HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

Attacks and Mitigation Methods In Huawei’s Perspective

Sep. 2014

enterprise.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

HKNOG

Hong Kong Network Operators' Group

HUAWEI

Security Challenges Facing Carriers and Driving Forces for Security Investment

Increasing Security Threats

Threat Defense

- Shorten equipment failure time
- Filter out sharp increasing junk mails
- Defend against known attacks
- Improve capability to defend against unknown threats

User Private Data Leakage

Privacy Protection

- Protect user data from theft

Ever Evolving Network

Network Evolution

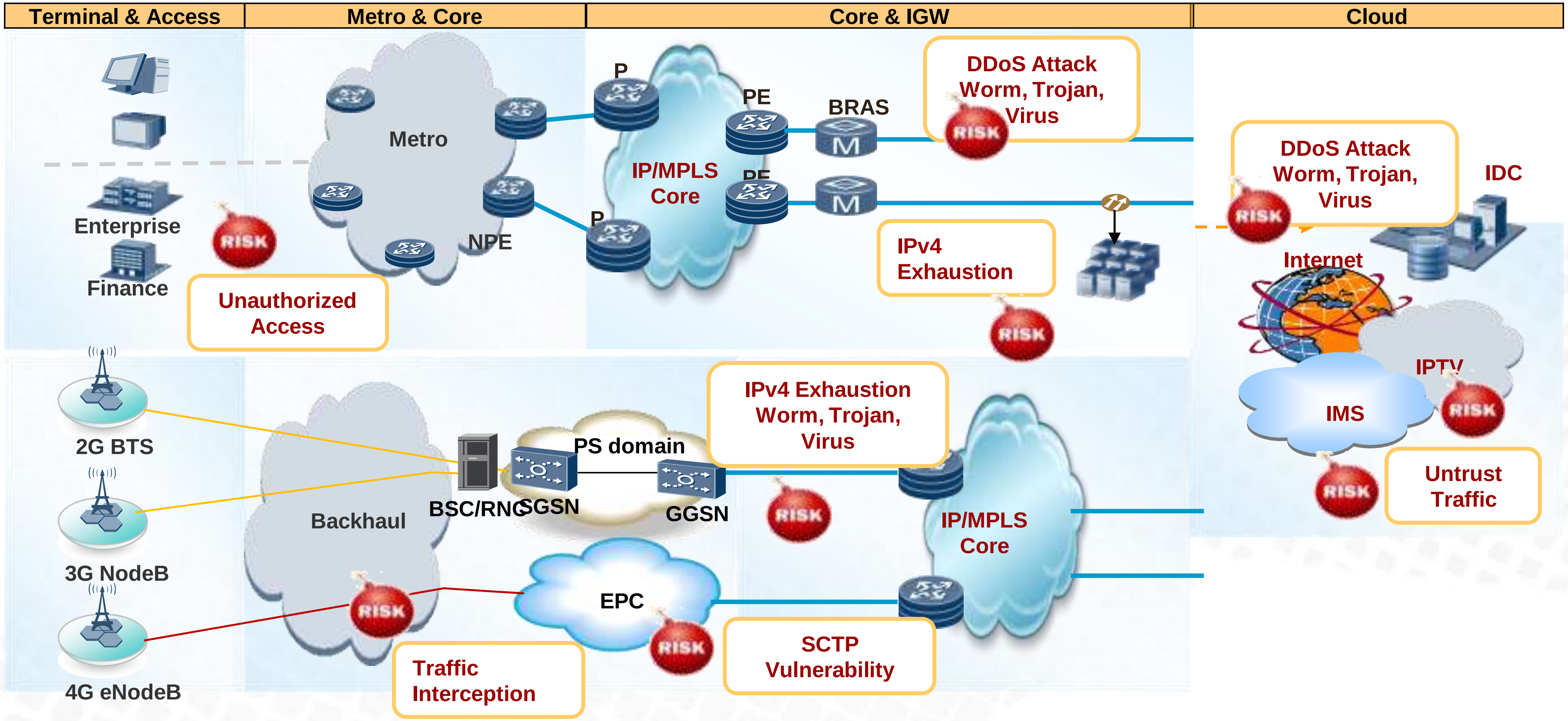
- Handle fast increasing traffic on backbone network
- Adapt to mobile network traffic growth
- Upgrade data center
- Employ cloud-based security solution

Limited Profitability

Profit Earning

- Seek new sources of profit
- Retain competitiveness of existing services

Threats Facing Carrier Networks



Comprehensive Detection: Defending Against All Possible Threats

Server-side attack detection

- Prevents various server-side attacks through HTTP, FTP, DNS, and Email, such as buffer overflow, system or service vulnerability exploitation attacks, and brute force attacks.

Client-side attack detection

- Provides in-depth detection for common applications, such as Office documents, PDF files, multimedia files, and browsers, preventing them from being the victims of Trojan horses or Botnets.

