



Anchiva Hardware Scanning Engine Whitepaper

Contents

- Overview
- ASIC Accelerated Content Inspection
- Highly Scalable Parallel Processing
- Field Upgradeable ASIC
- Malware Polymorphism Processing Technology
- Conclusion

Application content scan technology with patented algorithm on ASIC Architecture

Overview

As the adoption of web and internet based applications are increasing and have become critical business tools, web security solutions are required that can effectively block internet based threats without interfering with the normal operations of web based applications. Utilizing patent pending content identification algorithms and the industry's first ASIC accelerated content inspection engine, Anchiva's Secure Web Gateways (SWG) quickly and comprehensively inspect web content without compromising the integrity of the data or affecting the performance of web based applications.

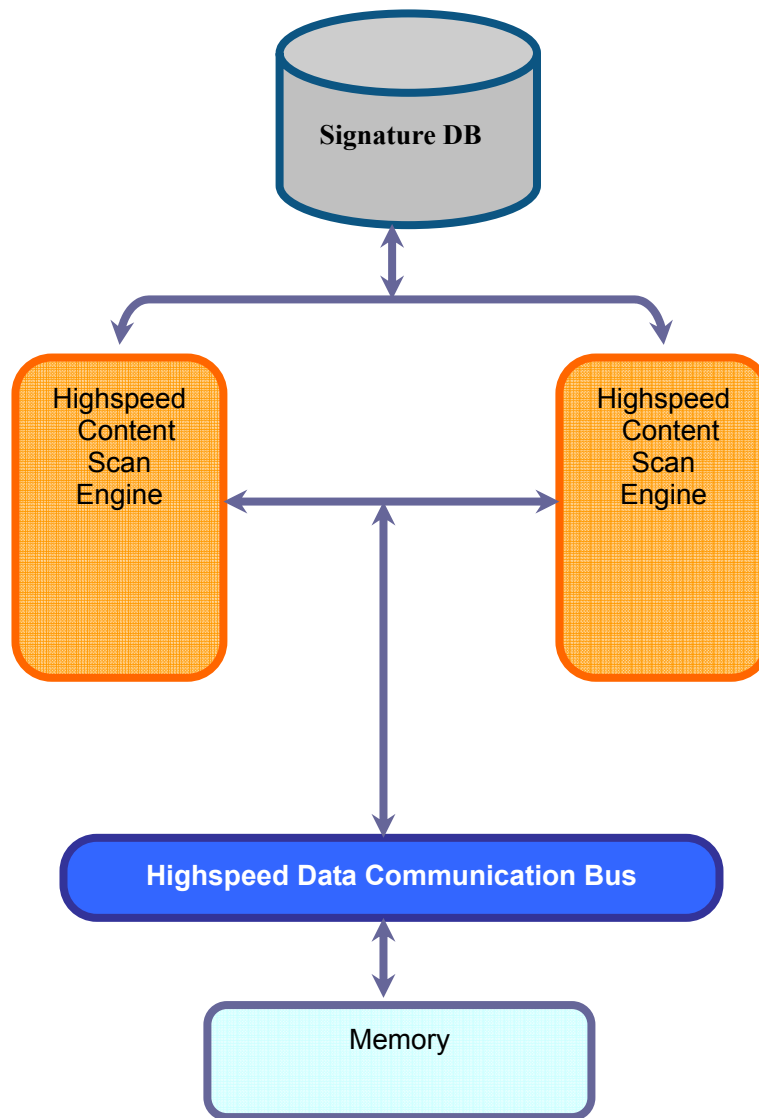
Traditional hardware acceleration technology in security appliances such as firewalls are focused mainly at accelerating packet processing at the network layer. This technology is useful in preventing network breakins when hackers aim their attacks at the network layer (TCP/IP), but is inadequate to detect or prevent today's attacks such as the spread of malware, which are embedded deep in the data content at the application layer. In comparison to firewalls, to prevent today's internet based threats Anchiva's innovative RapidRx ASIC focuses on accelerating content inspection at the application layer without affecting the performance of real time web based applications.

The ASIC plays a key role in the SWG content inspection process as web and internet based applications can be severely affected by network bottlenecks. Anchiva's SWG architecture was designed with a purpose built operating system, custom hardware acceleration and multi-core CPU's to provide industry leading, near gigabit performance and low latency processing of web based content to ensure the SWG does not become a bottleneck in the network. As web content is received by the SWG, patent pending algorithms are applied to the data to quickly detect and eliminate malicious code such as malware, viruses and spyware, identify the use of non-productive applications and enforce acceptable internet use policies in the workplace.

