

Barracuda Spam Firewall Rejects Invalid Non-Delivery Report (NDR) Messages

Submitted by: BondPR UK

Thursday, 21 August 2008

New Invalid Bounce Suppression Feature Blocks Bounce Messages Resulting From Spoofing Attacks

Basingstoke, UK – 21st August, 2008 – Barracuda Networks Inc., the worldwide leader in email and Web security appliances, today announced a new feature in the Barracuda Spam Firewall that can differentiate legitimate Non-Delivery Receipt (NDR) messages – also known as bounce messages – from invalid NDR messages resulting from spoofing attacks. Using Invalid Bounce Suppression, the Barracuda Spam Firewall prevents "backscatter" messages from reaching innocent email senders.

"Backscatter is an unfortunate side effect of the continued prevalence of email spoofing by spam campaigns that is now plaguing corporate email servers," said Stephen Pao, vice president of product management for Barracuda Networks. "It is also a frustrating, and sometimes confusing, problem for email users who are the innocent victims."

Backscatter occurs when spammers, hackers or other users with malicious intent, spoof the email addresses of legitimate email users to send spam, viruses or worms. The receiving email server typically rejects the email and sends an NDR message to the spoofed email address. As a result, the legitimate email user receives a bounce message for emails that they never sent.

"While one common technique to minimise the impact of backscatter is to simply define policies to block all incoming bounce messages, doing so can result in the blocking of legitimate bounce messages," said Pao. "As such, distinguishing legitimate from invalid bounce messages can be extremely important to users who send business-critical email."

Invalid Bounce Suppression tags the sender addresses of all outgoing messages sent from the Barracuda Spam Firewall's outbound relay, or through the Barracuda Spam Firewall – Outbound appliance. The tags are encoded with built-in expiration periods and encrypted to prevent forgery. When an NDR message is received by the Barracuda Spam Firewall, a valid tag must be present in bounce recipient address (i.e., the original sender address) for the bounce message to be delivered. If the bounce recipient address does not contain a tag or if a tag is invalid, the NDR message is rejected. Usage of the Invalid Bounce Suppression feature is transparent to legitimate senders and recipients.

"Beyond the reputation benefits of preventing spam and viruses from leaving an organisation's network, Invalid Bounce Suppression has a direct impact on reducing the amount of unwanted email that hits users' email inboxes," added Pao. "Invalid Bounce Suppression provides another compelling reason why organisations should also consider relaying their outbound email through an email security solution, such as the Barracuda Spam Firewall or Barracuda Spam Firewall – Outbound."

In addition to Invalid Bounce Suppression, the latest Barracuda Spam Firewall version also includes additional rules governing email policy, including new policy rules for character sets used in emails and attachments, reverse DNS resolutions of sending email servers, and full URLs (including query strings) embedded in emails.

Pricing and Availability

The latest features, including Invalid Bounce Suppression, are available with Barracuda Spam Firewall firmware release 3.5.12 and above. The Barracuda Spam Firewall is available in eight models with prices starting at £599.

About the Barracuda Spam Firewall

The Barracuda Spam Firewall is available in eight models and supports up to 100,000 active users with no per user licensing fees. Its architecture leverages 12 defence layers: denial of service and security protection, rate control, IP analysis, sender authentication, recipient verification, virus protection, policy (user-specified rules), Fingerprint Analysis, Intent Analysis, Image Analysis, Bayesian Analysis, and a Spam Rules Scoring engine. In addition, the entire Barracuda Spam Firewall line features simultaneous inbound and outbound email filtering with the inclusion of sophisticated outbound email filtering techniques, such as rate controls, domain restrictions, user authentication (SASL), keyword and attachment blocking, triple-layer virus blocking, and remote user support for outbound email filtering. The Barracuda Spam Firewall's layered approach minimises the processing of each email, which yields the performance required to process millions of messages per day.

For more information on the Barracuda Spam Firewall, visit <http://www.barracuda.com/spam>.

About Barracuda Networks Inc.

Barracuda Networks Inc. is the worldwide leader in email and Web security appliances. Barracuda Networks also provides world-class IM protection, application server load balancing, Web application security, and message archiving appliances. More than 50,000 companies, including Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar, are protecting their networks with Barracuda Networks' solutions. Barracuda Networks' success is due to its ability to deliver easy to use, comprehensive solutions that solve the most serious issues facing customer networks without unnecessary add-ons, maintenance, lengthy installations or per user license fees. Barracuda Networks is privately held with its headquarters in Campbell, California. Barracuda Networks has offices in eight international locations and distributors in more than 80 countries worldwide.

For more information, please visit www.barracuda.com.

#

For further press information please contact:

Paul Shlackman, BondPR

E: paul@bondpr.com

T: 01628 673 007