

Hillstone Security Platform

Next-generation Security Appliance Infrastructure

1. Introduction

With the fast growing of multi-media applications and more internal/external threats, business has to face the difficulties of meeting the high bandwidth demand while still being able to protect the network. The customer also is asking for a higher level of security as seen by the emergence of different application level security products such as QoS, IDP, network AV, Anti Spam, Content Filtering etc.

The current security devices are not built to handle these changes since they do not have enough CPU power to process data at gigabit speed, while doing all the security inspection at the same time.

Hillstone Networks innovative solution integrates leading edge hardware and software technology, and creates a brand new network security platform that address these problems we are facing today.

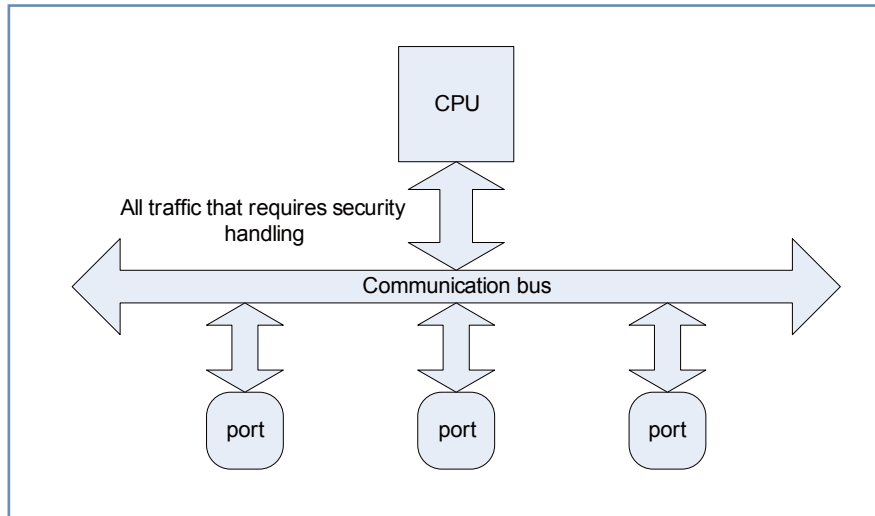
2. Evolution of Firewall Architecture

In 1995, Checkpoint introduced the first generation firewall product which was software based. It was a stateful inspection firewall which was a technology breakthrough at the time.

It became apparent very soon that the software solution had a performance variance which was hard to control and was not suitable for networks with that needs to provide an assurance of throughput and latency. In 1996-1997, out came the second generation firewall which was based on PC architecture and off the shelf or proprietary OS.

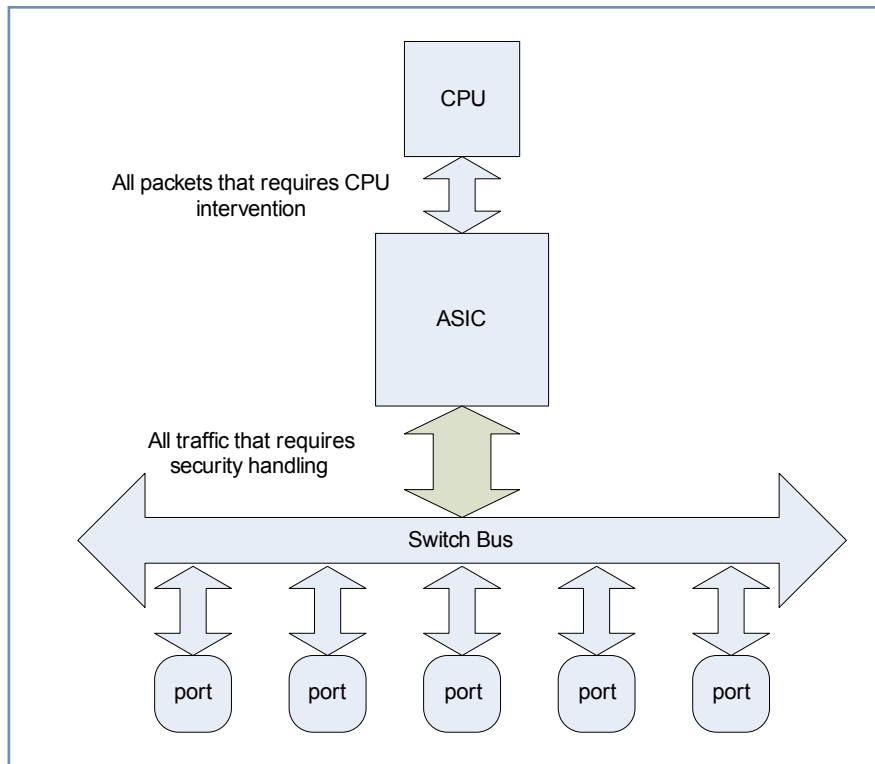
In 1997, Netscreen pioneered ASIC based firewall. The customized ASIC technology speeded up the security rule match and flow lookup by tens of times over software solutions. Netscreen firewall was the first that reached gigabit speed and provided excellent performance at the time for network level security.

