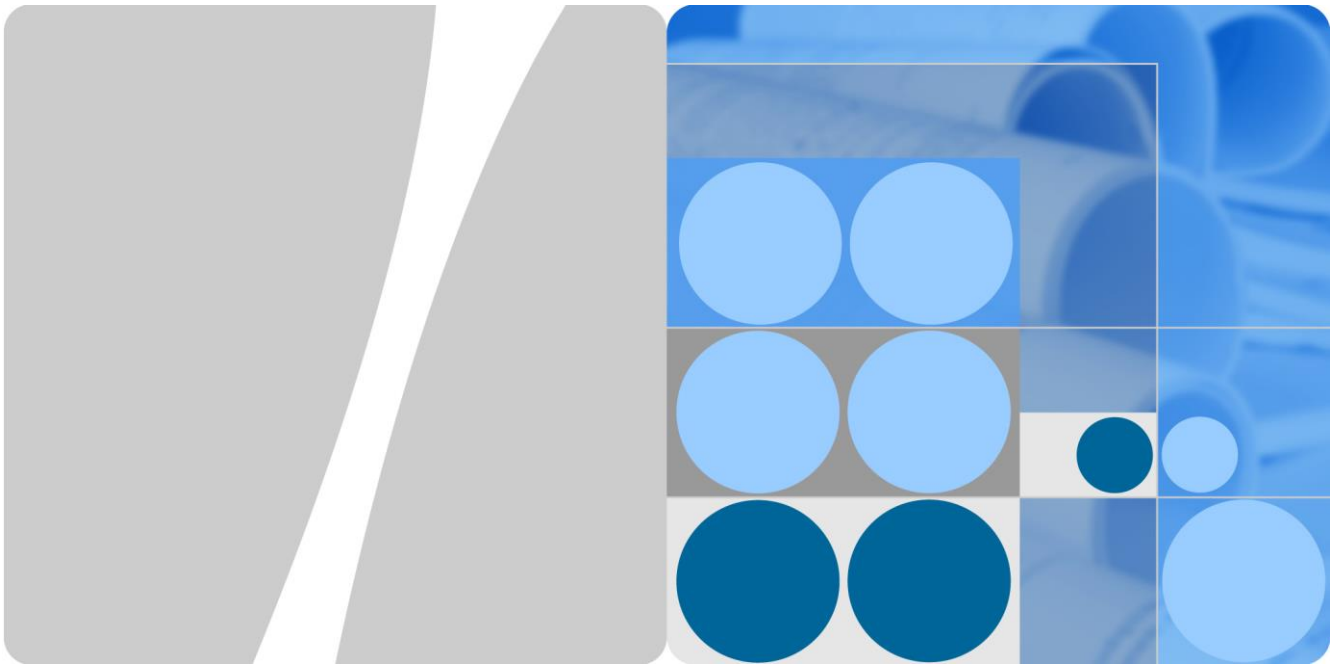


HUAWEI USG6000 Series Next-Generation Firewall

NG_Firewall Hardware Platform Technical White Paper

Issue V1.1

Date 2014-03-13

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

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

Email: support@huawei.com

Contents

1 Technical Background 5

1.1 x86 Architecture 5

1.2 NP Architecture 6

1.3 ASIC/FPGA Architecture 6

1.4 Multi-Core SOC Architecture 7

1.5 Summary 7

2 NG_Firewall Hardware Platform of Huawei NGFW 8

2.2 Multi-core MIPS CPU 8

2.3 Hardware Co-processor Acceleration 10

2.4 High-speed Switch Fabric 10

2.5 Storage Module 11

2.6 Scalability 11

2.7 High Reliability 11

2.8 Energy-Saving and Eco-friendly Design 12

HUAWEI Secospace USG6000 Series

NG_Firewall Hardware Platform Technical White Paper

Keywords: NGFW, NP, NG_Firewall, ASIC

Abstract: This document describes the application background of Huawei Next-Generation Firewalls (NGFWs), security requirements, and hardware structure advantages.

