# Scram Spam!

Securing Servers from E-mail Attacks

Security has become an increasing concern for IT professionals at medium and large businesses. This security concern extends to one of the most highly used IT business functions — e-mail.

According to Matthew Anderson, market analyst at the Radicati Group, "We're expecting directory harvesting attacks [DHA] and Denial of Service [DoS] attacks to grow almost 40 percent from 2006 thru 2007. Minimizing what gets to the server has become increasingly important."

More than ever, company e-mail servers need to be secured and protected — beyond the traditional firewall and antivirus solutions. "Security threats that come in through e-mail are now the server's responsibility," says Andrew Klein, senior product manager for SonicWALL.

"These threats aren't just spam. They are more serious threats such as phishing, viruses and e-mail attacks on the entire network. So the e-mail system has to be able to pick out all of these threats."

E-mail-based threats are becoming more and more sophisticated, and security strategy needs to be constantly assessed. "Most companies are finding that the security apparatus they installed three years ago isn't holding up," continues Klein. "It's too slow or it malfunctions a lot. It can't handle the increasing volume of e-mail. With two or three times the volume of spam today, plus other threats, companies need a new approach to stay ahead of it."

And while protecting the server against DHA, DoS and other network attacks is a primary aspect of server protection, filtering inbound and outbound e-mail is important as well.

"Companies are looking for effective solutions that minimize false positives and administrative overhead, and let the user manage their inbox," says Frank Oskorep, a security specialist at CDW. "And we're seeing more interest in content filtering, including the ability to block particular attachments based on content, both inbound and outbound. Compliance adds another reason that companies are asking for outbound content filtering."

SonicWALL's Klein agrees that compliance to government and industry regulations is an important aspect of the growing interest in filtering e-mail. "For compliance with regulations like Sarbanes-Oxley and HIPAA [Health Insurance Portability and Accountability Act of 1996], e-mail systems need to check messages for sensitive data like credit card and Social Security numbers.

"Others are concerned with intellectual property matters, like whether workers are getting e-mails from competitors. So protecting outbound and inbound e-mail has now become a security issue — you have to secure the information coming in and going out."

"There's great concern for outbound filtering," agrees Daniel Freeman, director of product management at Symantec. "Companies are now asking the question, do we know what intellectual property or key sensitive information is trying to exit our Internet gateway?"

## A Network Approach

To improve e-mail server protection and security, many companies are turning to network appliances, software and managed third-party services, rather than more features within their e-mail server. "We recommend that you separate security and filtering from the server, to insulate the e-mail server from attack," says Stephen Pao, vice president of product management at Barracuda Networks.

One important reason, Pao points out, is that up to 90 percent of incoming e-mail is usually spam. "You'd need e-mail servers capable of handling ten times the number of connections than you would if you had an e-mail security appliance blocking the spam upfront."

Another reason to separate security and filtering is that it makes good financial sense. "Having a separate e-mail security appliance can be cost-effective, and operationally more efficient," says Pao. "They're easy to deploy and set up, and can be kept up to date with almost no human administrative involvement. We've taken technologies that weren't readily available to medium-size businesses and now made them affordable."

The impracticality of server maintenance is another good reason to consider a network appliance. "In general, doing maintenance on an e-mail server can't be easily done on an hourly update basis, or at the level needed to address threats, without interfering with ongoing operation," notes Pao.

For similar reasons of practicality, many companies want to implement increased e-mail security by simply adding on an appliance. They are doing this rather than making this function part of a unified threat management solution."

"When most companies are looking to solve their spam problem, they want to solve it now, without having to rip out any of their network infrastructure," says Pao. "We often hear that they are happy with their current firewall, VPN (virtual private network) and intrusion prevention system (IPS). In these cases, they are looking to install a new, separate solution."

## 5.11 Tactical Targets Spam

Over the past three years, 5.11 Tactical Series, a law enforcement and tactical apparel maker based in Modesto, Calif., with a staff of 180, has seen its annual business grow rapidly from a mere $200,000 in 2000 to $65 million in 2006. With this growth, 5.11 Tactical's volume of e-mail has also increased — most, but not all of it being spam, viruses, phishing expeditions and other unwanted messages.

"Last year's e-mail security challenge were blocking phishing and hacking e-mail," says Elias Martinez, 5.11 Tactical Series' director of technology. "This year, it's spam, which we've tried to filter out. I quickly learned that if we tighten up the filters, they start capturing legitimate e-mails — false positives — and helping users get them back becomes a burdensome administrative effort." Martinez quickly discovered that fighting spam was no simple process.

"As the amount of spam coming in went up, our previous software filter couldn't handle it all," adds Martinez. "The antivirus and spam filtering software was slowing down our e-mail server. We needed to take the load off the server and let it just handle the e-mail." »

To find a happy medium of successful spam blocking with minimal false positives, as well as easy user access to blocked messages, 5.11 Tactical selected the Barracuda Spam Firewall (BSF) appliance. In Martinez's opinion, "It paid for itself in ROI within the first two weeks," as 5.11 Tactical Series saw immediate results from its new approach to fighting spam.

