



Case Study – York County, Va., rethinks Internet filtering appliances to solve remote monitoring needs

Virginia's York County's Chief of Computer Support Services wrestled with an all-too-common issue for ensuring appropriate and disparate Internet surfing policies are maintained in all of its departments; how to do so remotely without adding more layers of software to maintain.

"We originally contracted with a popular company to set and manage our web filtering policies across all County services, including emergency services, judicial, community services, administration and libraries," said Adam Frisch. "Their solution required us to implement one software system at our central IT operations, and another at each satellite location, thus driving up the initial integration and implementation expenses as well as our ongoing manpower costs. It became fairly cumbersome."

At the time, though, very few options to manage such needs remotely through web filtering appliances were on the market, they typically serviced small offices independently with little in the way of flexibility or remote monitoring capabilities. Nevertheless, when its current vendor contract came up for renewal, York County published an RFP to see what the options were.

One of the solutions reviewed was Phantom Technologies' iBoss Enterprise Internet filtering appliance. The system allows IT managers to create multiple Sub-Administrators (delegated administrators) to log into the iBoss interface and manage filtering rules for specific filtering groups. This allows for different authorized personnel to manage the rules for specific departments and groups without having access to others. .

"Traditional filters require blocking all secure 'https' traffic and manually allowing individual websites via an allow list," said Peter Martini, COO of Phantom Technologies. "Our system applies an organization's category selections seamlessly without having to guess which sites should be allowed and which should be blocked. IT managers can always allow or block any specific site (secure or not) by adding them to custom allow and block lists."

The iBoss Enterprise offering also includes a built-in reporter and archiver that generates detailed information allowing network security personnel to monitor and log online Internet activity and usage through a centrally managed web interface. The reports show percent Internet usage based on category as well as the number of attempted violations to the current set of filtering rules. The violation log shows a time-

ordered list of attempted violations with links to the offending website, the category of the violation, and the nickname of the computer that committed the violation.

“Two of the biggest selling points for us were that we could monitor different policies and settings around the clock and right down to the individual user without having to manage two different systems and tie them together,” said Frisch. “The appliances were not only robust, but essentially worked out of the box, as soon as we plugged them in. Like any government organization, we’re very much resource constrained. Being able to manage disparate web filtering policies without increasing our overhead is key, so we implemented the iBoss system to replace our current platform.”

More information is available at www.ipantom.com/ibe_overview_to.html.