List of acronym and abbreviations:

Acronym and Abbreviation	Full Spelling
NGFW	Next-Generation Firewall
NG_Firewall	Next Generation Security
NP	Network Processor
ASIC	Application-Specific Integrated Circuit
FPGA	Field Programmable Gate Array
UTM	Unified Threat Management
SOC	System on Chip
PWM	Pulse-Width Modulation

1 Technical Background

With the rapid development of IT technologies such as Web2.0 and mobile Internet, networks are changing people's lives, have high requirements on security products, and bring about great challenges. In particular, application-layer security detection and control require a high-performance hardware platform. The I/O capability and CPU performance of traditional hardware platforms cannot meet the requirement. Under this background, the Next Generation Security (NG_Firewall) hardware platform comes into being. The multi-core CPU architecture processes data flows concurrently and provides powerful application-layer processing capabilities such as in-depth detection and refined control. The multi-core CPU architecture also provides independent coprocessors for hardware acceleration, compression and decompression, and pattern matching. The NG_Firewall hardware platform with high performance, concurrent processing, and built-in co-processors meets increasing security requirements.

To deal with new security threats of network applications, you must choose an appropriate hardware platform. The hardware platform of security products may have the x86, Network Processor (NP), Application-Specific Integrated Circuit (ASIC), or multi-core System on Chip (SOC) architecture.

1.1 x86 Architecture

The x86 architecture, also called general CPU architecture, uses an industrial computer or server as the hardware platform and an x86 CPU as the core of the entire system to ensure high flexibility and scalability. In the x86 architecture, product functionality is implemented by software. The x86 architecture enables the rapid product launch, updates with the mainstream IT platform, and provides a software platform with high transplantability and compatibility, to meet common requirements on the performance and reliability of the hardware platform.

The x86 architecture has the following disadvantages:

- The architecture development is limited by the CPU structure. The x86 architecture, working as a common computing platform, has multiple levels and is hard to optimize, especially in processing small packets. The process scheduling and interruption handling of the x86 architecture significantly reduce the overall throughput.
- The x86 architecture does not provide any dedicated optimization or acceleration for processing network packets, even if the x86 architecture has high computing capabilities. The CPU performs all processing operations, which waste memory resources.
- The x86 architecture uses a common software architecture that is compatible with open-source or third-party software and can be used in all

fields, including entertainment, multimedia, and office. However, the software architecture does not provide dedicated optimization for processing network packets, its performance and memory usage are not the best, and many irrelevant or auxiliary applications waste memory resources.

1.2 NP Architecture

NP is a processor designed to process network traffic for network devices. The NP system and its instruction set have optimized the packet filtering and forwarding algorithms and operations. The NP architecture enables programmable customization development, efficient packet processing, and rapid and concurrent processing of network traffic.

The NP architecture has the following disadvantages:

- Application development and functionality expansion are limited by the NP microcode space. Therefore, NP technology–based security products are inflexible and dependent on the software environment. In the scenario where traffic is heavy, multiple security policies are applied, and application-layer traffic is complex, the NP architecture cannot meet requirements.
- The NP chip, designed for routing devices, does not provide any acceleration for security devices. Therefore, security products of the NP architecture provide only common firewall functions, but not advanced security features such as intrusion prevention and virus filtering.
- The NP provides dedicated microcode as a development language. Vendors may provide different microcode instructions and syntax rules. The hardware platform of the NP architecture has low transplantability and compatibility and increases software development costs.

1.3 ASIC/FPGA Architecture

The ASIC/Field Programmable Gate Array (FPGA) architecture uses a dedicated ASIC chip or logic FPGA component to accelerate hardware. Hardware circuits have been designed for a specific purpose with improved function modules and fixed to the ASIC/FPGA chip for massive production. The ASIC/FPGA architecture has high performance, and its forwarding performance is irrelevant to the number of security policies.

The ASIC/FPGA architecture has the following disadvantages:

- This architecture is poor in flexibility and scalability and has high development costs and long development cycle. The ASIC/FPGA architecture is fixed and cannot defend against various security threats due to its long development cycle. Therefore, the ASIC/FPGA architecture applies to firewalls and VPN products that has fixed functions.
- The new connection rate is low. The basic product model of this architecture is ASIC/FPGA+x86 CPU. The x86 CPU manages the system, configures policies, sets up connections, and synchronizes security policies and connection information to the ASIC/FPGA chip. The ASIC/FPGA chip then implements status-based policy control and packet

filtering. The status information must be continuously synchronized between the ASIC/FPGA chip and the x86 CPU. Therefore, the performance bottleneck of the ASIC/FPGA architecture is the low new connection rate.

