



Hillstone UTM Plus

1. Introduction

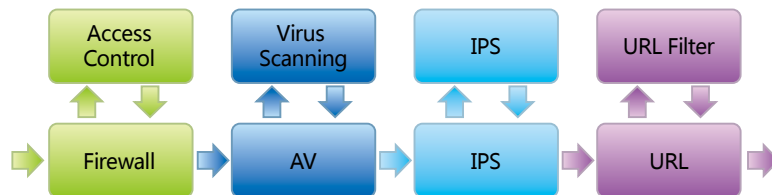
From Firewall to UTM

Earlier security devices mostly runs in-line. With the need to install different devices to protect against different attacks, the devices are connected serially and each device runs independently. Management is complicated, and it introduces many failure points. Many devices also means high capital investment and operating expenses. At the same time, network and application level processing are often duplicated among devices and information sharing is not possible.

From UTM to UTM Plus

The appearance of UTM (Unified Threat Management) seems to solve this problem. UTM consolidate all security processing onto one device. Theoretically, UTM solves the problem of single function devices such as firewall, anti-virus gateway, IPS etc. The security management can be centralized, capital investment and operating expenses are controlled and failure points are minimized. Does UTM solves all the problem?

- Traditional UTM simply collapse the security functionality of several devices. The performance of the system is drastically impacted and the system is unusable when all the security functions are turned on. The security functions are combined but they do not cooperate, resulting in waste of resources. The traditional UTM is becoming a concept.



- From users perspective, the need for security has evolved. Traditionally security has been mostly focused on defending intranet against outside attacks. But with the expanding use of the network in business operation, clogging of bandwidth by P2P



Hillstone UTM Plus

downloads, unrestricted internet surfing resulted in inappropriate or illegal activities, “security gate” , “data leakage” are becoming problems of equal importance. Security management for the whole network, not just attacks from outside, makes UTM solution insufficient in dealing with today’ s security problem.

What is UTM Plus

UTM Plus is built upon the Traditional UTM concept. With new generation of hardware architecture and software design, provide ample processing power for proper running of all functional modules. It can adapt to today’ s ever changing network applications and meet customer’ s security needs.

- From adapting to changing application landscape, UTM Plus solution must be able to identify and handle new kind of complex applications. After these applications are identified and visible, proper security engine can be applied for further processing.
- The protection UTM Plus offers will not only be attacks from the outside. Traffic management (QoS), network behavior control, together with IPS, AV will need to be organically combined in today’ s integrated products.
- From a usability point of view, after all security functionality are turned on, UTM Plus solution need to operate normally and meet customer’ s needs in terms of performance and manageability.

Moving from UTM to UTM Plus, the emphasis is on handling new network applications, making complex security management simpler and solving the performance bottleneck of a fully loaded system.

Hillstone UTM Plus Solution

Hillstone Networks UTM Plus solution consists of the following parts:

- New generation Multi-core Plus® G2 architecture
- Role based network services (RBNS)
- Strong DDoS prevention capability
- Flexible, high performance QoS functionality (role based and application based)
- High performance, fine grained session control capability
- High capacity IPSec VPN (up to 30,000 tunnels)
- High performance, high capacity 3rd generation SSL VPN
- Fast and Simple large scale VPN deployment (PnPVPN)
- High performance application level security
- High performance, high capacity Anti-Virus solution

Hillstone UTM Plus

- High performance, high capacity, accurate IPS solution
- URL Filtering solution based on more than 20 million URL databases.
- High reliability and stability, ease of use and maintenance, low TCO

2. Hillstone UTM Plus Characteristics

Fully Parallel Security Architecture (Multi-core Plus® G2)

StoneOS is Hillstone Networks proprietary 64 bit real time operating system. It is highly optimized for parallel processing. StoneOS patent pending multi-CPU fully parallel architecture is different from traditional multi-core processor or NP/ASIC systems. StoneOS processes network layer security and application layer security in fully parallel fashion.

SG-6000 compared with other multi-core or NP/ASIC solution of comparable hardware have an up to 5 times performance advantage. This provides the processing power needed to integrate security functionalities.