Web attack detection

- Protects Web applications, including Web 2.0 applications and their databases, from attacks, such as code injections and cross-site scripting attacks.

Network abuse detection

- Restricts the access to P2P and video-streaming applications, ensuring the bandwidth for services.
- Restricts the access to IM, online storage, web mails, VPN, online stocking, and online games, improving work efficiency.

Malware detection

- Worm
- Trojan horse
- Spyware
- Adware
- Botnet

DDoS attack detection

- Traffic-oriented DoS attacks
- Application-specific DoS attacks
- Operating system-specific DoS attacks
- Scanning and probing attacks

Low Negative Detection Rates Using Various Technologies

Full Stack Visibility

Ensures the detection on applications on ephemeral ports

Anti-evasion

Packet/flow Reassembly

File Type Identification

*Frequently used file type including *.doc, *.pdf etc…*

Signature Based Detection

Attack/vulnerability signature

Behavior Analysis

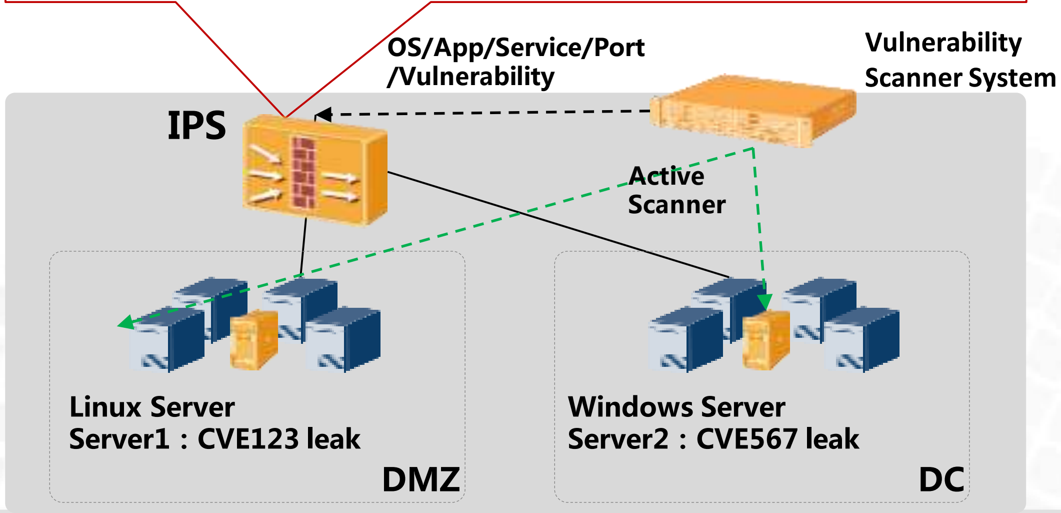
Abnormal Behavior detection including unknown vulnerability etc…

Heuristic Learning

Based on attack mechanism

IPS Policy Optimization

Previous IPS policy：
DMZ：DMZ default signature, CVE123 not enabled
DC：DC default signature, CVE567 not enabled
IT assets and vulnerability awareness：
DMZ： All Linux servers，has CVE123 vulnerability
DC：All Windows servers，has CVE567 vulnerability
ECS policy optimization：
DMZ：DMZ template Linux default signature，CVE123 signature enabled
DC：enable DC model Windows default signature，CVE567 signature enabled

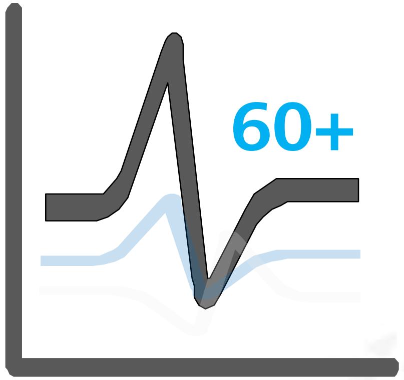


- **IPS Optimization**
  - According to OS/App/Service/Port/Leaks in IT environment, give a suggestion
  - Continuously IPS policy optimization

- **Value：**
  - Improve IPS Performance；
  - Vulnerabilities awareness and protection
  - Decrease false detection and report
  - Decrease maintenance cost and TCO

100% Data Collection & Analysis Make Response Faster

- 100% data detection
- Per packet 3 to 7 layer detection
- TCP behavior based on session
- Application behavior based on user



