



Hillstone Anti-Virus Solution

1. Introduction

Trend in network security indicates that there are more and more ways vulnerable PCs on the network are attacked and infected, and more mobile users and remote users means that PCs that are connected come with different Anti Virus and security profile. It is possible that PCs inside the network with inadequate defense can be compromised. Host based AV solution is no longer enough. Gateway Anti-Virus offers a second layers of defense that greatly enhance the security of the network.

From technical point of view, Anti-Virus scanning requires a large amount of system resource include memory, bus bandwidth and CPU. With limited hardware support, existing security gateways see dramatic performance drop when Anti-Virus feature is turned on.

Hillstone, based on state of the art Multi-core plus[®] G2 hardware architecture and parallelized stream based scanning engine, offers high performance Anti-Virus solution that detects virus, Trojans, worms, spywares and other malicious software. The hardware architecture provides enough horsepower necessary for antivirus scanning. The stream based scanning engine uses less system resource and offers high scalability in terms of simultaneous scanning sessions and maximum size of file that can be scanned.

Hillstone AV solution has the following characteristics:

- Multi-core plus[®] G2 based architecture addresses the need of AV application that is hungry for CPU and memory resources
 - Support for AV scanning application module for enhanced AV performance
 - Fully parallelized Stream-based virus scanning engine takes advantage of the hardware architecture and is optimized for scalability and performance
 - Stream based multi-level decompressor including RAR format
 - Frequent dynamic virus database update.
 - Support HTTP, File transfer and multiple Email protocols
 - Support multiple actions including terminating connection, fill magic and logging.

Hillstone Anti-Virus Solution

2. Hillstone AV Architecture

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.

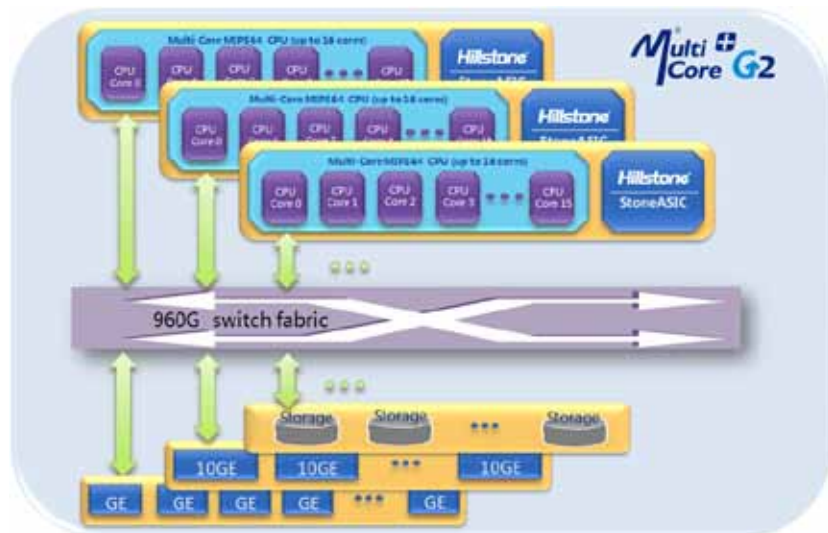


Figure 1: Hillstone hardware architecture

StoneOS, Hillstone parallel operation system, offers scalable AV performance on this platform by running AV scanning engine not only on multiple processor cores but on multiple processors. Each processor core can independently perform AV scanning or other security function as needed. The network traffic is load balanced to the least busy processor core for low latency security processing.