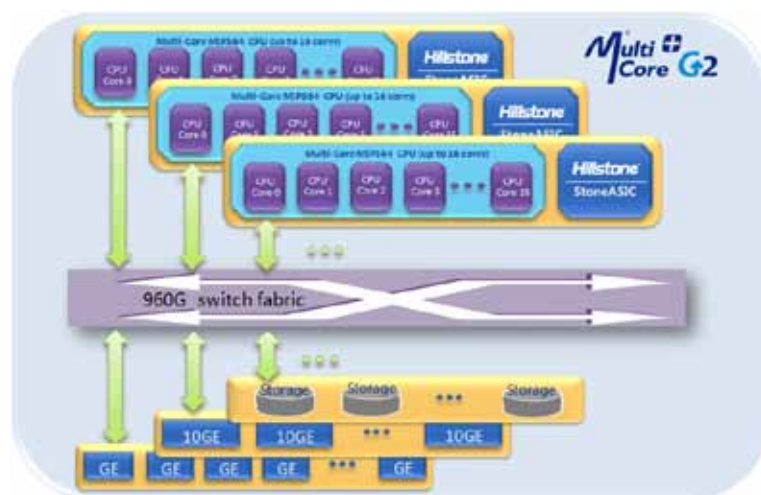


Figure 2: Multi-core Plus G2 Architecture

Based on Multi-core Plus® G2 hardware architecture, Hillstone StoneOS improves processing efficiency by using a fully paralleled approach. The new generation of Hillstone UTM Plus device can maintain high performance and low latency even when multiple security functions are turned on.

Today many multi-core systems use multi-core CPUs to replace NP/ASIC. In these systems, the multi-core CPU offers much better programmability than NP/ASIC. But

Hillstone UTM Plus

multi-core CPU only deals with network security functions. Application security functions are still left for control CPU. On many platforms, some firewall functionality such as new session creation is done on the control CPU.

In Hillstone parallel operating system, all data plane processing are developed for the multi-core CPU architecture, fully utilized the capability of the hardware platform. Hillstone today set performance records in some firewall functionalities such as session ramp up per second. In application security processing, all stream engines are programmed for high parallelism. The data dependency is minimized. This enables the performance and capacity to grow almost linearly with number of CPU and CPU cores. The fully optimized algorithm ensures that the system can maintain high throughput and low latency under complex requirements.

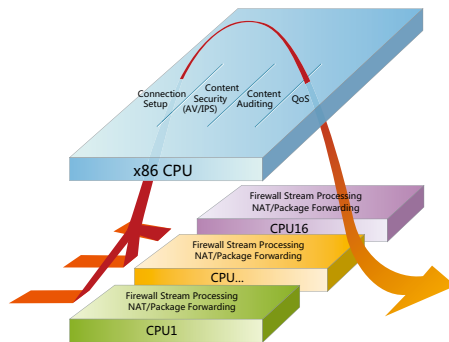


Figure 3: Other Multi-core Solution

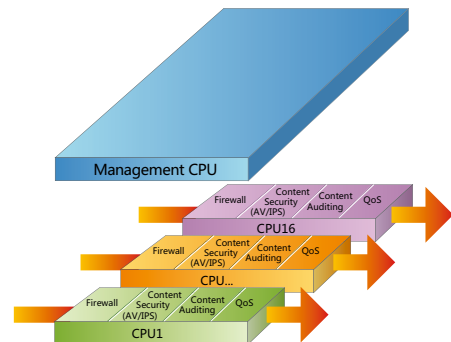


Figure 4: Fully parallel Multi-core Solution

Hillstone Multi-core control technology also minimizes the coordination and allows each core to run relatively independently. When one core malfunctions, the whole system can maintain normal operation.

Security Visibility – Management Based on Role and Application

There is not security without visibility. The application and user identification in StoneOS allows customers to see what is on their network and satisfy their application security needs.

Management based on user roles (RBNS) gives user a more straightforward and fine grained control. Different users, or even users from different location or at different time can have different security profile. Content of user access can also be logged and stored in the storage module or storage server. Searching using user name also makes auditing much easier.

Hillstone UTM Plus

Role based management consists of 3 parts: user based access control, user based resource allocation, and user based logging and auditing. Through authentication that identifies each user, the access rights can be determined, resource and bandwidth can be properly assigned. This can avoid data leakage due to IP spoofing or victims PC being improperly used.

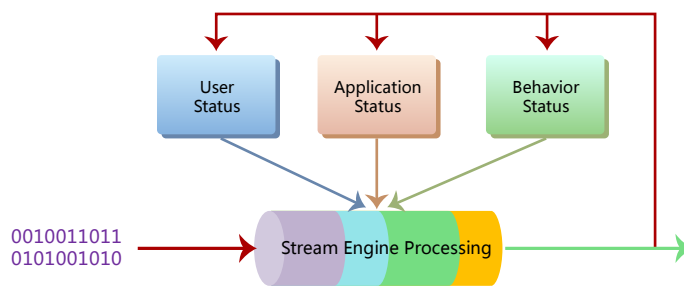


Figure 5: Cross inspection

Parallel Stream Engine

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.

