

“IT and security staffers no longer need to spend time cleaning up after the attacks, so they can spend time on more productive endeavors.”

Steve Olson
Las Vegas Review Journal
Support Services Manager

Las Vegas Review-Journal “Scoops” Website Attacks with the Juniper Networks NetScreen IDP

Page 1 | Customer Profile



Customer:

Las Vegas Review-Journal, Nevada's largest news resource

Industry:

Publishing

Challenge:

Prevent attacks from crippling the network and impacting productivity

Solution:

Juniper Networks NetScreen IDP

Benefits:

- Safeguarded network from malicious attacks
- Reduced network downtime
- Increased IT productivity
- Increased business efficiency

The Las Vegas Review-Journal, the Stephens Media Group's largest newspaper, operates 27 daily, weekly and specialty publications and runs Websites for each of its media outlets. Its media distribution spans eight states and is managed from the corporate headquarters in Las Vegas and its 17 regional offices.

Like many other newspapers, the Review-Journal relies heavily on the Internet to get information to the public and receive feedback from subscribers and news tips from sources. Like other media companies, the Review-Journal has found that its Websites are often targets for hacker attacks and other security threats. At no time was this more evident than earlier this year, when the Review-Journal's LasVegas.com Website was attacked by intruders, who manipulated an e-mail feature on the site so that thousands of spam e-mails were sent from the company's server.

The LasVegas.com Website receives, on average, more than 1.6 million visitors per month. It provides information on the Las Vegas area and gives visitors the ability to

perform online bookings for hotels and other travel functions. Many people rely on the site to give them accurate and timely information and the Review-Journal makes every effort to ensure that nothing jeopardizes the level of trust it has built with subscribers and sources. That trust was severely tested when hackers broke into the Review-Journal's "e-mail a friend" feature on the LasVegas.com site. The tool is provided so that people can message family and friends about Las Vegas. But the attackers got into the script, manipulated its function and began sending spam e-mails.

"We noticed the amount of traffic had climbed exponentially, causing our service to slow to a crawl," says Steven Olson, support services manager at the Las Vegas Review-Journal. "Then we started getting complaints from people saying we were spamming them." The Review-Journal immediately shut down the "e-mail a friend" service. The ensuing "clean up" was both costly and time consuming. Three people had to work full-time for more than a week to fix the problem and the e-mail feature was down for several days.



Although this particular intrusion was the most glaring in recent months, the Review-Journal's site had been—and continues to be—under attack every day. The LasVegas.com site, which began operating about five years ago, has seen attempted intrusions increase steadily. It is one of the most attacked sites on the Internet, says Vikas Khorana, network administrator at the Las Vegas Review-Journal. "And we had no effective tool in place to block those attacks," Khorana says.

The Solution

The Review-Journal started looking at tools in the marketplace such as intrusion detection devices, but the available products didn't provide what the company was looking for: something that would allow it to identify potential attackers and prevent attacks rather than report what had happened after the fact.

"There wasn't a whole lot of sense in how the intrusion detection products operate," Olson says. "They sit on the side of the network and watch everything happen and then tell you that you were attacked. But they don't do anything about it."

In May 2002, the Review-Journal IT staff began beta testing an intrusion prevention product from Juniper Networks, the Juniper Networks NetScreen-IDP 100. The Juniper Networks NetScreen-IDP 100 is the first intrusion detection and prevention (IDP) system that accurately detects attacks and stops them before they can impact critical resources.

By the end of May, the Review-Journal staff completed deployment of the Juniper Networks NetScreen-IDP in sensor mode and migrated it to full detection and prevention mode within a week. Operating the Juniper Networks NetScreen-IDP in sensor mode, which is often used to test accuracy of the system before installing it in-line, enables detection of attacks without deploying prevention capabilities.

Using proprietary technologies, the Juniper Networks NetScreen-IDP 100 identifies more real attacks and significantly reduces the number of false positives and missed attacks. With its high level of accuracy and ability to be deployed in-line, customers can drop a malicious packet or connection in real-time to eliminate the cost and impact of attacks. Centralized, rule-based management simplifies the deployment of Juniper Networks NetScreen IDP and allows users to keep it current.

The Review-Journal soon plans to install two Juniper Networks NetScreen-IDP 100s in High Availability (HA) mode. "High availability is what we want; we've created an entirely redundant security environment," Olson says. "The Juniper Networks NetScreen-IDP 100 really fit the bill and isn't as costly as most intrusion detection systems."

The Benefits

Protecting its Internet resources is especially critical to the Review-Journal, as it generates a growing amount of revenue from online advertising and news content on its 40 Web sites, and relies on the Web for all internal and external e-mail traffic. With the Juniper Networks NetScreen-IDP 100s in place, malicious packets that previously would have reached the Review-Journal's servers are being dropped before doing any damage.

"This is an in-line installation, so any traffic that comes into the network has to cross this device," says Olson. "We're able to block Web attacks to the sites that could result in a Denial-of-Service at any given time. This is a lot more preventative than intrusion detection systems."

"IT and security staffers no longer need to spend time cleaning up after attacks, so they can spend time on more productive endeavors," Khorana says.

The Review Journal recently discovered another benefit of the Juniper Networks NetScreen-IDP 100. After the system had been deployed the company suffered an attack when a hole was inadvertently left open in its network environment. The Juniper Networks NetScreen IDP system was able to capture enough log information to track down the source of the intrusion. The FBI is now investigating the case based on this information.

"Now we can track where the attacks are coming from and report them," Olson says. "The people who are being investigated for the attack did not know we had this technology in place. If they had known we had it, they probably would not have attacked."



CORPORATE HEADQUARTERS AND SALES HEADQUARTERS FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

www.juniper.net

Copyright © 2003, Juniper Networks, Inc. All rights reserved. Juniper Networks is registered in the U.S. Patent and Trademark Office and in other countries as a trademark of Juniper Networks, Inc. ERX, ESP, E-series, Internet Processor, J-Protect, JUNOS, JUNOScript, JUNOSe, M5, M10, M20, M40, M40e, M160, M-series, NMC-RX, SDX, T320, T640, and T-series are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.