



Hillstone Multi-core Plus[®] G2 Security Architecture

1. Introduction

With the fast growing of internet applications and more internal/external threats, business have to face the difficulties of meeting the high bandwidth demand while still be able to protect the network and business applications. 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 change 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 Multi-core Plus[®] G2 architecture integrates leading edge hardware and software technology, created a brand new network security platform that address these problems we are facing today.

2. Requirements for Security Product

Here are trends in evolution of applications, network threats:

Network applications are evolving: In one aspect, number and types of network applications are increasing. This includes IM (instant messaging), P2P, online video, online games and SNS etc. On the other hand, behavior of these applications is also changing. To facilitate transport, or avoid detection and blocking, many applications are build on HTTP, using random TCP/UDP ports, and using SSL to hide content. Facing these applications, traditional way of identifying application based on ports is no longer valid, and it would be impossible to manage the network. Network visibility is the problem that new generation of security appliance must solve.

Network bandwidth is increasing rapidly: Another trend that is becoming apparent is the consolidation of data. An enterprise will have many servers and these servers will have access request from headquarter, branch offices and even outside of the company.

Hillstone Multi-core Plus[®] G2 Security Architecture

A datacenter may have thousands of servers. Network bandwidth is reaching 10Gbps even 100Gbps. The increasing bandwidth put higher requirement for security devices in terms of performance, capacity and reliability.

Security functionalities are increasing: UTM (unified threat management) solution, is gradually replacing solution that using single function devices. Using unified engine for security processing is the trend in new generation of security gateways. Security is also evolving to include a wider range of functions, from UTM functions that mainly targeting outside threats, to intranet management, such as QoS, network behavior control. With visibility, manageability, auditing all on the same platform, how to deal with all the functional modules and guarantee usability of the system is the major problem facing security appliances.

Return on investment (ROI) of security solution: A usable UTM solution can at one level protect user' s investment. At the same time, with ever changing application and traffic types and new security requirements, it becomes vital to protect the customer' s investment for a period of time, even when new security functions emerge.

These trends put forward new requirements to today' s network security products:

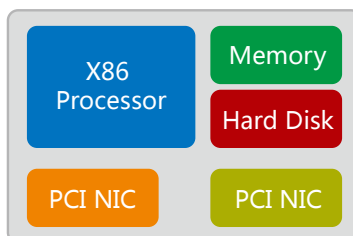
- To deal with increasing bandwidth and application requirements, and manageability requirement, new generation of security architecture need to support high performance and capacity.
- Fine grained network visibility is required. Without network visibility, there is no network security to speak of. The visibility will need to include: users, applications and behaviors.
- ROI for customer purchase. The new architecture need to be extensible in both hardware and software modules.

3. Evolution of Security Architecture

First Generation: x86 Based

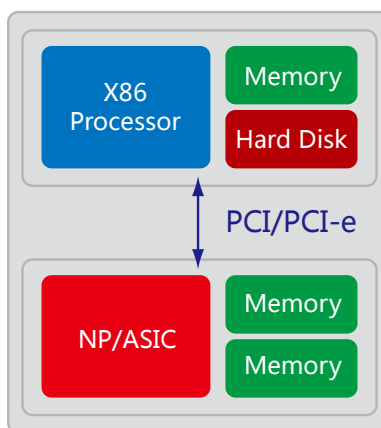
First generation of security devices are x86 based. The advantage is off the shelf hardware and cost of development is low. Its disadvantage is also very obvious. All packet processing is through the CPU. Since x86 architecture is not built for network packet transport. The bus quickly becomes the bottleneck. The solution has a performance variance that is hard to control and is not suitable for networks with that needs to provide an assurance of throughput and latency.

Hillstone Multi-core Plus[®] G2 Security Architecture



Second Generation: NP/ASIC Based

Compare with x86 architecture, purpose built NP/ASIC architecture improves the speed of rule matching and flow matching by an order of magnitude. But because of limitation on programmability, NP/ASIC can only perform simple, predefined operation at high speed. Network layer functionalities are realized in ASIC. But with integration of application security, these part of the processing still need to be done in the CPU. With CPU as performance bottleneck, the common symptom is drastic performance drop when application security is turned on. The disadvantage of ASIC is its inflexibility and low extensibility.