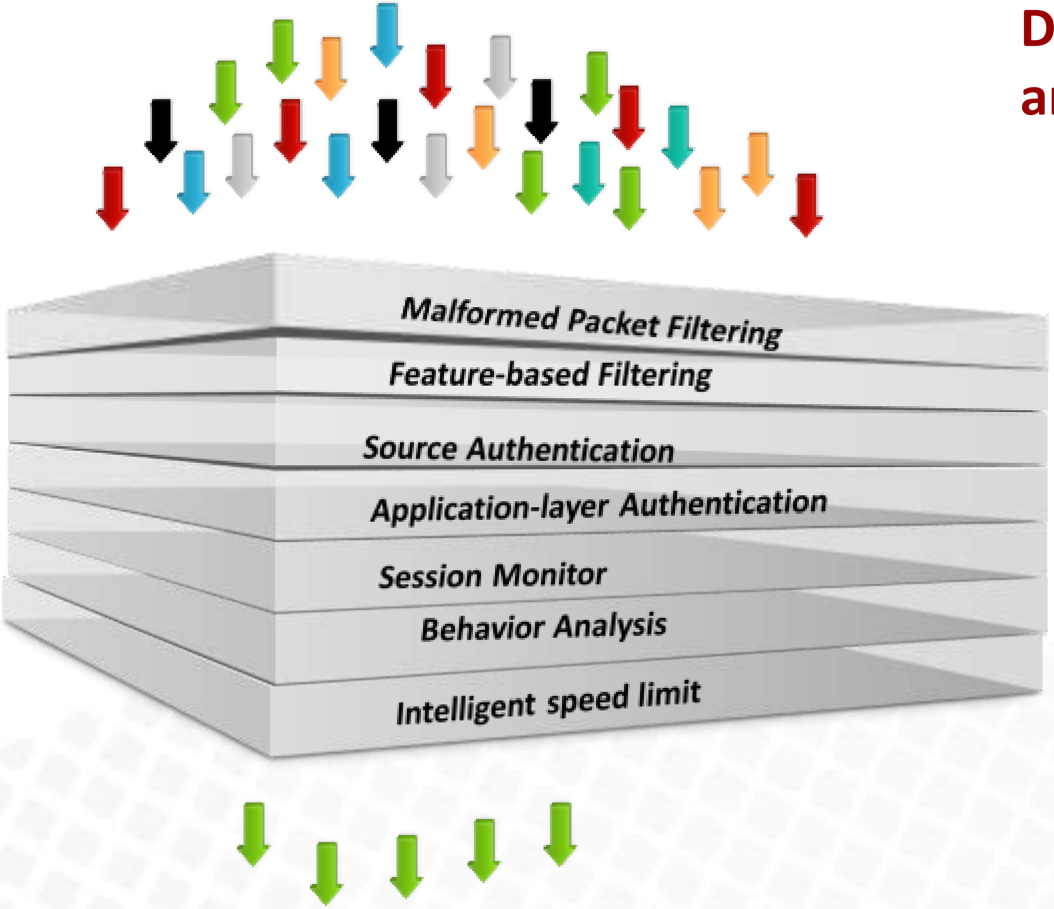
- 5 Dimensions: qps/pps/bps/cps and ratio
- 8 Protocols: IP/TCP/UDP/ICMP/DNS/HTTP/HTTPS/SIP
- 38 Protocol state
  - TCP Flags/TCP connections /TCP window size/UDP fragment、 HTTP connections /HTTP URI/HTTP Host/ SSL Renegotiating/DNS query /DNS domain ……
- 60+Traffic models
  - TCP SYN pps/UDP packet bps/DNS pps/HTTP get QPS/SIP pps/ICMP pps/TCP FIN pps/TCP ACK pps……

Fingerprint and Reputation Recognize “Black” or “White”

- Dynamic fingerprint learning
  - Over 20,000 dynamic fingerprint
  - 7*24 real-time updates
- Static fingerprints
  - Popular mobile terminal zombie tool

- Global reputation of Botnet hosts
  - 5M IP address, One day upgrade
- Local location reputation
  - rapid response for abnormal traffic
- Session reputation
  - >10M sessions to ensure customers use