Figure 1 PC based Firewall Architecture ▶



Much has changed since that time. ASIC based firewall excels at traditional firewall handling such as NAT and fast flow search. But with integration of application level security features, the CPU is far from adequate to handle the workload. In the current generation of security devices, the performance will drop, in many cases an order of magnitude if application security features are turned on.

Figure 2 ASIC based Firewall Architecture ▶



In recent years, some companies have experimented with Network Process (NP) architecture for security appliance. NP, while better than ASIC in

terms of extensibility, still is insufficient in the changing security requirement today. NP architecture has gradually been phase out because of this lack of extensibility and maintainability.

The fast growing integration of networking features such as QoS, traffic optimization also requires a lot of CPU intervention which is not well supported by existing security products.

3. Next Generation Firewall Architecture

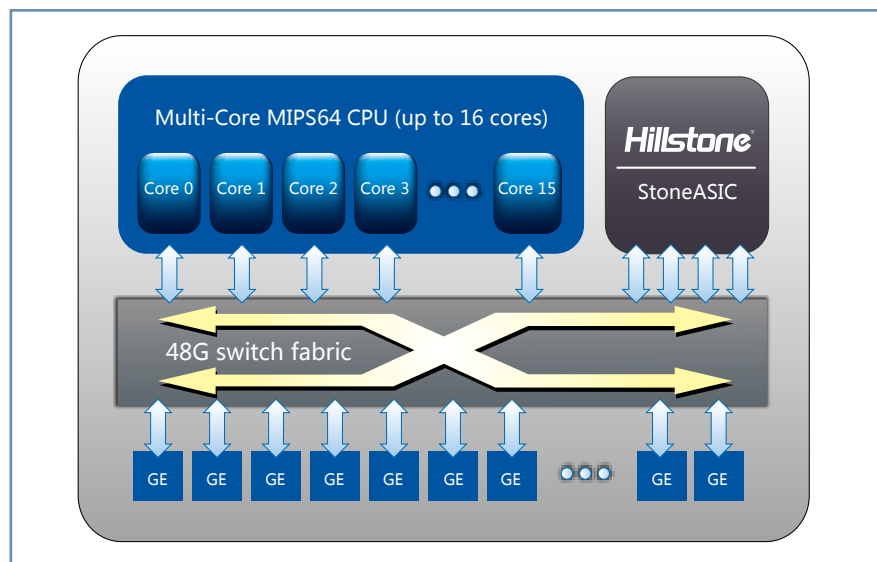
Hardware Platform

What ASIC can do is to perform simple and well defined operations at high speed. Proven technology that has been implemented in ASIC includes rule search, session match, packet switching/routing, QoS queue management etc. Many security features at network level can be implemented inside ASIC.

However, the shortcoming of ASIC is its inflexibility and low extensibility, compared to general purpose processors. While most of the application security logics today will require at least some level of CPU intervention, this is where multi-core CPU has its major advantage.

Hillstone security platform combines the best of ASIC solution to address network level security and uses multi-core CPU to speed up application level security. The hardware platform is complimented with high speed switch fabric to facilitate fast communication between the different components.