ASIC Accelerated Content Inspection

As shown in the packet processing diagram below, the SWG architecture integrates the RapidRx ASIC into the appliance design by way of a high-speed data communication bus. As data is received at the interfaces of the SWG, AnchivaOS acts as a transparent proxy intercepting traffic that matches a policy. During this process, AnchivaOS uses its multi-core CPU's and ASIC engine to identify, reassemble and classify the content of the data.

A file based inspection approach ensures AnchivaOS accurately identifies malicious from legitimate traffic and also defends against evasion techniques that hackers use to evade traditional security defenses such as network firewalls and Intrusion Prevention Systems (IPS).



Highly Scalable Parallel Processing

—Avoid performance degradation caused by virus signature serial scanning

Internet wide, malware research teams including Anchiva's RapidRx teams are seeing a spike in the number of active malware propagating on the internet. Tens of thousands of new malware samples are being captured and analyzed daily, coinciding with a similarly high number of new websites found to be distributing malware content. To defend against the growing number of malware, the SWG content inspection engine integrates the industry's most scalable signature engine in a gateway appliance along with heuristic analysis of suspicious files.

At present, the current onboard signature database includes 2+ million signatures that are used to detect the original and also variants of the original malware strain. To prevent the system from degrading performance during the content inspection phase, AnchivaOS launches parallel processes to send multiple inspection requests to the ASIC. As new web sessions are received at the SWG, AnchivaOS creates multiple threads of the proxies to simultaneously terminate multiple sessions and process multiple data threads. As files are reassembled, they are handed off to the ASIC engine for inspection of malware content.

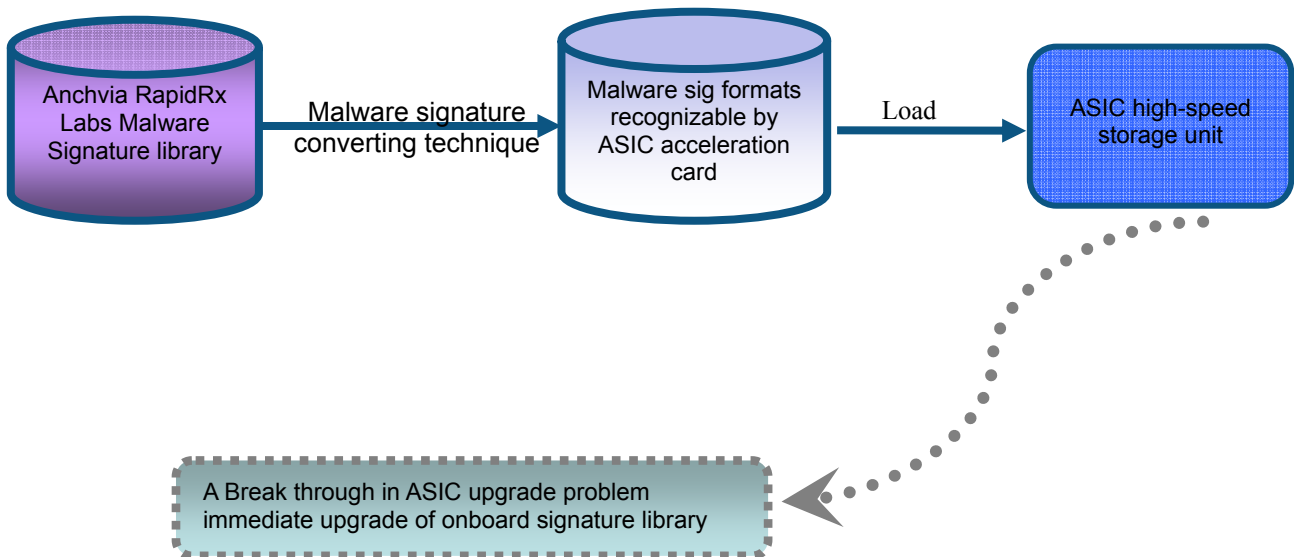
The ASIC itself processes multiple threads simultaneously to prevent one process from becoming a bottleneck, increasing the efficiency of the system along with offering low latency and a highly scalable processing engine.