Accurate and All-rounded

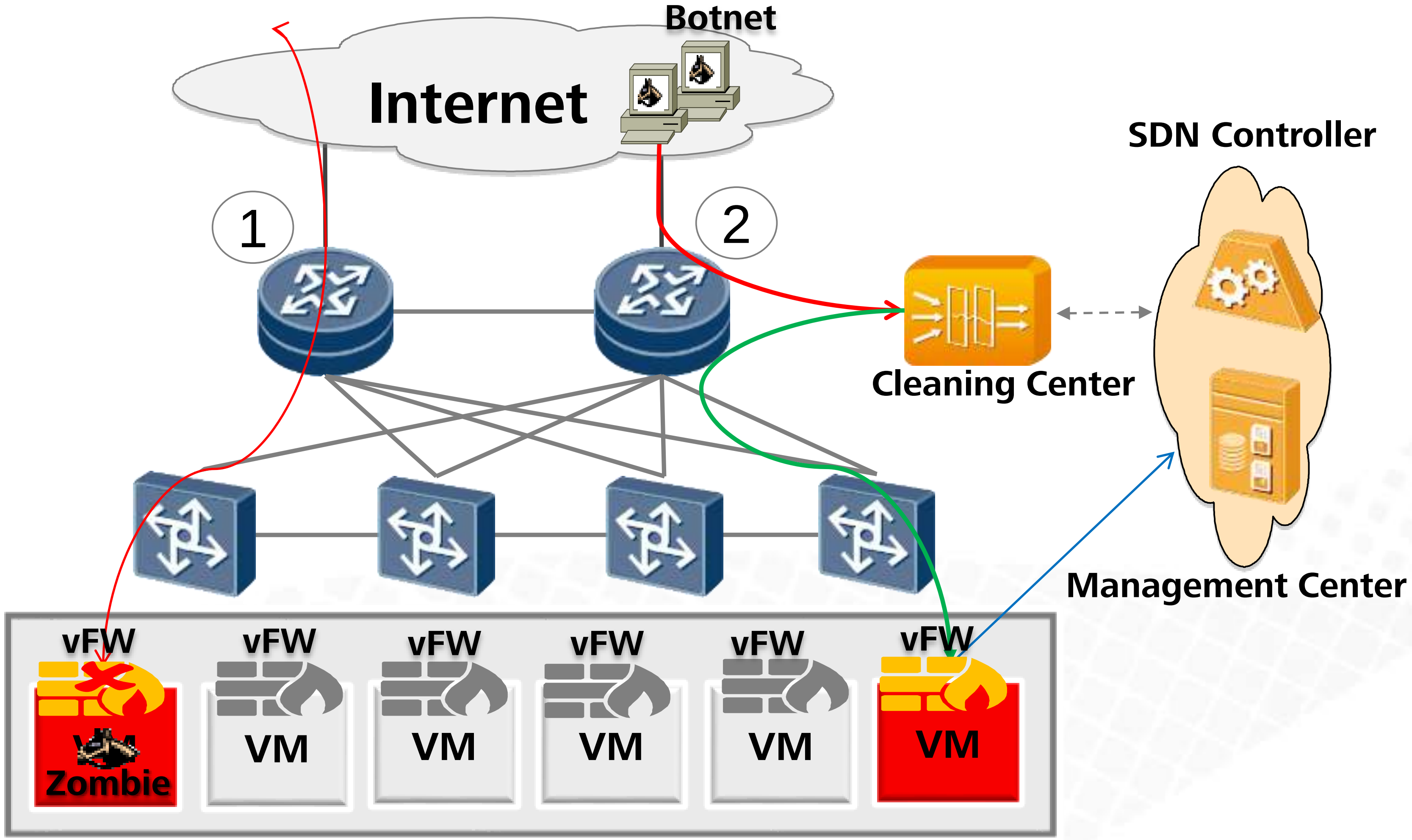


Defense Against More Than 100 Types of IPv4 and IPv6 Attacks

- Ability to defend against 30% more attacks than like products in the industry
- Unique ability to defend against SSL DDoS attacks
- Global first error-free attack identification solution
- Industry-leading IPv6 attack defense capabilities

- Capability to collect more than 20,000 GB traffic samples
- Seven-layer filtering and credit analysis
- Intelligent IPv4/IPv6 dual stack
- Intelligent redirection

On Premise Cloud DC DDoS mitigation



□ vFW functions

➢Detects & blocks botnet control channels to prevents outbound abnormal traffic from DC servers infected zombie.

➢Filters slow attacks.

➢Notifies cleaning center to divert traffic based SDN.

□ Cleaning Center

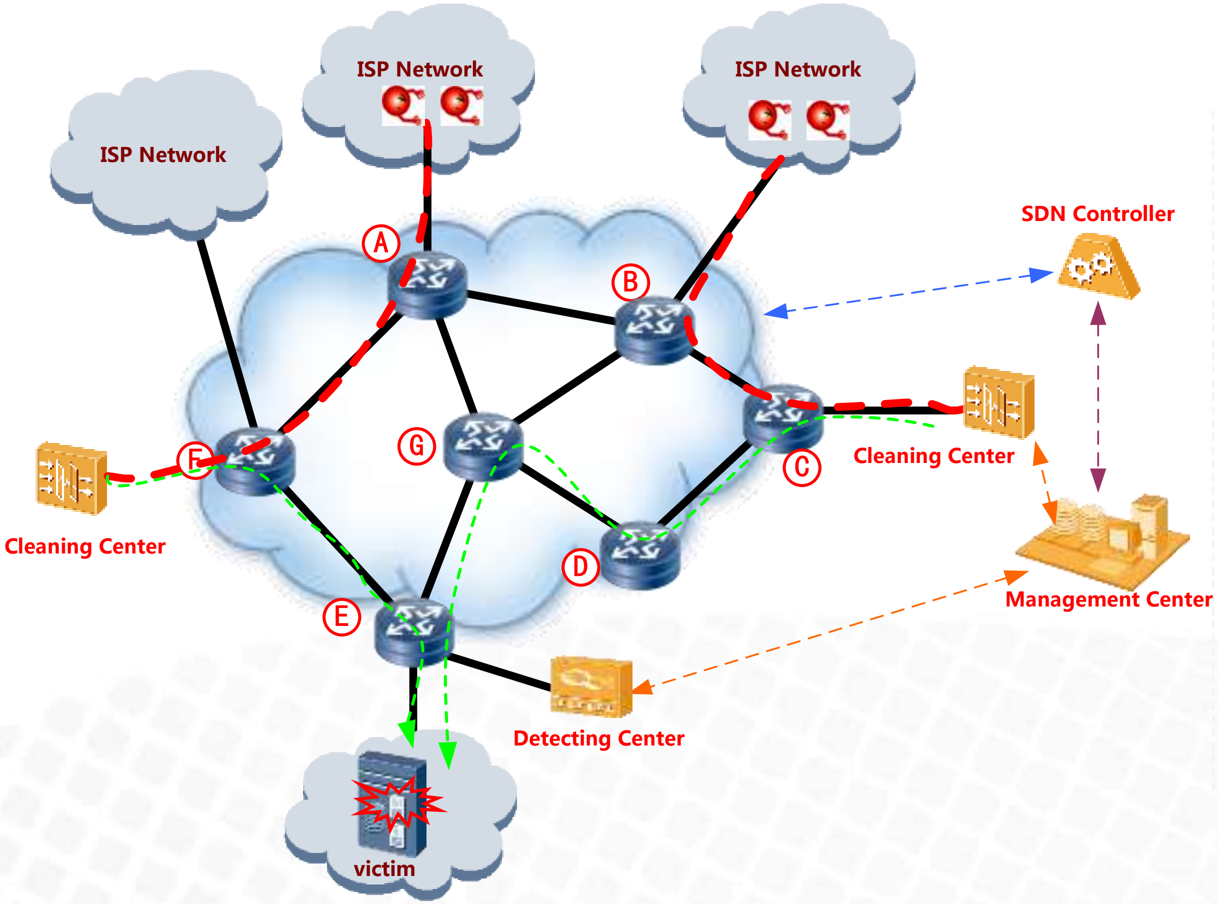
➢Deployed on the board of DC.

➢Diverts inbound traffic and filters DDoS traffic, then injects normal traffic.

□ Highlight

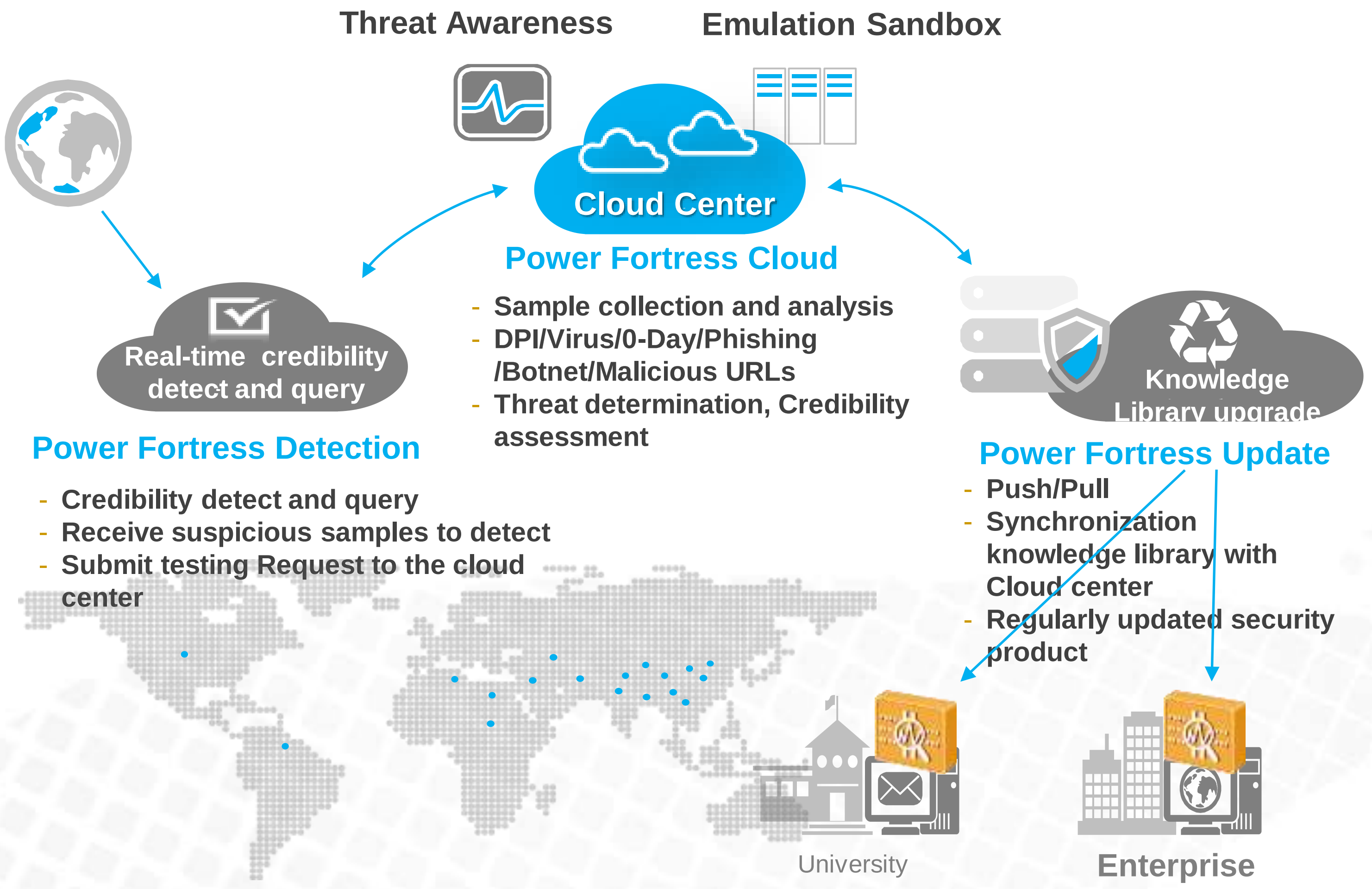
➢Active bidirectional protection for cloud DC based on SDN.