- Basic forwarding performance does not match the security processing performance. Although the ASIC/FPGA chip has high forwarding performance, this advantage disappears once application-layer security functions are enabled on a security product. The CPU processes all security services, and performance is dramatically degraded.
- Similar to the NP, the ASIC/FPGA chip provides a dedicated microcode or logic development language as the development language. Vendors may provide different instructions and syntax rules. The hardware platform of the NP architecture has low transplantability and compatibility and increases software development costs.

1.4 Multi-Core SOC Architecture

The multi-core SOC architecture is the latest high-performance solution for security products. Each multi-core processor supports concurrent processing of independent services. The multi-core architecture provides a high-performance hardware platform, a common programming language for design and development, and flexible service expansion. In addition, the design of a multi-core processor has taken users' application requirements into consideration. The multi-core processor has integrated hardware co-processors that provide hardware encryption and decryption, compression and decompression, and regular matching functions and Layer 2-to-Layer 7 application accelerators for security products, such as the firewall, VPN, antivirus, and intrusion prevention products. Technically, the multi-core SOC architecture of security products is perfect, with high throughput, high-speed session establishment, hardware supporting advanced security features, and high flexibility and scalability.

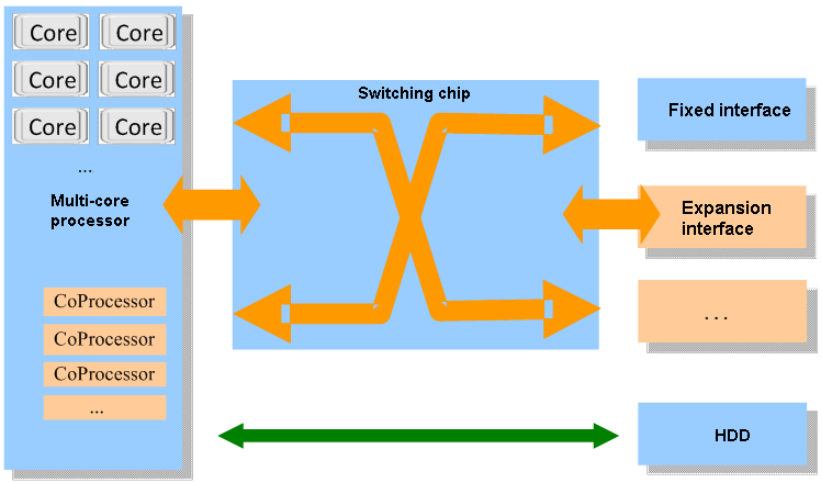
1.5 Summary

A hardware platform must meet requirements on functionality and performance. By analyzing characteristics of hardware architectures and comparing the hardware architectures in terms of flexibility and performance, you can choose the multi-core SOC architecture. Huawei USG6000 series uses the multi-core SOC architecture to meet new requirements for network security and development.

2 NG_Firewall Hardware Platform of Huawei NGFW

NG_Firewall hardware platform is a next-generation high-performance hardware platform developed by Huawei for security products. This platform, with a "Multi-core MIPS+Hardware co-processor acceleration+High-speed Switch Fabric" architecture, uses a high-speed bus to implement the communications between the multi-core CPU and the service processing and interface expansion modules. The redundancy design of the platform improves hardware reliability. In addition, the NG_Firewall hardware platform has enhanced performance and functionality and expands storage to meet requirements on the local storage of security device logs.

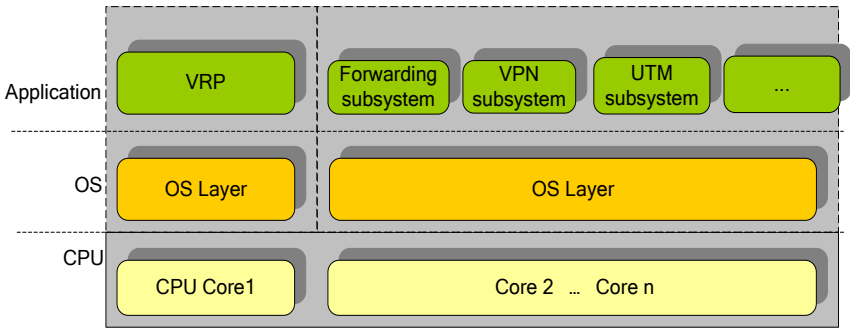
Figure 2-1 Huawei NG_Firewall hardware architecture



