

SurfControl Web Filter for ISA Server 2004 wins Gold Award from ISAServer.org

By Thomas W Shinder MD, MVP

As good as the ISA firewall's built-in Web site access control features are, you can always do better. To squeeze out the last ounce of stateful application layer inspection protection for Web connections, you'll need a comprehensive and smart add-on. **We tested SurfControl Web Filter for ISA Server 2004 and found it a stalwart partner in pumping up the ISA firewall security to the next level.**

The ISA firewall (ISA Server 2004) is a multipurpose unified threat management device that sports Web proxy, firewall and VPN capabilities in a single box. One of the most popular uses for the ISA firewall is as a Web proxy server. The Web proxy component of the ISA firewall enables network clients to forward Web connections (HTTP, HTTPS and HTTP tunneled FTP) to the ISA firewall and have the ISA firewall's Web proxy filter perform stateful application layer inspection and access control over what users on ISA firewall Protected Networks can access.



As good as the built-in access control mechanisms are, there is always room for improvement. Access control over Web content is a critical part of your overall network security policy and access control infrastructure. In order to get the most out of your ISA firewall's ability to protect your network from both known and unknown threats, you'll need some help from third party add-ons.

This is where the SurfControl Web Filter for ISA Server 2004 comes into the mix. **The SurfControl Web filter picks up where the ISA firewall development team left off and fills in the gaps to provide you with a superior level of access control over Web connections.**

I decided to give the SurfControl Web Filter for ISA Server 2004 a whirl on my own ISA firewall. My first concern with installing a new product is that I'm going to need a Ph.D. on that product just to get the thing installed. I was pleasantly surprised by how **easy it was to install the SurfControl Web filter onto my ISA firewall**. SurfControl even provided a link to a version of MSDE on their own Web site that you can use, instead of sending you to www.microsoft.com and letting you figure that part out for yourself. For this, I award SurfControl five social credits!

Of course, you can also use SQL logging for larger organizations. My goal in testing the product was to see if it worked, how well it worked, and how easy it would be to make it work. SQL would have removed the "easy" part, although for organizations who have the requisite SQL expertise, I'm sure that getting the SQL logging to work will be a relative no-brainer, as the **SurfControl philosophy seems to revolve around security and ease of use.**

Once the product was installed, I went to the Rules Administrator. This is where you configure access policy for Web connections through the ISA firewall. The Rules Administrator interface is very easy to work with, and even if you don't read the manual, you'll be able to figure out how to create access policies controlling what users can and cannot do when they connect to Web resources through the SurfControl Web Filter enabled ISA firewall.

SurfControl identifies the type of material on a site by assigning it a category such as Adult or Sports. They have 47 categories in total which gives you fine-tuned, granular control over the types of sites you want to manage. In their latest release, they've added Spyware and Phishing categories, which is a real help in protecting business from these emerging and especially dangerous threats

One thing I really like is a record of when users do something they shouldn't be doing. Users might access sites that violate network use policy, or they might be infested with worms trying to "call home" to upload private information to a hacker database. SurfControl Web Filter for ISA Server 2004 makes it easy to alert the network security administrator via e-mail and other mechanisms of such indiscretions.

Sometimes I like to see what's happening in real-time. While the ISA firewall's built-in real time log filtering allows you to see what users are doing on the Internet in real time, filtering out all the extraneous data isn't always for the faint of heart. After installing SurfControl Web Filter for ISA Server 2004, it was **remarkably easy to see what users on our network were doing on the Internet in real time**. I could also shut down a user in real time from the console, which was a special treat.

SurfControl Web Filter for ISA Server 2004 adds a couple of critical pieces missing from the out of box installation of the ISA firewall: control over the amount of time a user can spend on the Internet and control over how much content the user can transfer over the Internet. Both these technologies are things that ISA firewall administrators have been begging for for at least the last four years. **SurfControl has heard the pleas of these ISA firewall administrators and enables them the power and flexibility of bandwidth and time control over Web access.**

The vanilla ISA firewall configuration enables you to block access to sites using URL Sets and Domain Name Sets. While these are handy tools, you'll end up making it an avocation getting all the domain names and URLs into these sets if you use the ISA firewall's graphical interface.

Even if you had hundreds of spare hours to manually enter this information in ISA firewall's configuration interface, you still have to figure out what to block. SurfControl Web Filter for ISA Server 2004 solves both these problems by maintaining their own comprehensive database of millions of malicious and otherwise dangerous Web sites. They then go a step further and categorize these sites for you, so that you can control access by site category. This increases the flexibility you have over your site control plans.

But SurfControl even goes a step further. Since it's impossible to update the database of malicious and dangerous Web sites in real time, SurfControl uses artificial intelligence (AI) technologies to evaluate sites users visit in real time and blocks them dynamically if they meet the specs in the AI controls. You are able to review the sites the SurfControl Web Filter AI technology categorized by running a report on the activity.

We found this real time AI evaluation of Web site risk to be exceptional and a real boon to any company who needs very strong access control over dangerous Web site visitation.

One thing I thought was **exceptionally cool (and useful) is the SurfControl Mobile User protection feature**. One issue often forgotten by firewall administrators is that while users with corporate managed laptops are subject to corporate access control requirements when on the corpnet, these users can do just about anything they like once they leave the secure confines of your well-managed network. The problem is that once these managed devices return to the corporate network, they bring in all the junk users accumulated when they were on the outside.

SurfControl solves this problem by enabling you to install an Agent on managed devices. The Agent communicates with the SurfControl components installed on your ISA firewall and enforces the same Web usage policy you have for your corporate network devices. Or, if you want a custom policy enforced on the mobile clients, you can create a custom ruleset that applies only to the mobile clients.

This ability SurfControl provides for protecting and controlling mobile clients alone is worth the price of admission!

The only downsides of SurfControl Web Filter for ISA Server 2004 are that not all the features I expected were available to ISA firewall administrators. Two features I was really looking forward to were the ability to perform access control on all protocols (such as peer to peer) not just Web protocols, and popup/banner blocking. None of these features were available in the version of SurfControl Web Filter (5.0) for ISA Server 2004. Had these features been available, I could give this product an unequivocal five thumbs up. For this, I'll have to ding the product one-half star.

Even without these features, I found SurfControl Web Filter for ISA Server 2004 to be easy to install and use, and didn't break anything (a common problem with ISA firewall add-ons). The product did everything it said it would do and configuring it didn't require me to pour over the manual. Product stability was excellent and I was also pleasantly surprised by the low number of false positives and negatives.

Overall, I'd recommend anyone looking for enhanced Web access control for machines located both on and off network to check out SurfControl Web Filter for ISA Server 2004. I think you'll like what you see and agree that it is an exception solution for your ISA firewall's Web access control policies.

RATING: 4.5/5.0