Next Generation Security Architecture

Hillstone Networks pioneered the next generation Multi-core Plus[®] architecture. This architecture deal with the increasing processing requirement put forth by application security in today' s security appliance. Multi-core Plus[®] utilizes multi-core processor to accelerate application security, uses ASIC to deal with network layer processing, and with high-speed switch fabric to facilitate data exchange. Multi-core Plus[®] G2 improves upon the previous generation by extending the capacity and functionality of the architecture. Storage and processing modules can be added. When multiple security functions are

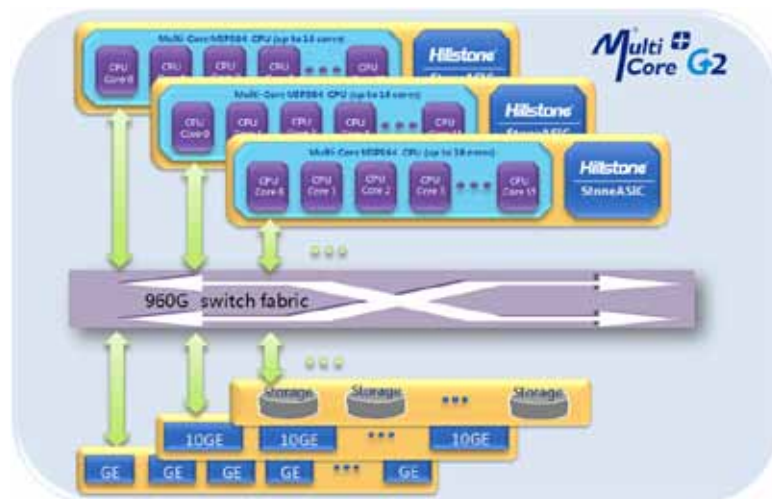
Hillstone Multi-core Plus[®] G2 Security Architecture

enabled the system can maintain high throughput and low latency. The characteristics of the new architecture is as follows:

- Multi-core processor, StoneASIC and high-speed switch fabric, providing high processing capability for network visibility, manageability, and auditing requirements.
- Extensible pluggable module protect customer' s investment
- Fully parallelized stream based scanning engine realizing high performance and capacity
- Cross inspection technology for network visibility

4. Hillstone Multi-core Plus[®] G2 Security Architecture

Hardware



- Multi-core CPU: Hillstone utilize high performance 64-bit CPU for parallel processing of application security. Each CPU has up to 16 cores and the system can be extended to include multiple CPUs. Hillstone platform also include hardware acceleration of IPSec, SSL, crypto, compression/decompression and DFA. These functionality guarantee high performance VPN and application processing. 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.

- Extensible Modules: Hillstone appliances has modular design, with pluggable modules that extends processing capability, provides storage functions and more interfaces. The modular design protects customer' s investment. With processing

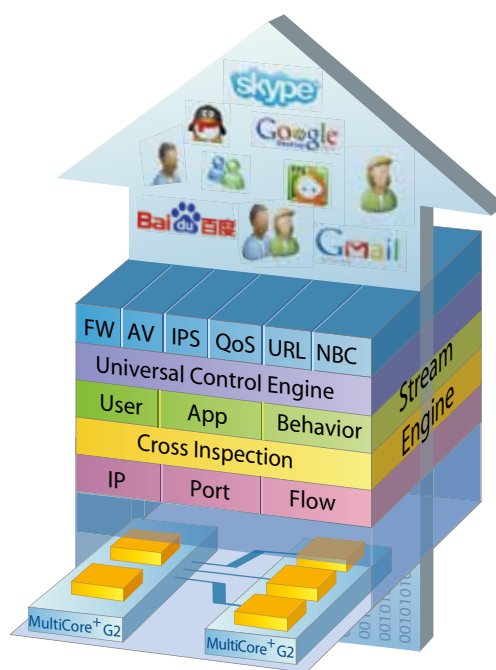
Hillstone Multi-core Plus[®] G2 Security Architecture

modules, application processing performance can be enhanced. Storage modules provide for permanent storage of logs and statistics. Interface modules provide flexible connectivity options to meet varying deployment scenarios.

- 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.

- High speed switch fabric: This switch fabric of up to 960Gbps interconnects multiple multi-core CPUs, StoneASIC with switch ports, guaranteeing fast, nonblocking communication between all parties.