SDN-based Cloud Mitigation



1. **Based SDN to trace source routes where DDoS traffic from.**
2. **Do intelligent diversion-traffic based on usable defense bandwidth of every cleaning device and the peak attack bandwidth.**

Unknown Threat Protection on the Cloud



Threat Awareness

Emulation Sandbox

Cloud Center

Power Fortress Cloud

- Sample collection and analysis
- DPI/Virus/0-Day/Phishing /Botnet/Malicious URLs
- Threat determination, Credibility assessment

Real-time credibility detect and query

Power Fortress Detection

- Credibility detect and query
- Receive suspicious samples to detect
- Submit testing Request to the cloud center

Knowledge Library upgrade

Power Fortress Update

- Push/Pull
- Synchronization knowledge library with Cloud center
- Regularly updated security product

University

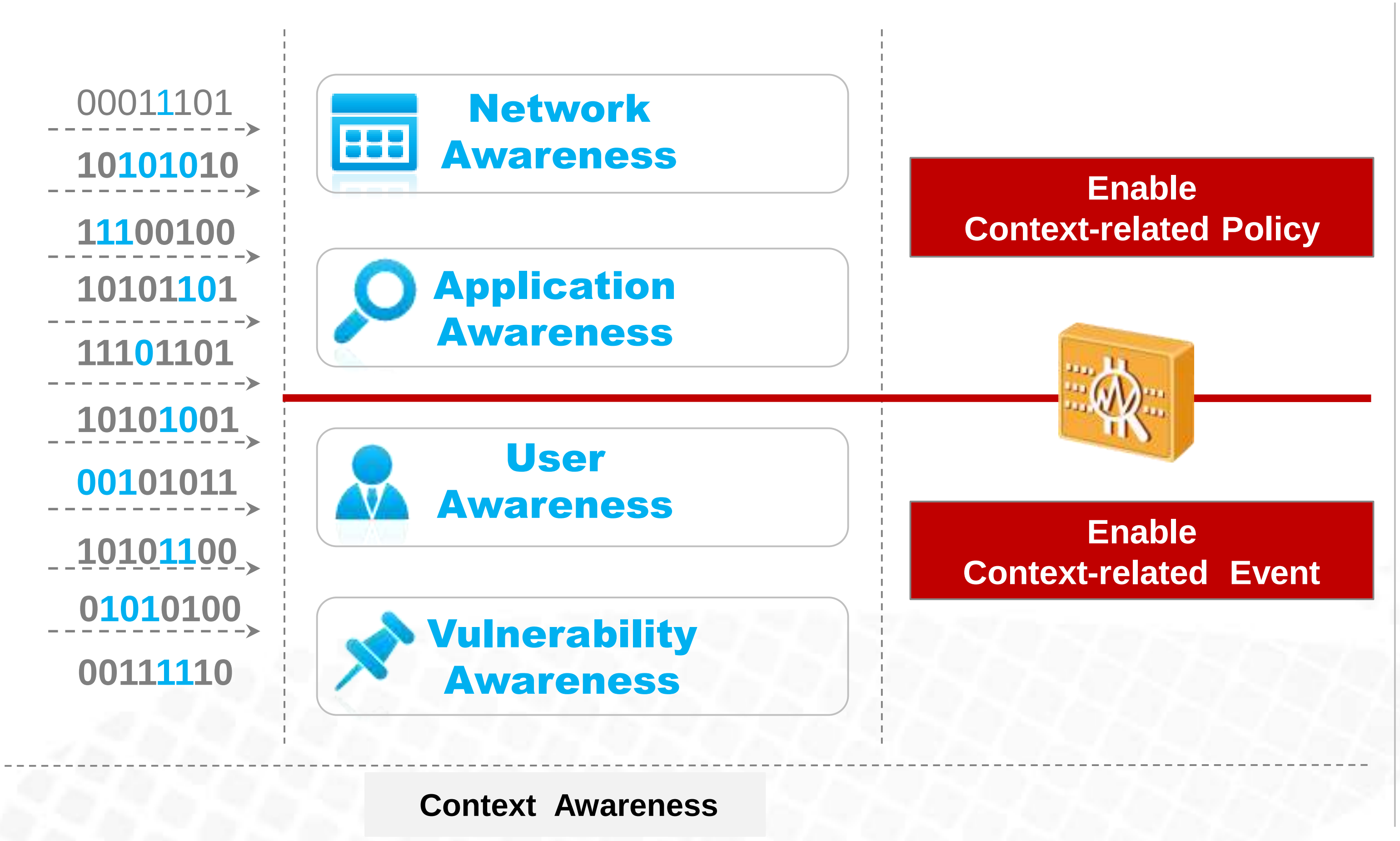
Enterprise

Rapidly responds to unknown threats

1、The high-performance cloud computing in cloud center ensures real-time and high-performance security response.

2、Supports cloud analysis of unknown threats, dynamic defense, and global synchronization of the threat signature library.

