DEFENDING AGAINST SPAM WITH SYMANTEC VIRTUAL APPLIANCES

By Mathew Lodge
Doug Iler

The unpredictable and rapidly growing volume of spam e-mail can present a major management challenge in enterprise environments. Deploying Symantec® virtual antispam appliances on Dell™ PowerEdge™ servers can help organizations cost-effectively scale e-mail filtering capacity to meet the peaks and troughs of spam volume while reducing management time and costs.

Related Categories:

Symantec
Systems management
Virtualization

Visit DELL.COM/PowerSolutions for the complete category index.

Server virtualization has become a key technology for many enterprises, enabling efficient utilization of hardware resources and a host of other advantages. In the case of e-mail filtering, however, virtualized antispam software can be useful not only because of the general advantages of virtualized environments, but also because the filtering can actually function more effectively in those environments than it can as a dedicated appliance—providing a flexible way for enterprise IT administrators to meet the challenge of the unpredictable and rapidly growing volume of spam assaulting e-mail defenses. By using Symantec virtual antispam appliances, organizations can both cost-effectively scale their filtering capacity as needed and help reduce management time and costs.

UNDERSTANDING THE CHALLENGE OF SPAM

Symantec first introduced Dell hardware–based antispam appliances in early 2005, but has been in the antispam business since it purchased Brightmail in 2004, and is currently the market share leader in messaging security according to IDC.[1] This is important because it allows Symantec to collect spam data from an extremely large base of e-mail accounts—intelligence that is key not only to accurately identifying spam messages, but also to learning the traffic patterns and tactics of spammers. Symantec continuously harvests spam messages from 2–3 million "probe accounts"—dummy accounts set up to receive spam at Internet service providers and companies worldwide.

The trend in spam has been ever upward—there is more spam now than ever before—but its rise is not linear; spam comes in waves as spammers take advantage of news and events to get responses, and as they try different techniques and tactics to get around antispam filters. Figure 1 demonstrates this pattern, showing e-mail messages identified as spam as a percentage of all e-mail messages processed by Symantec over a one-year period, including variations in the seven-day moving average.

Spam is a form of e-marketing, and spammers try to exploit the same marketing opportunities as legitimate businesses. For example, in January 2008 e-mail servers were flooded with spam ads for a handbag that aimed to take advantage of Valentine's Day gift giving. The message was a scam; there was no handbag for sale, and the spammers used the same geotargeting technology utilized by legitimate businesses to send users who clicked on the links to a variety of destinations depending on their IP address. (Those in Europe and parts of Asia, for example, were routed to an online dating site.)

[1] "Worldwide Messaging Security 2007–2011 Forecast and 2006 Vendor Shares: DLP, Encryption, and Hosted Services Heating Up," by IDC, Doc #209602, December 2007.

The key point is that the commercial reality behind spamming drives peaks and troughs of inbound Simple Mail Transfer Protocol (SMTP) traffic that are difficult to predict, making engineering antispam filtering capacity a significant challenge. Too little capacity, and the system may block or delay legitimate e-mail, or flood mailboxes with spam when the filter is turned off to clear the backlog. Too much capacity, and spam appliances may sit idle—not only wasting IT resources, but also consuming unnecessary energy. But when a spam peak arrives, what was idle capacity the previous week is now necessary to allow an organization's e-mail to continue flowing.

Traditionally, antispam organizations have been locked in an arms race with spammers on both effectiveness and accuracy: the antispam organizations have tried to ensure that spam filters could accurately identify as much spam as possible, even as spammers tried tactics such as image and PDF spam to get around filtering technology. However, the sheer volume and unpredictable variation in spam has also meant that effective antispam technology must be both powerful and easy to operationalize—in other words, requiring as little ongoing administration overhead as possible.

