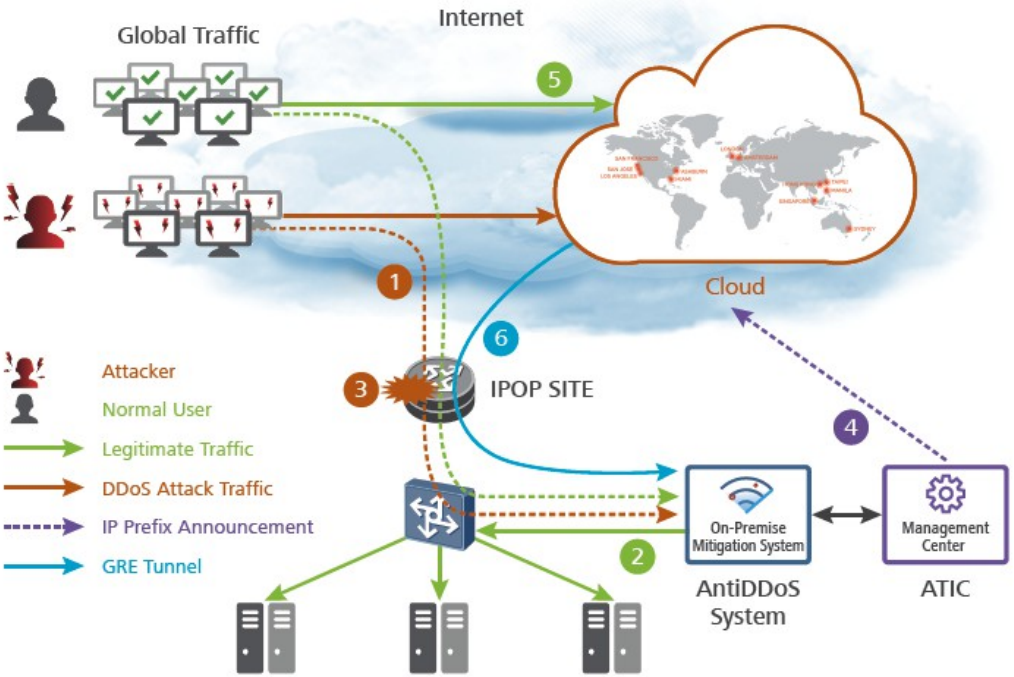



- Can be operate as service in IDC Scenario
- High Reliability
- Easy to manage



HUAWEI

# Huawei Dynamic Hybrid DDoS Mitigation Solution




① Global attack traffic mixed with normal traffic comes into customers network.

② Huawei on-premise mitigation system mitigates the attack traffic and re-inject normal traffic into customers network.

③ The attack traffic increases continuously and exceeds the network threshold, which causes congestion of the upstream link.

④ Huawei DDoS Management Center sends cloud mitigation signal to Cloud.

⑤ Global scrubbing centers advertise routes and distribute traffic.

⑥ After mitigation, the normal traffic will be re-injected into customer's network via GRE tunnels.

# Huawei Global Cloud Scrubbing Centers

- Huawei & partners provide cloud mitigation center in Asia , Europe, and North America to mitigate the global DDoS attack
- A total of 2T+ mitigation capacity help to resolve the super large traffic attack which congest the uplink.


| Partner | capacity | Region | Mitigation Center |
|---|---|---|---|
| Global | 1.2T | USA | • San Jose<br>• Miami<br>• Los Angeles<br>• Ashburn |
| | | Europe | • London |
| | | Asia | • Singapore<br>• Hong Kong |
| China | 1.2T | China | • Beijing<br>• Shanghai<br>• Guangzhou<br>• Hong Kong |



HUAWEI

# Detection Options (Flow vs. Per-Packet)

| | Flow-base Detection | Per-packet-based Detection |
|---|---|---|
| Protection Capability | Volumetric attack<br>Session Exhaustion attack | Volumetric attack<br>Session Exhaustion attack<br>**Application Layer attack** |
| Response Time | 2~3+ minutes | **2~3 seconds** |
| Requirements on Router/Switch | **Routers or switches must support feature to exports netflow information** | **No additional requirements on existing network's router and switch** |
| Performance demand | Lower for large network(>200Gbps)<br>(Based on flow sample, e.g. 1000:1) | Higher for large network(>200Gbps)<br>(Detects every packets) |
| Scalability | Not linear expansion<br>1. If the network bandwidth is lower than the flow analyzer capacity, no need to expand flow analyzer<br>2. If the network bandwidth exceeds the capacity of flow analyzer, expand to flow analyzer) | Add detection links<br>(Linear expansion with physical network bandwidth growth) |
| Summary | Less accurate detection and longer latency<br>Additional requirements on NEs | Faster and more accurate detection<br>No additional requirements on exiting NEs;<br>Higher cost, need expansion with network links |

# Key Differentiations of Huawei Hybrid DDoS Solution

- Per packet detection
  - no performance impact to existing network infrastructure
  - detection in 2-3 seconds
- Protection against application-layer and volumetric attacks
- Global scrubbing centers – 2.4T total capacity
- Near-source mitigation
- Automatic cloud signaling trigger cloud mitigation
- Collaboration: Global threat intelligence coverage
- Real-time monitoring through portal


# Huawei Enterprise A Better Way