Context Awareness Using NGE Engine



00011101

10101010

11100100

10101101

11101101

10101001

00101011

10101100

01010100

00111110

Network Awareness

Application Awareness

User Awareness

Vulnerability Awareness

Enable Context-related Policy

Enable Context-related Event

Context Awareness

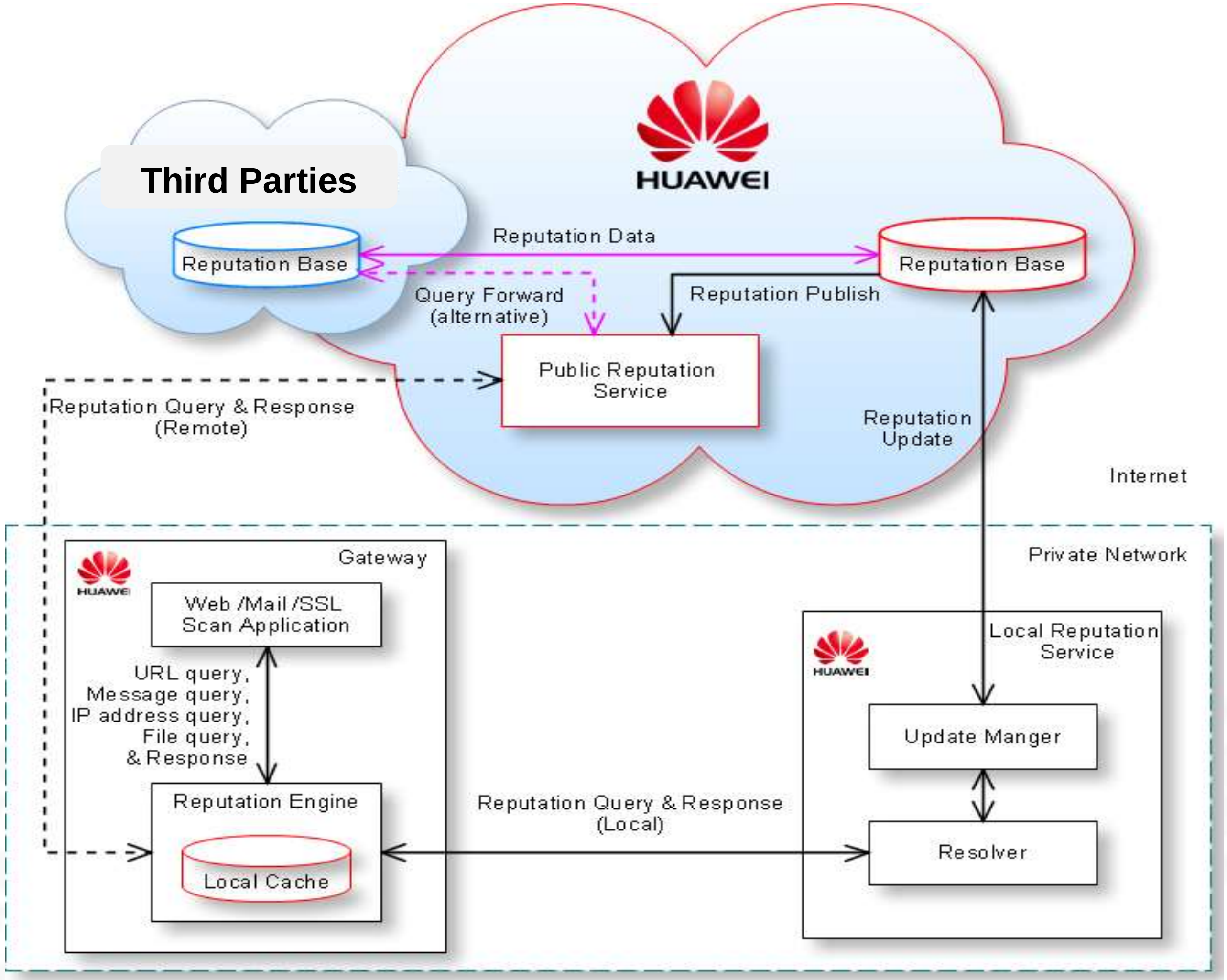
Provides Context-oriented Policy

1、Reduce unnecessary rule matching and improve performance

2、Enable precise policies and rules for vulnerabilities and improve performance

3、Reduce the number of alarm events, improve the efficiency of operation and maintenance