Figure 3 Hillstone Security Platform Hardware Architecture



- **StoneASIC:** Hillstone ASIC solution for network and security acceleration. The hardware combines state of the art network security processing and attack defense functions. When it comes to fast packet forwarding and defense against various type of flooding from botnet, StoneASIC offers unsurpassed performance. This frees up the general processor to handle other functions that requires CPU power. Also StoneASIC's predictable hardware pipeline provides high bandwidth throughput at guaranteed low latency for the data stream that otherwise do not need other security handling.

- **Multi-core CPU:** Hillstone utilizes high performance CPU optimized for network packet processing. These CPU have built in packet engineer to handle packet ordering and distribution among the processor cores. Multi-core CPU if used in a coordinated fashion delivers highly scalable performance in network and security processing. It also offers maximum flexibility to deal with the changing requirement that is facing the security devices today.

- **High speed switch fabric:** This switch fabric interconnects the multi-core CPU and StoneASIC with switch ports, guaranteeing fast, nonblocking communication between all parties. This avoids the shortcoming of a lot of security devices on the market that depend on slow buses for CPU communication.

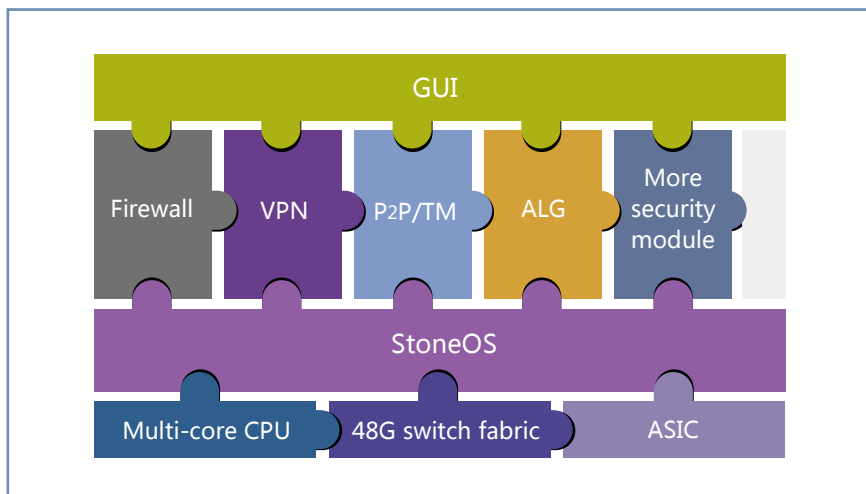
Hillstone platform also integrates hardware acceleration of IPSec, SSL, crypto, compression and DFA functions.

Software

StoneOS is Hillstone's customized 64-bit real time OS. It supports patent pending multi-core processor control technology and ASIC control technology. StoneOS offers highly scalable computing platform for both network and application security functions.

StoneOS consists of complete separate control plane and data plane. This separation offers a high level of control plane reliability and stability with unsurpassed data plane performance. StoneOS packet forwarding engine - Scalable Security Engine (SSE) is completely custom designed and security hardened. The security and network processing is highly parallelized to take full advantage of the multi-core and ASIC architecture, while at the same time, preserve the packet ordering as required by a reliable network.

Figure 4 StoneOS software architecture ▶



StoneOS SSE combines network packet classification, attack defense, security rule matching, QoS, switching and routing, VPN processing, all parallelized to run efficiently on the multi-core processor. Hillstone multi-core controlling technology allows each core to run independently while minimizing the coordination that is needed between the processor cores.

For data flows that require security processing that can not be handled by ASIC, the multi-core CPU and StoneOS takes over. The processing power of CPU cores working in parallel can now match the speed of ASIC packet processing rate. This removes CPU as the bottleneck as is the case for pure ASIC based system.

The Hillstone security platform is modular designed and can be extended to support addition of security and networking features either through embedded integration or external hardware modules.

4. Conclusion

The firewall is now moving beyond the ASIC based solution and going into a new era. The integration of security and networking market is demanding high computing power in the device. Armed with state of the art hardware and software technology, Hillstone networks security appliance is leading this trend. The Hillstone solution offers

- Superb attack defense capability for various DoS and DDoS attacks
- Session ramp up rate 5-10 times competition
- Superb performance in small, large, mix packet and VPN traffic
- Superb performance in application security handling
- Outstanding QoS performance, per IP traffic and session control for tens and thousands of users.