Martinez continues, "Since moving to the spam firewall appliance, we've been able to improve our control of the spam flow by about 98 percent. Spam complaints have gone way down. Regional sales managers say it has helped their productivity. They no longer have to spend 10 to 15 minutes a day just sifting through and deleting spam.

They're also able to go into the BSF repository and pull out false positives easily. And the e-mail server has settled down, and is now running a lot smoother. "The Barracuda Spam Firewall has made day-to-day IT administration much easier," according to Martinez.

## Layers of Protection from Spam

The Barracuda Spam Firewall (BSF) is available in six different models and can support up to 30,000 active end users, with no per-user licensing fees. The appliances are compatible with all e-mail servers and can fit into nearly any medium or large business environment.

The BSF is designed to protect against e-mail-borne threats like spam, viruses, phishing, DoS attacks and other malware (malicious software designed to damage the host computer) that enter the network from outside the organization. Multiple firewalls can be clustered to provide greater capacity and higher availability.

"We recommend installing a spam firewall at the network perimeter," explains Barracuda Networks' Pao. "That way it receives inbound e-mail connections on behalf of your entire e-mail infrastructure — for example, a cluster of Microsoft Exchange, Lotus Notes and UNIX e-mail servers, as well as any other e-mail servers that support SMTP [Simple Mail Transfer Protocol]. It will reject threat-laden e-mails and pass on the good ones to the downstream e-mail infrastructure."

During the connection management process, the Barracuda Spam Firewall filters e-mail messages through five defense layers, beginning with verifying the authenticity of the envelope information. If a message attempt does not meet this test, the connection is dropped. More than half of the total e-mail volume for the average medium or large business can be blocked through such connection management techniques.

After passing through the five connection management layers, messages undergo message analysis in seven subsequent defense layers that include: checks against custom policies defined by IT (such as reflecting compliance or Internet usage policies), behavioral layers (such as Rate Control), attack profiling (such as too many attempts to reach invalid users), and data-driven and rule-driven layers using information provided by the Barracuda Central operations center (delivered via Barracuda Energize Updates issued automatically every hour).

Only if an e-mail message successfully passes through all the Barracuda Spam Firewall's 12 defense layers is it sent along to the e-mail server, and then onto the user's mailbox. Messages that fail these tests can be sent to quarantine areas, where users can check for false positives.

"Out of the box, we deliver a 95 percent spam accuracy rate, and a false positive rate of 0.01 percent," says Pao, adding that with additional tuning and increased use, businesses can increase the accuracy ratings. "We avoid setting the filters too tight, because this can end up creating additional administration work in having to process false positives."

All Barracuda Spam Firewall models have outbound filtering techniques including attachment scanning, virus filtering, rate controls and encryption. These features help organizations ensure that all outgoing e-mail is legitimate and free of viruses. The Barracuda Spam Firewall Outbound-mode also lets IT enforce outbound e-mail policies, such as blocking e-mails containing sensitive identity information from leaving the network.

## Another Ally in the War on Spam

Canyon Partners, an alternative asset management company based in Los Angeles with a staff of 130, reports experiencing similar improvements in dealing with e-mail. Its choice for spam defense is SonicWALL Email Security software, according to Tim Capps, senior engineer at Canyon Partners.

"We've been running SonicWALL Email Security for about three years and it has made a huge difference in suppressing spam," reports Capps. "As a front end to our e-mail system, SonicWALL Email Security has taken a lot of the garbage processing and storage load off our exchange server.

And since we're subject to compliance, we have to archive every piece of e-mail that is delivered to users' mailboxes — for a number of years. That's a lot of disk space. Anything we can do to minimize how much e-mail we have to be responsible for storing — such as blocking spam before it gets to the e-mail server — is a good thing."

SonicWALL Email Security doesn't register very many false positives, according to Capps, and makes it easy for users to look for and retrieve blocked messages. "We get a daily summary of all the e-mails that got caught. Users can quickly review the summary, and if they find anything that shouldn't have been junked, they can click on it and get it back. This also whitelists the sender [updates the rules database to accept e-mail from that address]."

SonicWALL Email Security can be used for outgoing e-mail as well. Canyon Partners has made use of this feature to block any questionable outgoing e-mails. Capps says, "Our primary concern is blocking outbound viruses. We also use it to block any outbound spam."

## Manning the Gateway

"SonicWALL Email Security sits in front of the server, and fends off many types of attacks," explains SonicWALL's Klein. "For example, if someone is sending a DoS attack to the e-mail server, we can shut off that port. Or if they're trying to do a directory harvest attack, we can detect that and shut it down."

