ContentKeeper

White Paper

Deploying a Multi-Gigabit Web Filtering Architecture

As Internet bandwidth demands continue to increase for school districts, many IT administrators realize that their existing web filtering solutions can no longer keep up. With no way to intelligently scale to handle multi-gigabit traffic loads, districts are often torn between allowing access to useful information online and ensuring student safety and CIPA compliance.

This white paper will review what school districts can do when growing bandwidth and processing requirements hamper web filtering efforts. We will list several approaches on how to grow from a simple "single box" web filtering solution into a multi-gigabit architecture as well as provide the pros and cons of each approach. Additionally, we will recommend a load-balanced, fault-tolerant filtering architecture along with a checklist of evaluation considerations.

With no way to intelligently scale to handle multi-gigabit traffic loads, districts are often torn between allowing access to useful information online and ensuring student safety and CIPA compliance

Situation – Your Web Filter Can't Keep Up

Today's websites and social media provide a wealth of dynamic content; however, they use considerably more bandwidth than their predecessors. For example, YouTube supports increasingly high-resolution videos, Facebook and other sites now play videos automatically and high-definition live streaming video is becoming more popular. At the same time, many school districts deploy 1:1 programs and issue mobile devices to students for access to online educational content on and off campus. Keeping up with this tech-savvy learning environment means further demands on bandwidth.

As if these requirements don't already keep district IT administrators busy, companies like Google and Facebook are shifting to "SSL only", restricting access to their information and services to SSL-encrypted sessions. Filtering solutions without SSL encryption capabilities have no visibility into this encrypted traffic, and therefore, will be unable to apply filtering policies to anything below the top-level domain. Filters that do support SSL decryption must now perform on-the-fly SSL inspection and analysis of secure web traffic in order to "see" user-requested content and apply proper filtering policies—a CPU-intensive operation.

Few filters can perform SSL decryption, analysis, reporting and policy-based control at multi-gigabit speeds. However, ContentKeeper, with its *TurboBridge* technology, can decrypt SSL traffic effectively without negatively impacting network performance.

Your Web Filter Can't Keep Up. What Now?

When you reach the point where your single filter architecture can no longer process all your Internet traffic at acceptable speeds, you must decide how to proceed. There are several possible options, each of which we will investigate below.

Live with it: Accept latency and sluggish performance

Why live with the problem? A variety of factors influence a school district's IT decisions, including: unforeseen growth, unrealistic product performance expectations (undersold and overpromised),

unanticipated technology changes (SSL), or other factors that result in degraded network performance. Often, when these unanticipated situations arise, no budget is available to fully remedy the problem. In this case, IT administrators have to consider accepting and dealing with latency and sluggish performance.

One of the most common reasons web filters create network bottlenecks is excessive processing cycles required to properly manage SSL traffic. Some web filtering products are negatively impacted more than others. Some IT administrators disable SSL encryption to improve their network throughput. This prevents the web filter from seeing anything below the top-level domain, meaning they know what site a given student visits, but have no way to track specific pages within those sites. And this significantly risks CIPA compliance. So, to provide properly-filtered access to SSL-encrypted sites, districts need to enable SSL and accept network latency.

Split up your network, add another web filter and route traffic between network segments

On the surface, this appears to be an attractive option: increase your Internet connection bandwidth, split your entire network in half, add another web filter for the new segment, and as a result, double your capacity. Though theoretically, this is a reasonable solution, it comes with many potential problems. For example, if a previous single Internet connection was saturated, then adding another connection could reduce the bottleneck. However, overall bandwidth requirements would increase immediately, leaving administrators with two Internet connections that now overwork two web filters, essentially placing you back where you started. You also face potential problems with breaking applications that serviced devices or users that were once all on the same network but are now spread across two networks. This scenario may be very costly to resolve.

Additionally, depending on the deployed web filter, managing policies, logging, reporting and user search activities could be lost or require significant workarounds. This adds complexity and significantly reduces the effectiveness of a web filtering solution.

Also, because a new gateway connection requires hardware such as routers, switches, firewalls and other infrastructure components, the money saved by implementing this approach is soon lost on additional hardware and support costs.

Finally, it is nearly impossible to split one network into two segments and divide the bandwidth requirements equally between the two new network segments. Even if this worked initially, over time requirements would change, and inevitably one segment would become saturated while the other would retain unused bandwidth. At best, the network splitting option is a temporary fix for a larger problem.

SSL decryption is a major problem for many web filtering solutions, most of which require additional hardware to support it.

Disable (or never implement) SSL decryption

SSL decryption is a major problem for many web filtering solutions, most of which require additional hardware to support it. Some solutions require the redirection of SSL traffic to completely separate hardware via proxy servers and the deployment of proxy pac files. Most web filters negatively impact network performance. Choose a solution that was designed to decrypt and process SSL traffic at multi-gigabit speeds with minimal impact on network throughput. This is where ContentKeeper excels in comparison to other products that attempt to compensate for poor software design through the “just add more hardware” model.