VIRTUALIZING ANTISPAM TECHNOLOGY

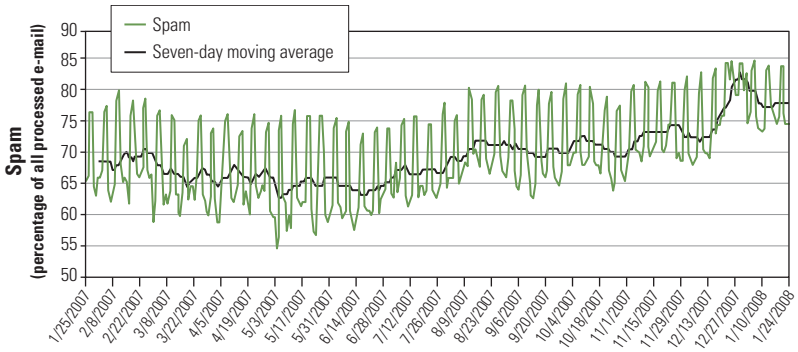
Some organizations using Symantec antispam technology have reported dissatisfaction with appliance-based antispam protection because the waves of spam do not map well to fixed units of appliance capacity. The increasing adoption of server virtualization offered an opportunity to address the problem of effectively operationalizing antispam technology, leading Symantec to introduce a new VMware® virtual appliance version of its Mail Security 8300 antispam appliance. By using a virtual appliance rather than a dedicated hardware appliance, organizations can add or subtract capacity as the level of incoming spam increases or decreases, helping avoid both insufficient capacity and wasted resources.

This virtual appliance is certified to run on the VMware ESX Server and VMware Server platforms. Unlike using virtual environments for development and testing, deploying production applications on virtualized servers is not simply a matter of building an image, booting the virtual instance, and hoping it will behave and perform the same way as one booted on a bare-metal OS. Most enterprises today are heavily dependent on e-mail, so antispam software is typically a key production application that they cannot afford to have compromised.

To help ensure performance is not compromised and with the assistance of VMware, Symantec has thoroughly tested its virtual antispam appliance and modified the code to help optimize performance in VMware environments and to work around known limitations and other issues. For example, virtualized I/O is typically more processor intensive than bare-metal I/O, and antispam technology is heavily dependent on I/O to help ensure peak message flow. In addition, the VMware approach to running operating systems not designed for virtualization is to dynamically patch the kernel code to force sharing of resources that the OS assumes it controls exclusively, such as I/O. To an application, this approach can mean that the OS behavior is different—often in ways that make little or no difference, but sometimes in ways that do. The Symantec virtual appliance is designed for production environments where reliability can be critical.

The Symantec virtual appliance is also designed for simple deployment and management in enterprise environments. The operational benefit of adding new virtual instances to help boost antispam capacity is wasted if each instance needs extensive configuration to provide consistent message handling across the group of virtualized instances. It is therefore key to ensure that the Symantec management application can synchronize antispam configurations and policies across multiple concurrently operating virtualized servers, and that reporting is available at a summary level, not just at the level of individual servers. After all, if administrators cannot see what volume and types of spam their environment is receiving as a whole, they would find it difficult to tell whether they need more or less antispam capacity.

Figure 2 shows a Symantec virtual appliance dashboard that illustrates several key points. First, the volume is volatile: over a 24-hour period, the volume varied from less than 20,000 to more than 30,000 messages per hour—more than 33 percent variation. Second, sender reputation is a key way to identify malicious e-mail and other spam, with 73.6 percent of the messages identified as threats based on reputation—a reminder of why intelligence about spammers is so important to effectiveness.



Source: "The State of Spam," by Symantec, February 2008, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Spam_Report_-_February_2008.pdf.