Software



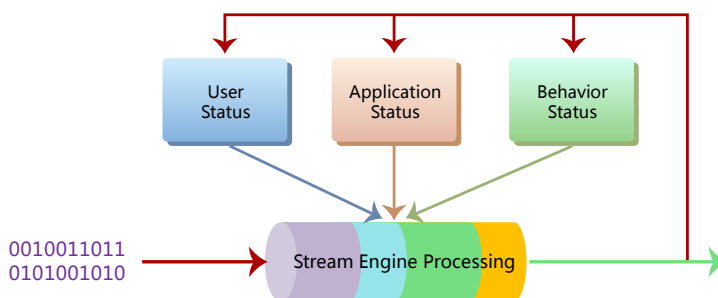
Operating system is the heart and soul of a security device. All hardware are controlled and managed by the operating system. Based on Multi-core Plus[®] G2 hardware, Hillstone proprietary StoneOS[®] is a 64 real time parallel operating system. This operating system uses fully parallelized scanning engine to provide for network visibility and unified security scanning, at high speed and with high reliability.

Hillstone Multi-core Plus® G2 Security Architecture

Cross Inspection

As stateful inspection firewall evolves, more and more attacks are targeting specific application. Deep inspection technology emerges. Deep inspection is a integration of IDS/IPS technology in the firewall. Through decoding and analyzing of traffic, capture events that violates protocol or intrusion attempts. With growing number of applications utilizing encryption, tunnel and other evasion techniques, inspection techniques need to evolve to deal with new types of attacks.

Hillstone Cross Inspection techniques not only does deep analysis of protocols, it also use decryption and decompression to open up data streams that is packed with techniques such as SSL and GZIP. Security filtering can be based on protocol or content. Work with AAA infrastructures to correlate IP address with users, inspection engine groupes user traffic into behavior and use it in application and behavior analysis. Cross inspection analyze user state, application state and behavior state to identify traffic and apply security policy accordingly. Cross inspection technology also provide a strong foundation for network visibility and user behavior control.



Stream Based Scanning

Traditional threat detection is file based. This is often the case for host based security solution. Many security gateway grandfathered this solution. With this method, the whole file need to be downloaded before scanning can be performed. The file is then sent out. There is long latency between the sender sending the file to recipient receiving the file. For a large file, user application may timeout. At the same time, the device buffers a large amount of data. This effectively limit the capacity of the device when dealing with large amount of files that needs to be scanned.

Hillstone Multi-core Plus® G2 Security Architecture

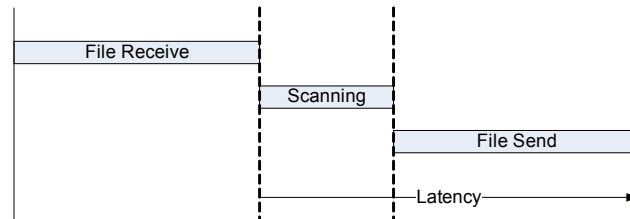


Figure 6: File based scanning

All of Hillstone security scanning is flow based. Security scanning engine scan each packet at arrival, if no threat is detected, the packet is sent immediately. This greatly reduces the latency and users experience a much better response time. In the meantime, since stream based scanning does not need to buffer a large amount of data, the capacity of the system is also greatly improved.

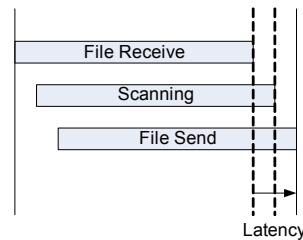
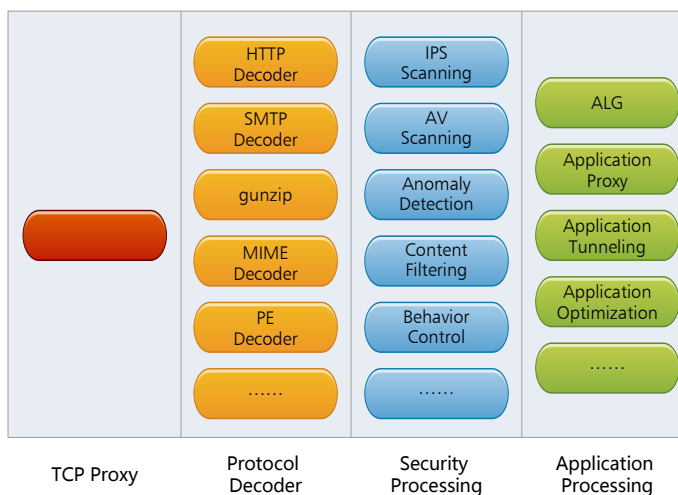


Figure 7: Stream based scanning

Stream based technology requires all processing steps of the system are stream based. A system may have a stream based TCP proxy, stream based protocol decoder, but a file based security scanning, the effect will be a file based system. The worst performing part in the processing pipeline determines the system performance. Hillstone uses stream engine technology at many levels, implements a fully parallel stream engine based data plane:

- TCP Proxy
- Decoder: include protocol decoder (e.g. HTTP, SMTP etc), content decoder (e.g. MIME, base64 etc), content decompressor (e.g. gunzip, unrar etc), file decoder (e.g. PE etc) and SSL decryption
- Security Processing: including protocol control, content control, AV scanning, IPS scanning, anomaly detection etc.
- Application Processing: including ALG, application proxy, application tunnel, application optimization etc.