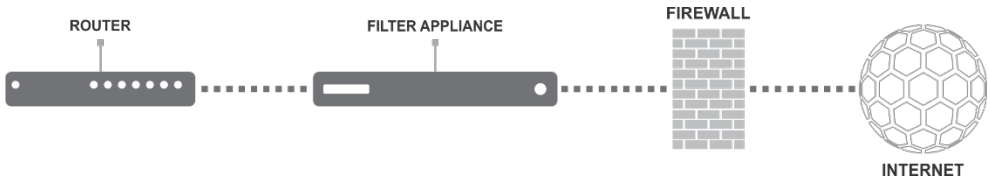
If your web filter causes network latency, a commonly considered option is to turn off SSL decryption. While this approach likely improves filtering performance, administrators will need to block encrypted websites, denying access to valuable resources like YouTube, Facebook and many teaching and learning sites. Also, you will not be able to enforce SafeSearch across encrypted search engines.

Deploy a Multi-Gigabit Load Balanced, Fault Tolerant Web Filtering Architecture

A well designed load balanced web filtering solution has many benefits over previously-mentioned options such as: High speed Ethernet bridge, multi-gigabit capacity, fault tolerance, cost effective growth and centralized management. The image below shows a typical single filter architecture.

As your traffic requirements grow beyond the capacity of a single filter solution, you can easily install a ContentKeeper Layer 2 Load Balancing Appliance and immediately double your capacity by adding an additional filter

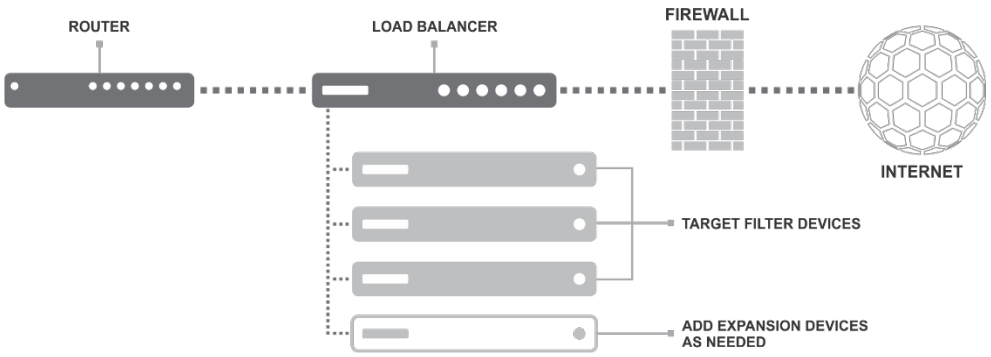
SINGLE APPLIANCE SOLUTION



As traffic requirements grow beyond the capacity of a single appliance, IT administrators can easily install a ContentKeeper Layer 2 Load Balancing Appliance (CK-LBA), and immediately double capacity by adding an additional filter. The CK-LBA is built to handle speeds of 10gbps, 20gbps and beyond.

The diagram below shows ContentKeeper's load balancing architecture. A single CK-LBA intelligently balances traffic between the identical target filter units. If a unit is taken out of service for maintenance or otherwise becomes unavailable, the CK-LBA seamlessly redirects traffic across the remaining target filter units.

LOAD BALANCED SOLUTION

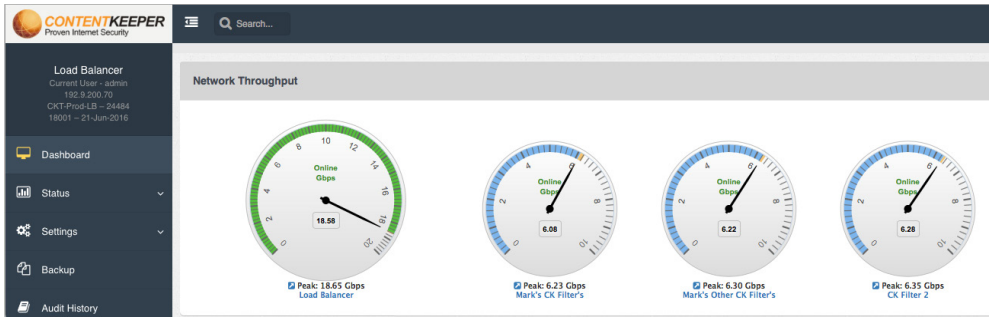


If you deployed your system using the N+1 method (number of filter units required to support your capacity "plus one" extra), the removal of a target filter will not decrease throughput or performance.