Field Upgradeable ASIC

—a break thought in the industrial problem of ASIC's inability to upgrade

In some ASIC designs, its programming is hardwired and requires a replacement to be upgraded. This is just the opposite for the Anchiva ASIC as the design of the RapidRx ASIC allows it to be field upgradeable when needed. The ASIC's flexibility and high performance allows the Anchiva system to extend its product lifecycle and continue to add value to a network's security infrastructure for years without the need for costly system replacements.

To adjust to changing malware attacks and design methods, key elements of the ASIC programming can be enhanced or logic needed to be adjusted to detect new malware patterns. To perform this function Anchiva designed the ASIC to be field upgraded simply by upgrading the system firmware which can be done using the standard methods from the WebUI or the CLI. The Anchiva ASIC engine includes onboard high-speed dynamic memory which the ASIC accesses directly across a high speed bus. When the malware signatures are updated, AnchivaOS writes the malware updates directly to the memory cells on the ASIC engine allowing the ASIC to detect the new malware patterns.

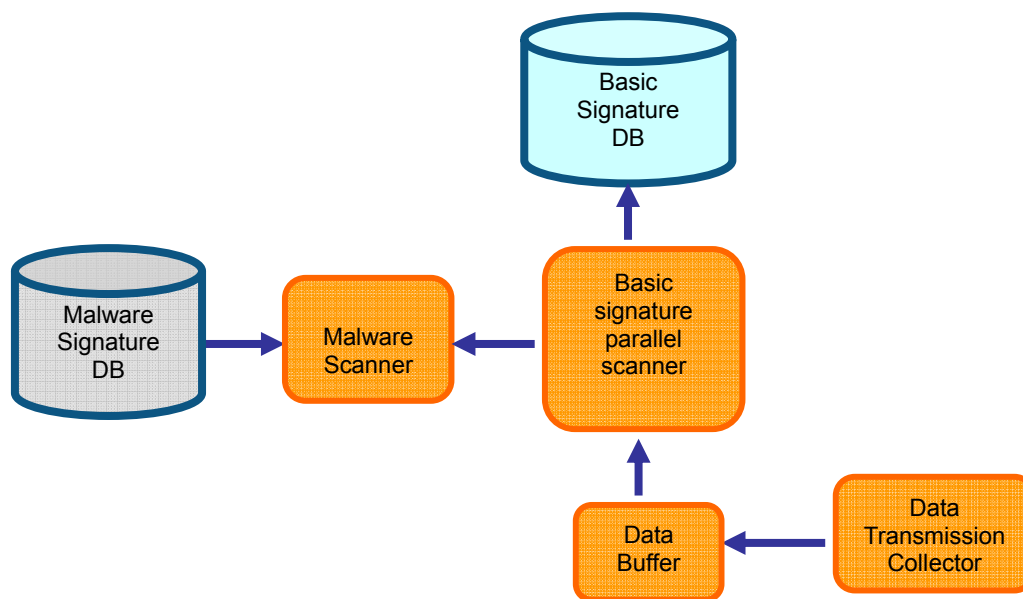


Malware Polymorphism Processing Technology

—Multilevel matching technology

In the real network environment, malware signatures have a wide range of variety, so when a signature library is built, all the factors such as file types, offset addresses and wild cards are included in it, making the signature matching logic more and more complicated.

Anchiva's proprietary hardware scanning algorithm is illustrated in the flow diagram. When data are transmitted into ASIC accelerator's built-in data buffer, the signature parallel scanner starts working and matching basic signature library. Afterwards, the cleaned-up data flow passes through while suspicious traffic is sent to malware scanner for an exact matching. It only takes a small amount of time to execute both match filtering by parallel scanners at the first step and exact matching of malware scanner, which reduces scanning and matching time without having influence on the scanning result.



Conclusion

As internet use becomes mission critical for enterprises and internet traffic increases, organizations need a high performance web security solution that can quickly and accurately differentiate malicious traffic from legitimate web traffic. To meet these requirements, Anchiva's SWG provides the industry's only application layer ASIC that hardware accelerates the deep content inspection process without degrading the performance of mission critical web based applications.

In addition, expanded security features such as web filtering, non-productive application controls and application rate limiting enables the security reach of the SWG allowing customers to collapse multiple security functions onto a single, centrally and easily managed appliance.

All information referred in this document may be updated at any time, and Anchiva will not notify especially.
 Copyright©2005-2009 Anchiva System Ltd. All rights reserved.
 Anchiva OS and Anchiva are registered trademarks.
 The names of actual companies and products mentioned herein may be the trademarks of their respective owners.