

AV Scan Engine

Anchiva AV Engine Dedicates to Network Safety via Parallel Scan and Signature Match

As an exponential growth is witnessed in malware sample number, it is required that malware detection engine be able to recognize more malware signatures, and this number has brought a direct impact on the scan and detection performance of anti-malware gateways.

Bearing a large amount of signatures, Anchiva dedicates to the enhancement and optimization of the signature parallel scan technology, presenting not only the ASIC hardware-accelerated scan engine, but also the software-based parallel scan engine which is able to take full advantage of multiple kernel platform that can scan multiple lines and processes, and thus generates a better anti-virus scanning performance than that of the traditional solutions.

Let's first have a glance at the virus scan engines in the current market.

I. Features of traditional desktop virus scan engine

- Low requirement in performance. High CPU occupation rate not allowed lest other businesses operation might be affected.
- Both virus detection and removal of compromised files should be taken into consideration when producing signatures.
- According to the features above, the traditional desktop virus scan engine have failed to consider the appropriate CPU utilization in their design concept. Today's multi-kernel hardware network platform is especially excluded.

II. Main features of scan engine based on traditional desktop virus engine

1. Embedded Infrastructure

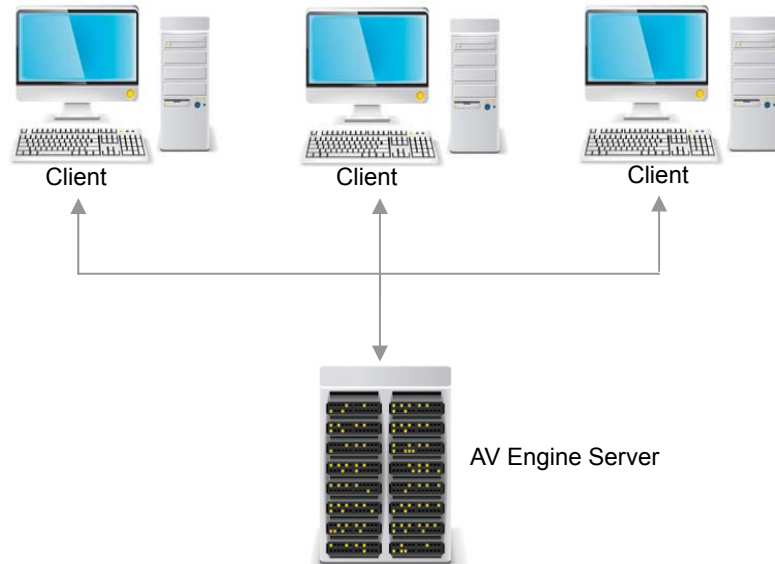
This is a single-line anti-virus scan infrastructure, in which developer shift both the traditional desktop anti-virus scan engine and the signature library into the existing network hardware platform. This simple embedding supports only the transferring of the root line instead of multiple lines, and therefore is unable to take use of the performance edge of the current popular multi-kernel hardware network platform.

2. Independent backend program

This model, which has been widely used by vendors, is developed out of the application system's demand for handling multiple line processes. As depicted below in Figure 1, its main architecture contains several virus scanning processes that can be taken as the clients. The clients send all of their scanning requests to the AV Engine Server and wait for the results. This model has meet the demand for multiple line processes, AV Engine Server, however, has become the bottle-neck of the whole system. Meanwhile, the

frequent switches among AV engine client/server has increased considerably the as well as the I/O port utilization.

Figure 1:



As we have a better understanding of the traditional virus engine, now let's turn to Anchiva's virus scan engine.

When designing its own virus engine, Anchiva has taken the virus gateway-specific features into full consideration, and decide the engine's focus to be on the anti-virus scan and inspection. Its another emphasis on the parallel scanning a great number of signatures and data have resolved the performance bottle-neck caused by the increased signatures. As shown in the Figure 2 below, the AV Engine initializer creates a shared AV Engine initializer environment, of which other processes can make free use. During the AV scan and inspection, every process enjoys the shared and independent access to the environment in a parallel way. This method supports multiple lines of virus scan and reduces both unnecessary switches and I/O Block, taking full use of the multi-kernel hardware network platform, whose upgrade may boost the whole performance.

Figure 2:

