



Hillstone IPS Solution

1. Introduction

Network Trends

- Networks attacks are moving from simple network layer attacks to more complex application layer attacks. Simple firewall functionality is no longer enough. Intrusion detection working in TAP mode cannot block attack sources in real time. There is no standard protocol for IDS and firewall to interoperate. Intrusion detection solution is being replaced by intrusion prevention solutions.

- It seems that security holes and vulnerabilities in software are unavoidable. Applications on the internet are enjoying explosive growth. Application types are increasing and application signatures are more complex. For example, many of today's applications are based on HTTP protocol. This makes the traditional way of identifying applications based on ports no longer valid. How to identify these new applications, and defend against attacks that target these applications, is the problem that the new generation of IPS gateway needs to solve.

- Network bandwidth is increasing, number of applications is increasing. Applications are getting more complex. Types of attacks are increasing. Attacks are becoming more evasive. Traditional IPS is limited by the processing power and cannot do deeper application analysis and attack analysis. Even though people know simple signature matching is not enough for IPS, but limited by the resources, these kinds of false negative and false positive often occur.

Hillstone Networks Intrusion Prevention System is based on Multi-core Plus[®] G2 hardware architecture, fully parallel stream engine and attack detection based on attack forensics. The Multi-core Plus[®] G2 architecture makes it possible for a high performance IPS system. It also provides the high processing capability necessary for the deep application analysis and attack forensics. The fully parallel stream engine optimizes usage of the system resources and provides high usability in case of high concurrent scanning sessions and when other attack defenses are turned on. Attack detection based on forensics reduces false alarm and increases the accuracy of detection.



Hillstone IPS Solution

Characteristics of Hillstone IPS

- Based on deep application inspection, and analysis of complex attacks
- Multi-core Plus[®] G2 architecture provides processing and memory capability for application analysis and intrusion prevention functions
 - Attack detection base on attack forensics which improve accuracy
 - Support analysis and attack protection for protocols include HTTP, FTP, SMTP, IMAP, POP3, TELNET, TCP, UDP, DNS, RPC, FINGER, MSSQL, ORACLE, NNTP, DHCP, LDAP, VOIP, NETBIOS, TFTP etc.
 - Periodic attack signature update. Team of security experts responding to new attack and vulnerabilities in a timely fashion
 - Intrusion prevention based on policy or security zone, and can define different rule set for different protected target.

2. Hillstone IPS Solution

Application Analysis

Hillstone StoneOS adopts a new generation of application identification based on application behavior and characteristics. The deep application identification technology breaks the port based network defense methodology. Only after identifying the application that a flow is corresponding to, can we start protecting against attacks that targets that application. StoneOS supports an application database with several hundreds of applications. And application database can be updated automatically without a software upgrade. With network applications fully visible, StoneOS IPS support intrusion 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.

Extensible Multi-core plus[®] G2 Architecture

Hillstone state of the art hardware platform is a powerful combination of 64 bit multi-core processor, in-house developed ASIC and high speed switch fabric. Multi-core plus[®] G2 hardware architecture provide extensibility for more processing power and I/O options.

Hillstone IPS Solution

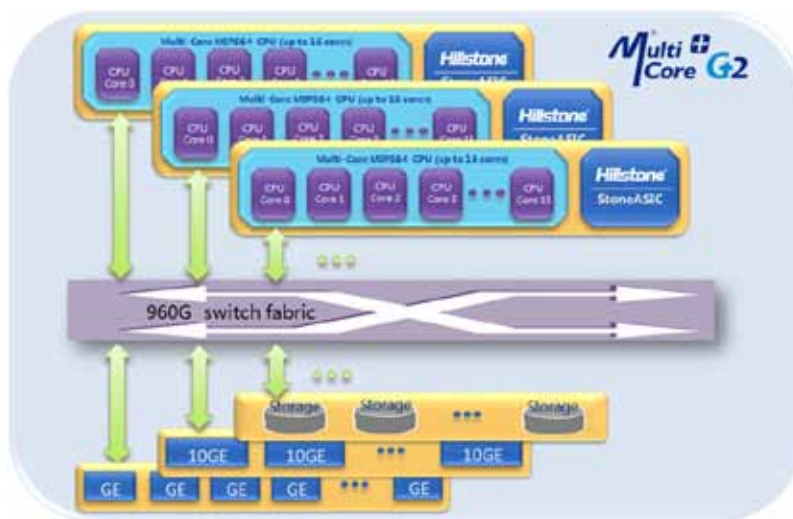


Figure 1: Hillstone hardware architecture

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. StoneOS 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.