Hillstone Anti-Virus Solution

Software Architecture

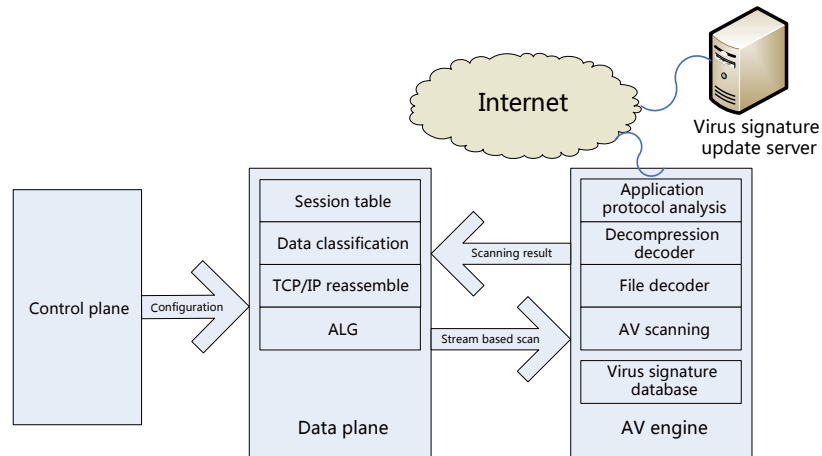


Figure 2: Software architecture

Hillstone Gateway AV uses modular software architecture. The separation of AV engine with packet forwarding means that user have more options in their deployment. On modular hardware platforms, a user can in the beginning use embedded AV where AV engine runs with the packet engine, and when time comes, upgrade to plug-in hardware module to get higher performance.

Modular architecture also means that AV function can be flexibly combined with other security and network features provided by StoneOS, such as role based policy, IPSec and SSL VPN.

Hillstone AV can function in transparent mode, route mode and mixed mode.

3. Hillstone AV Solution

Stream Based Scanning

Traditional AV Scanning is file based. This method is what host AV solution is implemented and older generation of AV solution inherit this method. With this method, the complete file is first downloaded, and then the scanning starts and the file is sent out. The latency as measured by the time between the sender completes its sending and the receiver completes the receiving is very long. For large files, the user application may experience time out.

Hillstone Anti-Virus Solution

Furthermore, file-based AV scanning is not suitable for gateway in that gateway device do not have the large disk storage that is available on the host. The device can not deal with very large files that do not fit in the memory of the gateway. The sizes of files that can simultaneous fit in the device memory also put a limit on how many AV scanning can go on at the same time and how big those files can be.

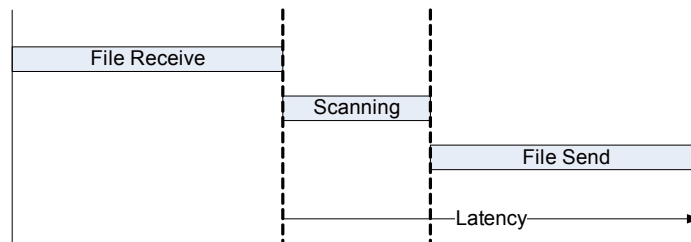


Figure 3: File based scanning

Hillstone scanning engine is stream based, the AV scanning engine examine the stream of packets as they arrives and the stream of packets are sent when no virus are detected. As a result, the user will see significant improvement in latency and their application will appears much more responsive.

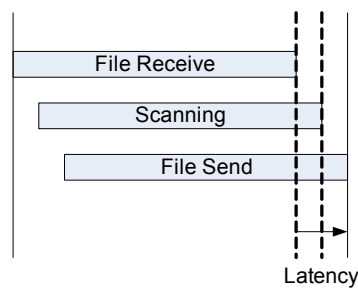


Figure 4: Stream based scanning

Stream based scanning only need to buffer a limited number of packets. It does not have limitation on file size as file based scanning has. The low resource utilization also means more streams of files can be scanned at the same time. Stream based scanning is suitable for Gateway AV solution where high performance, low latency and high scalability is topmost concern.

Stream based scanning can terminate connection when virus signature is detected early on in the stream, therefore save network bandwidth and processing power that



Hillstone Anti-Virus Solution

is needed to buffer the entire file. This is particularly beneficial during virus outbreak when a lot of files encountered may contain virus and the gateway virus scanning could become a bottleneck.

Without streamed based decompressor, stream based scanning engine can do little on compressed files. These files still have to be downloaded before they can be decompressed and scanned. Hillstone offers stream based decompressing engine on popular compressed file format such as ZIP, GZIP and RAR. In another word, on Hillstone security devices, compressed files can be uncompressed and scanned on the fly.

Hillstone AV scanning is highly parallelized to take full advantage of the hardware platform.

Policy Based AV

On Hillstone device, AV is fully integrated with Hillstone' s policy engine. The administrator has full control on what domains of traffic to perform AV scan, what users or group of users to scan, and what servers and application to protect.

4. Conclusion

Hillstone stream based Gateway AV offers a high performance, high scalability solution that meets the need of today' s demanding application that requires low latency and response time.