



Intelligent to the Core.™

Netronome Prevents “Man-In-The-Middle” Attacks

*Threats to SSL traffic and OS update services in the Enterprise are prevented
by Netronome SSL Inspector Appliance*

PITTSBURGH, PA – July 31, 2009 – At Black Hat USA 2009 taking place in Las Vegas, Nevada this week a popular breakout session exposed security concerns with the way browsers and operating system update software handle SSL certificates containing null characters. These weaknesses allow a man-in-the-middle attack to intercept HTTPS sessions without the user being aware that this is occurring. In addition, it allows for an attacker to intercept software update requests and return their own update code to the client without the client’s knowledge. The Netronome SSL Inspector Appliance™ prevents this from happening by detecting all SSL traffic and validating the SSL certificates and stopping the SSL connection from being established if the certificate contains null characters.

The Netronome SSL Inspector Appliance is the industry’s highest performance transparent SSL proxy and allows security appliances, in both government and enterprise networks to detect threats inside SSL traffic. As an in-line device, the SSL Inspector Appliance sees all SSL traffic traveling in and out of the enterprise and inspects the SSL server’s certificates used for each session. The appliance enables any server certificates containing null characters, such as those outlined in the attacks described at Black Hat, to be detected and prevents the SSL connection from being established. To ensure that the enterprise is aware of the attempted attack, a log is kept of the details for the blocked session.

The SSL Inspector Appliance provides complete policy control over all aspects of SSL encryption for enterprise networks. This allows the network manager to set policies controlling traffic to servers using self-signed SSL certificates which are commonly used by malicious software. The SSL Inspector Appliance also works with security appliances such as intrusion detection systems (IDS), intrusion prevention systems (IPS), data loss prevention (DLP) systems and network forensic systems to enable these systems to detect hidden threats inside SSL flows, which would otherwise go undetected.

“With the recent data breaches and the breakout session given at Black Hat, people are becoming more aware of the problems with SSL,” said David Wells, vice president, technology and general manager EMEA at Netronome. “The SSL Inspector Appliance enables users to get the full security benefits of SSL while preventing sophisticated man-in-the-middle attacks and other threats that exist within SSL traffic.”

About Netronome Systems

Netronome is a leading developer of highly programmable semiconductor products that are used for intelligent flow processing in network and communications devices. Netronome’s solutions include network flow processors and acceleration cards that scale to more than 20Gbps. They are used in carrier-grade and enterprise-class communications products that require deep packet inspection, flow analysis, content processing, virtualization and security. Netronome is headquartered in Pittsburgh, PA, with core operations in San Jose, CA and Boxborough, MA, and international locations in the United Kingdom, China and South Africa. To learn more about Netronome and its products, please visit www.netronome.com.

###

Media Inquiries:

Heather Fitzsimmons
Mindshare PR
On behalf of Netronome
Phone: 650.947.7400
Email: heather@mindsharepr.com

Jennifer Mendola
Marketing Manager
Netronome
Phone: 724.778.3290
Email: jennifer.mendola@netronome.com

NETRONOME.COM

144 Emeryville Drive, Suite 230 Cranberry Township, PA 16066
Phone: 877.638.7629 Fax: 724.778.3312