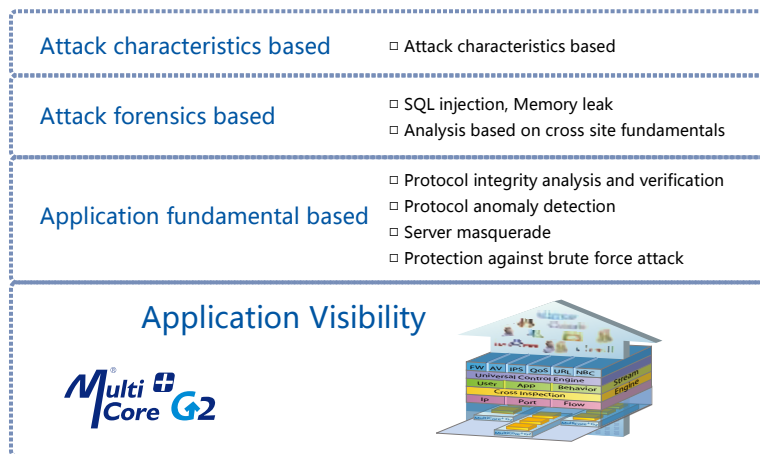
StoneOS offers scalable IPS performance on this platform by running IPS engine on multiple processor cores. Each processor core can independently perform IPS scanning or other security function as needed. The network traffic is load balanced to the least busy processor core for low latency security processing.

Intrusion Prevention based on Application Knowledge and Attack Knowledge

IPS based on signatures is no longer enough for people asking for better accuracy and less false alarms. From technology point of view, how to improve the accuracy of the IPS detection rate? First, the system needs to have strong processing power, able to perform deep application analysis and attack analysis. Secondly, high detection accuracy is based on deep application identification. Thirdly, attack analysis should be based on attack forensics and not just based on signature. Intrusion prevention based on deep

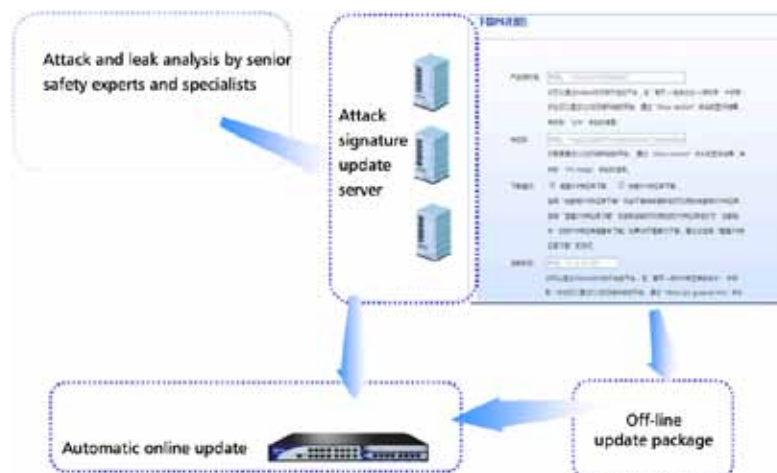
Hillstone IPS Solution

application analysis and attack forensics can detect some evasive techniques of attacks and increase detection accuracy. From deep application state inspection, protocol inspection to attack forensic analysis and finally attack signature match.



Fast Response to Attacks

Support detection and prevention of over 3000 types of attacks, with security response team which actively dealing with new attacks. Attack signatures are updated automatically and periodically.





Hillstone IPS Solution

Policy based Intrusion Prevention

Hillstone IPS can integrate with policy engine completely. Administrator can fully control the following aspect: traffic from which security zone needs IPS, which server or application needs to be protected. Also IPS rule set can be customized for each server under protection.

3. Conclusion

Hillstone IPS provides application protection based on deep application analysis, Multi-core Plus® G2 architecture. With accurate protection, high performance filter and fast response, Hillstone IPS offers an attack prevention solution in today' s complex network environment.