Figure 1. *E-mail messages identified as spam over a one-year period*

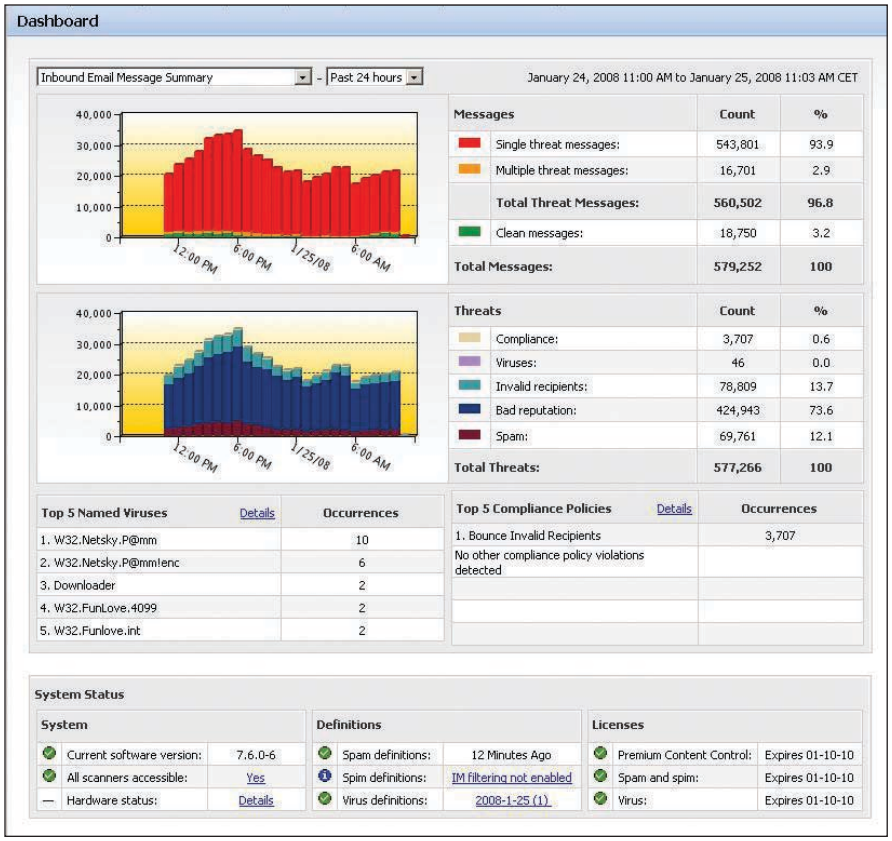


Figure 2. *Symantec Mail Security 8300 virtual appliance dashboard*

Finally, in this example environment, 96.8 percent of the messages were spam. This ratio is much higher than the average of 78.5 percent recorded by Symantec in January 2008,[2] and illustrates what a localized problem spam can be: with such change and variation in spam traffic, average figures (often used for forecasting) may not apply to specific environments.

Using a virtual antispam appliance offers several other advantages as well. Extra server capacity, for example, need not be dedicated to antispam technology—multiple applications can share the pool of virtualized servers, which cannot be done with single-purpose appliances. Virtual antispam appliances also offer licensing advantages. Per-server licensing of a dynamic application is impractical in virtualized environments, because administrators would need to know in advance how many server licenses they need to buy. Licensing per mailbox protected, or using another metric unrelated to the number of servers, can be essential.

Both physical and virtual appliances can offer significant advantages in enterprise environments, and Dell is working with partners like Symantec to take advantage of this technology. The Dell virtualization portal at DELL.COM/Virtualization, which features the Symantec Mail Security 8300 series, provides links to the Web sites of Symantec and other vendors where administrators can download preconfigured virtual appliances for a variety of VMware and other platforms to preview the features. Those who feel a hardware-based solution will suit their needs may choose to purchase a hardware version of the appliance. However, many may opt for a virtual appliance—like that provided by Symantec—to take full advantage of the dynamic flexibility offered by a virtualized infrastructure.

CREATING FLEXIBLE DEFENSES AGAINST SPAM

Antispam technology can be far more effective when virtualized than when running in a dedicated appliance because it can help overcome a major challenge for enterprise administrators—efficiently matching e-mail filtering capacity to spam volume, and avoiding both blocked inbound e-mail and potentially expensive wasted capacity. Symantec virtual antispam appliances provide synchronized antispam rules, filters, and other configuration data as well as clear summary reports across the virtualized environment, features that can be essential to realizing the advantages of virtualization. Deploying these virtual appliances offers a cost-effective, scalable way for enterprises to create flexible defenses against the ever-growing volume of spam.

Mathew Lodge is a senior director of product marketing for the Symantec antispam and e-mail archiving product set.

Doug Iler is a senior manager for enterprise virtualization solutions at Dell.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINKS

Symantec Mail Security 8300 Virtual Edition:
www.symantec.com/business/products/overview.jsp?pcid=2242&pvid=1721_1

Symantec Security Response Weblog:
www.symantec.com/enterprise/security_response/weblog

Dell virtualization solutions:
DELL.COM/Virtualization

[2] "The State of Spam," by Symantec, February 2008, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Spam_Report_-_February_2008.pdf.