2.2 Multi-core MIPS CPU

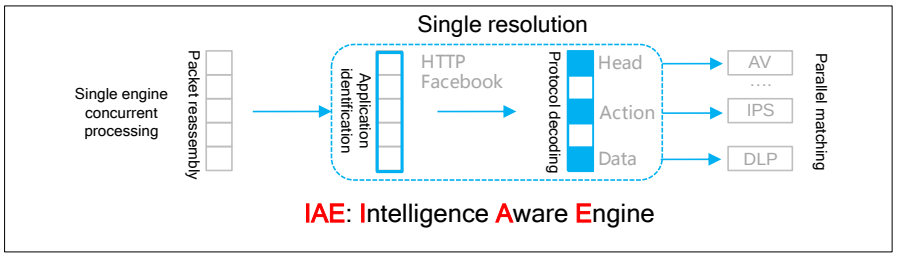
Huawei NG_Firewall hardware platform uses a 64-bit multi-core MIPS architecture that has high performance and is based on the regularly encoded instruction set of a fixed length. The MIPS architecture provides streamlined instruction sets, hierarchical design of the instruction and high-speed data cache, concurrent multi-level flow lines, and dedicated high-speed interfaces and DMA capabilities for traffic throughput, and incorporates Huawei carrier-class embedded real-time operating system to ensure the high performance of the NGFW platform.

Figure 2-2 Multi-core MIPS architecture



The NG_Firewall hardware platform can be expanded with a CPU processing unit to implement "1+1" CPU capabilities. Each CPU is a multi-core MIPS processor. Such expansion doubles hardware processing capabilities.

Figure 2-3 Huawei NG_Firewall software platform



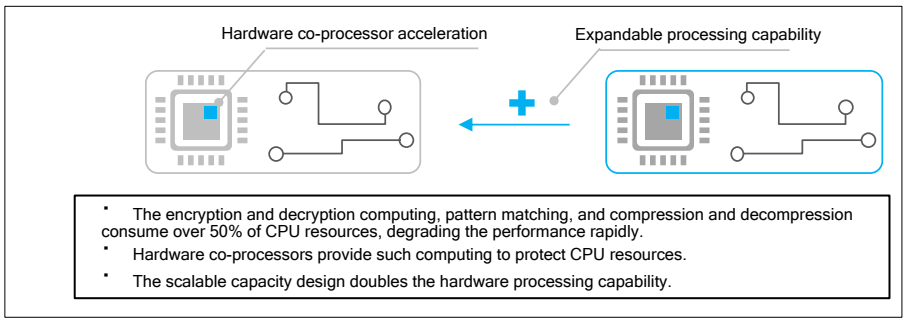
The architecture of the Intelligence Aware Engine (IAE) in the USG6000 series is different from that of traditional threat detection engines. The attack detection engine of a traditional firewall matches each packet with the attack signature database. Attacks can easily evade such detection. The IAE reassembles packets based on sessions, parses protocols, and matches signatures for a more accurate detection of protocol-specific attacks. During attack detection, the IAE parses each packet only once over the multi-core CPU architecture and can perform multiple security inspection tasks at the same time. The hardware acceleration module identifies applications and matches signatures at a high speed. If all signatures for an attack are met, the IAE takes an appropriate action according to the configured policy. If the signatures are not met, the IAE automatically adjusts the tracing status to ensure the high-speed forwarding of secure traffic. This architecture ensures the minimum compromise of the overall performance with multiple security services enabled.

The IAE uses a multi-core hardware platform for concurrent service processing. In addition, the IAE uses the hardware acceleration technology for application identification and signature matching, greatly improving attack detection efficiency.

2.3 Hardware Co-processor Acceleration

Huawei NG_Firewall hardware platform has integrated the IPSec and SSL encryption and decryption, compression and decompression, pattern matching, and hard disk RAID hardware co-processors. These co-processors processes the services that may degrade CPU performance, such as encryption and decryption, compression and decompression, and pattern matching to reduce the consumption of CPU resources.