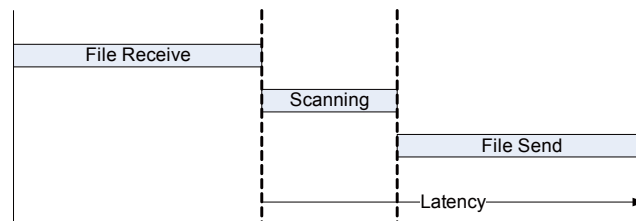


Figure 6: File based scanning

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.

Hillstone UTM Plus

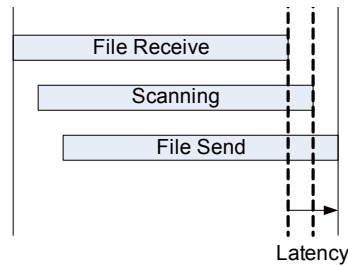


Figure 7: Stream based scanning

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.

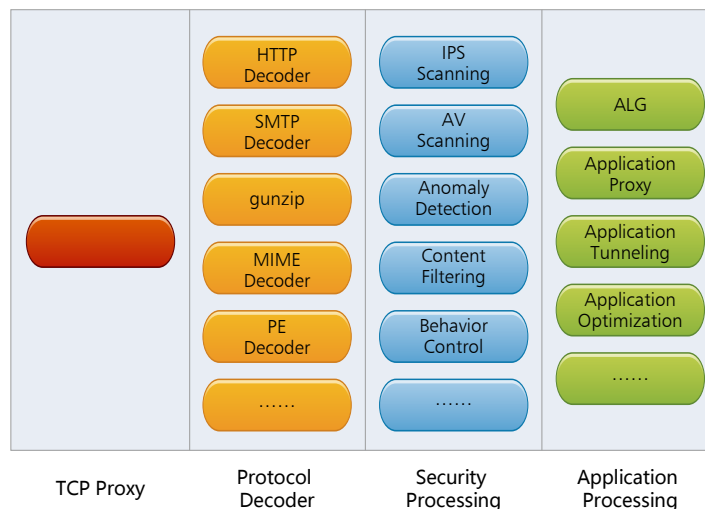


Figure 8: Stream Engine

Hillstone UTM Plus

In traditional UTM system, a flow needs to pass several independent network engines, classification engines, matching engines and policy engines. The redundant effort reduces efficiency and results in low performance. Hillstone implements a unified security processing. Once a packet enters processing pipeline, each stage is only processed once. This includes network functionality, protocol decode, protocol security, content decode, content security, user/application/behavior identification etc. The processing results of the prior step will be input into next steps of the pipeline, as needed. This greatly reduces repetitive analysis and processing, results in improved latency and system capacity and performance.

3. Hillstone UTM Plus Functions



Figure 9: Hillstone UTM Plus Functionalities

Firewall

- New generation of application firewall
- Policy based on application and user roles
- Protect against DNS Query Flood, Syn Flood, DoS/DDoS attacks
- Malformed packet attack protection
- ARP spoofing protection



Hillstone UTM Plus

VPN

- Support standard IPSec VPN and adapt to many deployment scenarios
- Innovative PnVPN
- Support SSL VPN (with support for 2-factor authentication)
- Support L2TP VPN

Anti-Virus

- Stream based engine, low latency, high concurrent sessions, high performance
- Support scanning of large files
- Real time blocking of virus, event logging
- Support common protocols for virus transmission: HTTP, FTP and various email protocols
- Over 400k virus database, updated in real time

IPS

- Stateful, accurate, and high performance attack detection and prevention
- Real time blocking of attack source, IP blocking and attack event log
- Support intrusion detection and prevention for protocols such as HTTP, FTP, SMTP, IMAP, POP3, TELNET, TCP, UDP, DNS, RPC, FINGER, MSSQL, ORACLE, NNTP, DHCP, LDAP, VOIP, NETBIOS, TFTP etc
- Support more than 3,000 attack signatures

Network Behavior Control

- URL filtering based on URL database with more than 20 million entries
- Fine grained access control based on application (P2P, IM, online games, office application)
- Content audit, including BBS post, outbound email, IM chat
- Filtering of sensitive file types, blocking of Java applets/ActiveX

QoS

- QoS rules based on user roles, application, IP address and time
- Support CoS based management, compatible with DiffServ marking
- FlexQoS can dynamically adjusted for optimized bandwidth usage



Hillstone UTM Plus

4. Conclusions

Hillstone UTM Plus solution is based on Multi-core Plus[®] G2 hardware architecture, and utilize fully parallel stream engine for security inspection and security visibility. This solution gives customers an integrated product that deals with today' s complex application and security environment while maintains high performance.