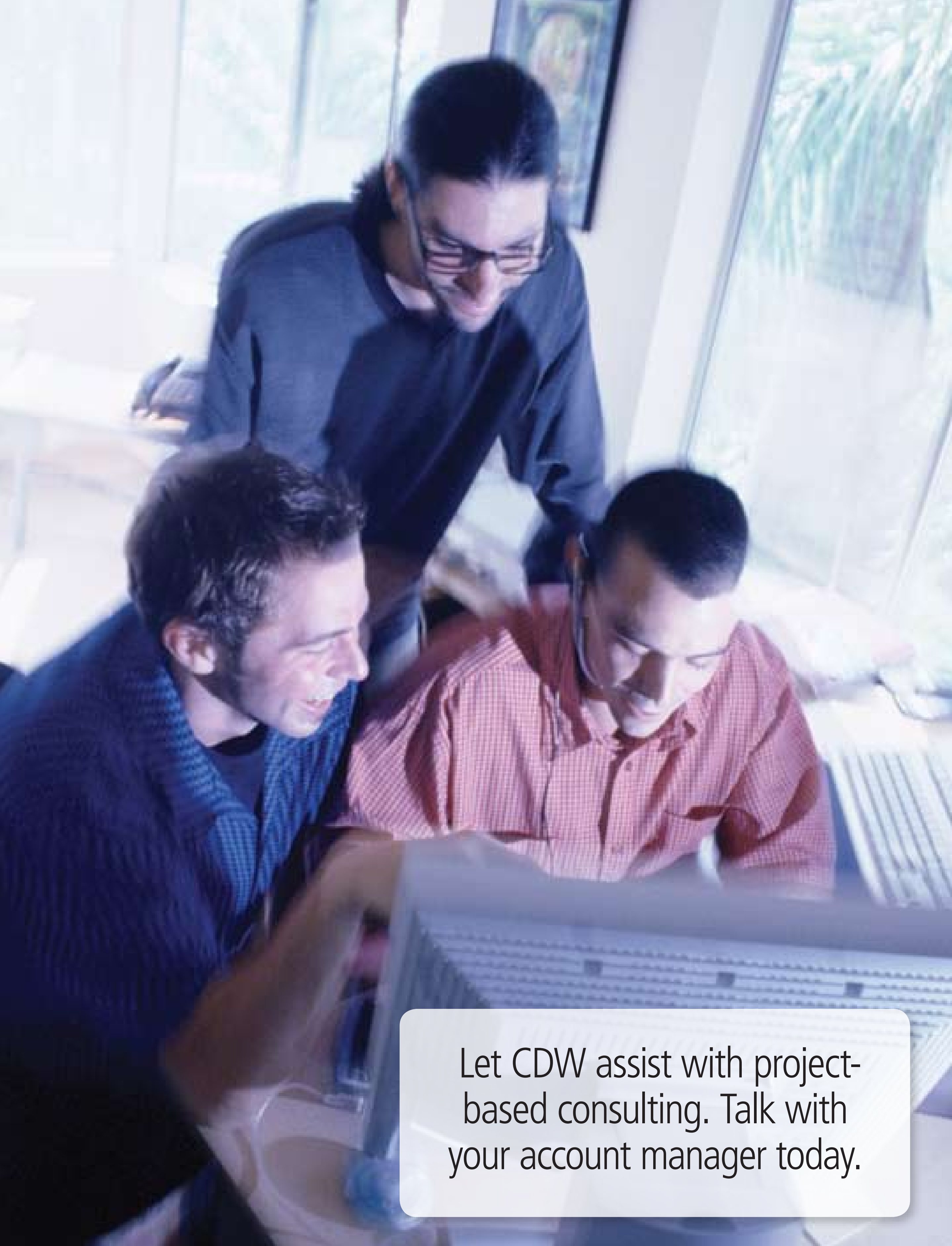
SonicWALL offers its Email Security as 1U Mini and 1U Full Linux-based appliances, as software running on Microsoft Windows 2000 and Windows 2003 Server. Models 200, 300, 400 and 500 are for up to 50, 250, 750 and 2,000 users respectively. There are also two enterprise models, one for up to 5,000 users, and one for over 5,000 users.

SonicWALL's Preemptive Scanning MTA (Message Transfer Agent) provides the fast message analysis and delivery speeds needed to keep pace with today's skyrocketing e-mail volume. By scanning e-mails in memory before they are processed by the Message Transfer Agent for queuing and delivery, SonicWALL appliances pass only the good e-mail along into the network.

SonicWALL Email Security takes less than an hour to install, and needs less than 10 minutes of administration a week. Some of its primary features include quick configuration, seamless LDAP (Lightweight Directory Access Protocol) integration, end-user spam management reporting, automatic updating and a streamlined interface.

SonicWALL's mail protection includes its Time Zero Virus Technology; Directory Harvest, DoS and Zombie attack protection; inbound and outbound e-mail management; and end-user spam management.

"The best advice I can give IT people is 'It doesn't have to be complicated,'" says SonicWALL's Klein. "If you're spending more than a few hours working on e-mail security, you're spending too much time. Keep in mind, there's a simple solution available." ◊



Let CDW assist with project-based consulting. Talk with your account manager today.