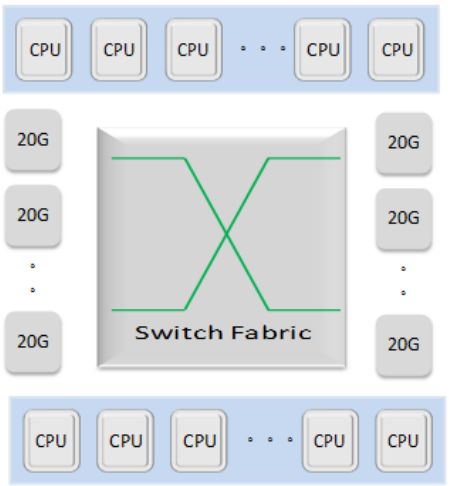
Figure 2-4 Huawei NG_Firewall co-processor and CPU expansion capabilities



2.4 High-speed Switch Fabric

Huawei NG_Firewall hardware platform uses a 480 Gbit/s switching chip for the communications among the multi-core CPU, service processing module, and interface expansion module. Its high-speed switching bus provides sufficient bandwidths for all modules and ensures the smooth switching.

Figure 2-5 Huawei NG_Firewall software platform



2.5 Storage Module

Huawei NG_Firewall hardware platform supports the 300 GB high-speed SAS hard disk to store real-time logs and reports.

Two hard disks work in RAID1 mode to back up user data.

The hot swap design of hard disks enables capacity expansion and upgrade.

2.6 Scalability

The following scalability features enable customers to configure only required modules in the initial phase and expand capacities when necessary to maximize customer investments.

1. The USG6000 series uses the flexible and scalable architecture to increase security performance by adding more SPUs for different application scenarios. The combination of the intelligent awareness engine and the elastic hardware structure enable the USG6000 series to deliver 10-Gigabit level threat prevention performance, meeting the security protection requirements of large enterprise data centers.
2. The NGFW supports multiple slots for high-density expansion interface cards and diversified interface cards that provide the GE electrical and optical ports and 10GE ports. You can flexibly improve hardware forwarding capabilities and device performance according to actual conditions.
3. Based on the virtual system function of the USG6000 series, you can divide a physical device into multiple virtual devices that are independent and locally isolated to implement system-level expansion and meet the requirements of device leasing and cloud computing.
4. Hard disks are optional. You can choose hard disks as required.

2.7 High Reliability

The high reliability features of Huawei NG_Firewall hardware platform are as follows:

1. Power supplies provide 1+1 redundancy, and hard disks work in RAID1 mode. When one power supply or hard disk is faulty, the other one takes over all the services. The hardware design ensures service continuity.
2. Fault detection: The system monitors the working statuses of the integrated device and key components on SPUs and LPUs and generates alarms (such as the fan failure, power failure, and over temperature alarms) when an anomaly is detected.
3. Hot standby: The comprehensive hot standby mechanism ensures high availability. When an NGFW is faulty, services are smoothly switched to the other NGFW without affecting user services. Hot standby implements real-time data backup for key configurations and connection entries to ensure that firewall performance is not affected by the switchover. You can also manually back up data in batches.

4. Hardware bypass: The built-in bypass card is supported. If the NGFW is faulty, traffic is bypassed to ensure service continuity.

2.8 Energy-Saving and Eco-friendly Design

Dynamic power consumption management: The NGFW has an architecture that uses low power consumption components and high efficiency power supplies to reduce power consumption. In addition, system software dynamically controls power consumption based on the device operating, function enabling, port connection, and temperature statuses, for example, dynamically closing idle ports and functional units and adjusting fan speeds.

Intelligent heat dissipation: The NGFW uses PWM speed adjustment fans and reduces power consumption by 70% using the refined speed adjustment and area-specific heat dissipation technologies. The technologies also reduce noises.

Eco-friendly manufacturing process: The design and production of the NGFW strictly comply with RoHS and WEEE laws and regulations, without any toxic substances. The design allows product disassembly and has high recyclability. Recyclable materials are widely used, and the product recycle ratio is above 90%. The packing design complies with the EU requirements 94/62/EC. Eco-friendly and recyclable materials are used, and the types, quantity, and weight of required materials are reduced.

