



Rush Hour on the Internet: Oregon Department of Transportation Takes the High Road with the M86 Web Filter and Reporter

Client:

Oregon Department of Transportation

Web Site:

www.oregon.gov/ODOT

Number of Users:

4,000

Requirements:

Web Filtering and Reporting

Solutions:

M86 Web Filter and Reporter

Profile

The Oregon Department of Transportation (ODOT) is recognized as one of the most progressive and innovative government agencies in the country. Responsible for providing a safe, efficient transportation system that enhances Oregon's economic competitiveness and livability, ODOT maintains a large staff of over 4,000 employees spread across more than ten different divisions.

The Challenge

The Internet is a mission-critical tool for ODOT, enabling its employees to effectively carry out their job functions. As a government agency, ODOT also has a responsibility to protect its employees from inadvertently viewing objectionable Web sites. Should an employee choose to misuse the Internet, ODOT must protect itself from potential legal liabilities. To make Internet use as productive and safe as possible, ODOT needed a filtering solution that would: 1) allow fast, reliable, and uninterrupted Internet access, and 2) Effectively block inappropriate sites while keeping needed informational sites accessible.

ODOT originally had a filtering solution integrated with its Unix-based firewall server. This approach, also known as "pass-through" filtering, is common practice in many companies, yet it can create problems in the areas of performance, system failures, and troubleshooting. Since ODOT's filter was integrated with the firewall, this resulted in two possible points of failure on their network: the first being the firewall server, the second being the filtering server.

An important job function of many of ODOT's departments is to visit vendor sites, technical sites and newsgroups. The installed filter "over blocked," preventing access to necessary sites. Additionally, the filter blocked only the domain and not the IP address, which meant that sites had to be manually unblocked. This resulted in more labor and increased support costs, as end users had to contact the IT staff to unblock needed sites on an individual basis. The extraction of a blocked site would typically take as long as one hour.

Internet logs are a key piece of company information and must be easily available. Reports with the installed filter took a long time to generate. Additionally, Web access could not be tied back to particular individuals – a component that is necessary for companies to increase productivity and protect themselves from potential legal liabilities.

Solutions

In an effort to improve filtering effectiveness while reducing overhead costs and the burden on its IT staff, ODOT replaced its existing filter with the M86 Web Filter and Reporter (M86 WFR) high volume filtering server.

“The M86 WFR’s stand-alone appliance design was a very important consideration for us,” explains Marshall Wells, Manager of Security for ODOT. “It was easy to install and has been very simple to use. This saves us valuable time and resources since we do not have to devote our technical support staff to fixing problems. If a support issue arises, M86 is able to fix it over the Internet rather than deploying a technician to troubleshoot. The M86 WFR also provides effective blocking without over-blocking. In instances where we do need to get sites unblocked, M86 is very efficient. It takes them only 10-15 minutes, where we were previously accustomed to waiting one hour or more.”

The implementation of the M86 WFR has also simplified ODOT’s existing infrastructure. Since it is not integrated with the firewall server, it does not create choke points, interfere with unfiltered web requests, or add another point of failure to the network.

“The M86 WFR generates reports very quickly and easily, enabling us to identify potential problems early on,” continues Wells. “This is in sharp contrast to our previous filter, which took hours, days or even weeks to generate a single report because of its real-time processing. The M86 WFR has enabled us to accomplish our original goals of protecting ourselves from legal liabilities, reducing administration and maintenance costs, and improving employee productivity. We are very pleased with the products’ performance and M86’s attention to our needs.”

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry’s leading Secure Web Gateway provider. The company’s appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advance threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters

828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific

Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 04/06/10