Reputation Base Helps Detection and Defense



Support Reputation System

1、Email / IP Reputation

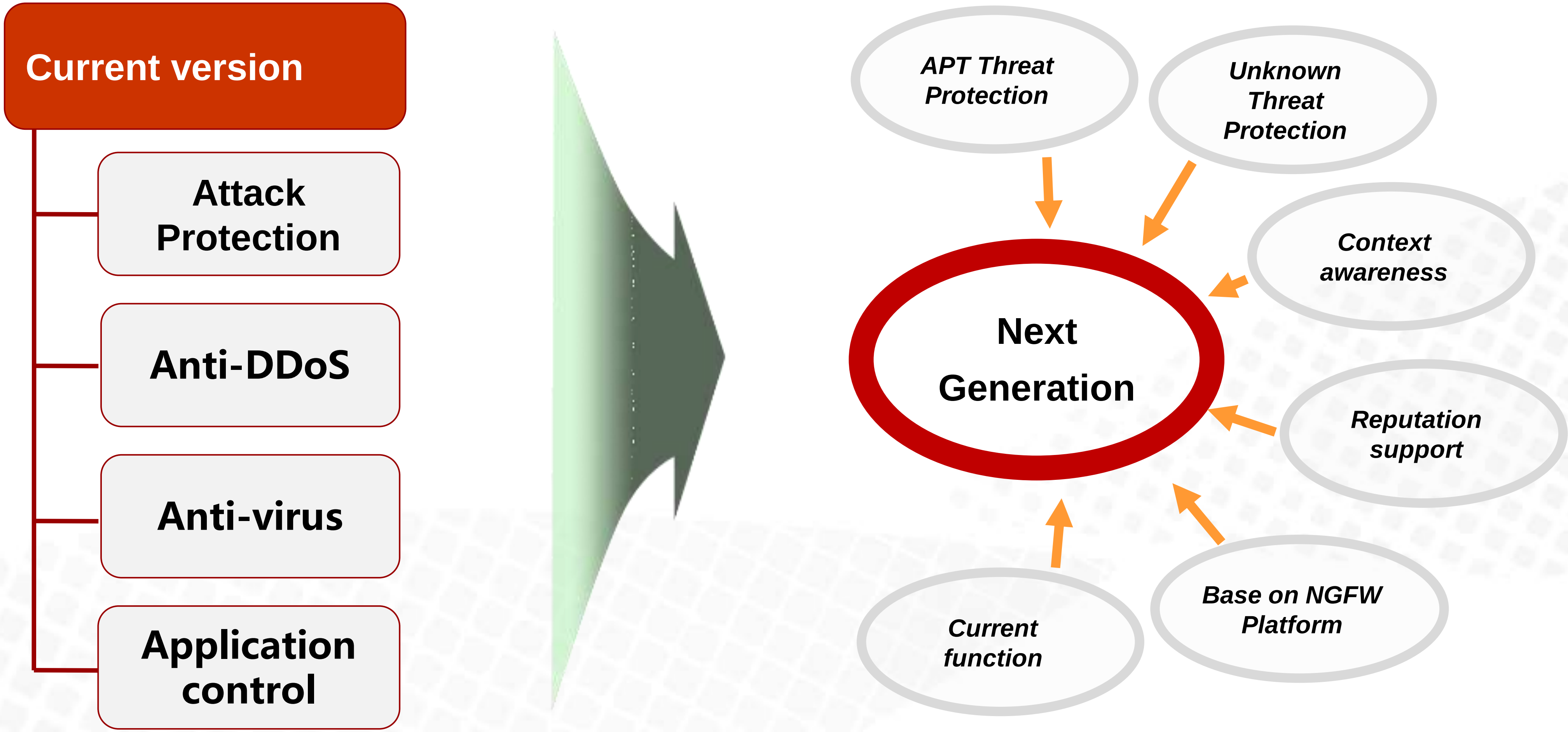
2、File / Web / IP Reputation

3、update the huawei reputation system According to the third partners

4、Processing security products reputation queries, forwarded to the third reputation system partners

6、 Local reputation data cache management, reduce and delay time requirements

Future Strategy



Thank you

www.huawei.com

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.