Hillstone Multi-core Plus® G2 Security Architecture



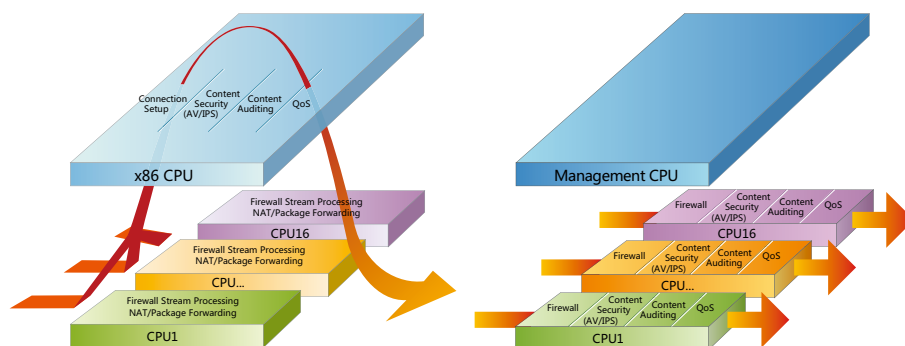
Fully Parallel Architecture

Based on Multi-core Plus® G2 hardware architecture, StoneOS® uses a fully parallel architecture to realize the full potential of the hardware. Hillstone's new generation of UTM devices can maintain high performance and low latency when multiple security functionalities are enabled.

In some multi-core platforms, multi-core processor merely replace the position of NP/ASIC. In these systems, multi-core processor provided better programmability of than NP/ASIC. But multi-core processor only performs network layer security. Application security and content security is still performed by main CPU. On many platforms, some firewall functionality such as session setup is still done on the main CPU.

In Hillstone StoneOS, all data plane processing are developed with multiple multi-core CPU in mind. This results in industry leading performance such as firewall session setup rate. In application processing, all stream engines are programmed for high parallelization, reducing data dependency to a minimum. Performance and capacity can scale nearly linearly with CPU cores. The fully parallel architecture fully realize the potential of the hardware and provided for high throughput and low latency even under the most demanding circumstances.

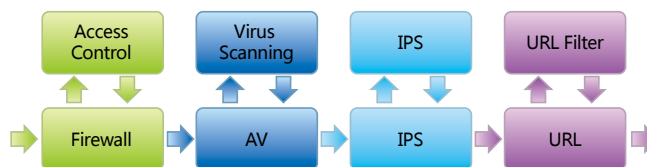
Hillstone Multi-core Plus[®] G2 Security Architecture



StoneOS[®] multi-core controlling technology reduces intercore dependency to a minimum and allows each core to run mostly independent.

Unified Processing

In traditional UTM equipments, traffic need to pass through several independent security engines, each with its own network engine, classification engine, matching engine and policy engine. The repetitive work is redundant and reduces the overall performance of the system



Hillstone StoneOS[®] use a unified processing engine. Data packet once enter a process pipeline, each state of the pipe is only performed once, this include network functions, application identification, protocol decode, protocol security, content decode, content security, user behavior analysis. The result of each stage of the pipeline is input into next stages that requires the information. This elimination of redundant processing reduces the processing latency and increases system capacity and throughput.

Independent Control and Data Plane

StoneOS[®] has independent control plane and data plane. This separation provide for the reliability of the control plane and superb performance of the data plane. Independent control plane means even when the system is experiencing high traffic or under attack, the system can still be managed and logs can be stored. Separate



Hillstone Multi-core Plus[®] G2 Security Architecture

data plane guarantees uninterrupted traffic and service during configuration change, delivering a high performance, high reliable network.

5. Conclusion

Today, we are seeing a new era in network security. The market demands a high performance appliance that can provide network visibility and application security, and protecting customer investment at the same time. Hillstone Multi-core Plus[®] G2 architecture is leading this trend.