Capacity can be increased in the ContentKeeper load balanced solution by adding another target filter device to the filter array. All devices in the array can be viewed in real-time and centrally managed through a single web-based intuitive user interface. Policy management, authentication, logging and reporting are also centralized for all target filter units, so administrators can monitor, track and report on user activity across the entire environment from one central console.

The CK-LBA dashboard image on the next page shows real-time and peak throughput for each device in the target filter array in addition to real-time and peak throughput for all filter devices in the target filter device array.

ContentKeeper strongly recommends when evaluating and selecting a web filtering solution, you verify the solution's performance, features and functionality on your network— processing your traffic and fully configuring the filter the way you intend to deploy it.



Things to Consider When Evaluating Filtering Solutions for Multi-Gigabit Network Environments

There are many web filtering products available on the market and some vendors make feature, functionality and performance claims that are often misleading.

ContentKeeper strongly recommends when evaluating and selecting a web filtering solution, you verify the solution's performance, features and functionality on your network — processing your traffic and fully configuring the filter the way you intend to deploy it. Do not take a vendor's word that it will perform properly on your network or that you can simply turn on a particular feature later and it will work fine with no adverse impact. You need to verify throughput and latency especially with SSL decryption enabled and in production under normal load. Detailed reporting at extremely high traffic volumes requires a reporting solution that is designed to meet these requirements. Reporting solutions designed for small to medium capacity networks often fail catastrophically in 10 gigabits/second and beyond networks, and in some products, a failure in the reporting system can also have an adverse impact on the filtering system.

Here are six key criteria when evaluating a solution:

Capacity and Network Compatibility – The load balanced filtering solution should have the correct interface (1G/10G/40G) compatible with your current network infrastructure. The load balanced solution in its production configuration should have the capacity to process and filter all your web traffic without noticeable delay or latency at peak throughput.

Scalability and Expandability – The solution should meet or exceed your current capacity requirements and easily scale to meet or exceed your anticipated future requirements. For example, if you have a 1Gb connection now, but plan to expand to either multiple 1Gb connections or a 10Gb connection, you should ensure that the solution can properly support any future growth requirements. It is unlikely that you can verify this in your own environment, so you should speak to other districts that operate multi-gigabit networks.

Filter processing speed is more dependent on the software design and internal software architecture than it is on the hardware. Do not assume that a solution designed for small and medium size networks can scale to support multi-gigabit networks by just adding additional hardware.

Fault Tolerance – The solution should continue to function properly in the event a filter device becomes unavailable or is removed from the device array. Ensure that in this condition, the solution will continue to provide complete filtering and meet peak throughput requirements without adding latency. It is also important to ensure that the load balancer properly recognizes devices which are disabled and immediately ceases to direct traffic to these devices. A case could exist where a filter device in the array fails to wire (a condition where a filter device continues to pass traffic, but it does not filter the traffic) and the load balancer continues to direct web traffic through the failed device, thus bypassing filtering. This could have unintended consequences and should be understood.

Few filters can perform SSL decryption, analysis, reporting and policy-based control at multi-gigabit speeds. ContentKeeper, with its *TurboBridge* technology, can do this without negatively impacting network performance.

Device Compatibility – Your solution should support all the types of devices you have deployed or will deploy in the future. If you plan to issue mobile devices to students, you will likely want to filter those devices when they are off your network as well. Ideally, your solution should provide centralized policy-based management, filtering and reporting both on and off campus.

Architecture – The solution should be well designed to manage multi-gigabit traffic with maximum throughput and efficiency. Proxy-based solutions and those that require redirection of SSL traffic should be avoided due to throughput bottlenecks. Choose a solution where the software is purposely built to support large multi-gigabit networks.

Load Balance Design Compatibility – Ensure the web filtering vendor offers a load balancing solution to avoid compatibility issues with third-party hardware and software. Load balancing web traffic at multi-gigabit speeds is very challenging. Using a load balancer that is not specifically designed to handle the distribution of SSL traffic may cause latency issues, errors and even failures. Also, deploying a third-party load balancer increases the chance of finger pointing between vendors when troubleshooting and identifying the source of network issues.

In Conclusion

As bandwidth and SSL processing requirements continue to increase, more schools and districts will require multiple web filters to meet their multi-gigabit filtering requirements. Although there are several architectural deployment options available, the option that makes the most sense in almost all situations is a properly load-balanced filtering solution.

This type of architecture provides fault tolerance, high availability and an easier and cost effective way to upgrade when your bandwidth requirements increase. When implemented correctly, especially with an integrated solution like ContentKeeper, you can manage your entire filtering environment with a custom solution designed for multi-gigabit networks.

Try it for yourself! Call **888.808.6848** or email **k12@contentkeeper.com** to set up a free demonstration.