Why am I Getting More Spam? FAQ

Introduction

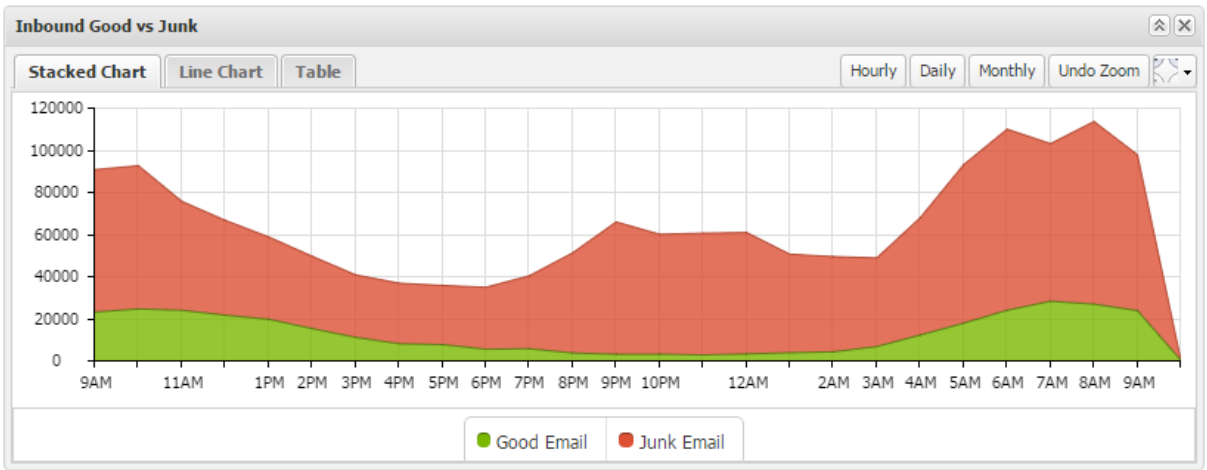
The increasing numbers of spam is a hot topic in the media, with organizations reporting increases each year. Image spam and pump-and-dump stock spam are the primary spam types on the rise, and they are the most difficult to catch.

FAQs

How is SonicWALL Email Security protecting me against this increased deluge of spam?

SonicWALL targets world-class effectiveness through a combination of data and product updates. Customers running the latest product versions experience the most success. Below is a chart from the SonicWALL Lab where is shows the rate of inbound good versus junk email. This was tested using SonicWALL Email Security 8.2.1 with messages plotted on an hourly basis.

Inbound Good vs. Junk email rate on SoniceWALL Email Security 8.2.1



How do I know the effectiveness level for my company?

It is not immediately easy to determine the effectiveness level for your company. As the administrator, you can view the report Inbound Good vs. Junk. While this will not tell you your effectiveness rate, it will show you what percent of your email we are catching as junk, and therefore the minimum effectiveness rate assuming that all your good mail is actually junk that we are missing (which is obviously not the case.) To evaluate the effectiveness you are experiencing in your own inbox, a basic approach is to divide the total spam caught in your Junk Box by the total in your Junk Box plus the total missed spam. For example, if 5 spam were in your inbox and 55 spam emails were in your junkbox, then your effectiveness is 55 divided by 60 for an effectiveness rating of 92%.

NOTE: Any effectiveness you're experiencing in your inbox is going to be after SonicWALL Email Security cleans out all directory, dictionary spam, and denial-of-service attacks, along with any messages stopped by policy/content filtering. In a typical company, these frequently make up over 50% of incoming messages. Thus your personal effectiveness will typically be significantly lower than the actual effectiveness.

NOTE: The most efficient spam-blocking occurs after SonicWALL Email Security cleans out all directories, dictionary spam, and denial-of-service attacks, along with any messages stopped by content filtering policies.

What can I do to increase my effectiveness?

Check to make sure you are properly configured. Often small configuration mistakes can lead to significant spam leakage. For example, companies sometimes have their own domain on their whitelist, which spammers will frequently spoof, thereby giving them a free pass.

What is SonicWALL doing to protect me going forward?

SonicWALL Email Security uses a combination of technologies to fight spam, phishing, virus, and other attacks:

- SonicWALL SMART Network is a one-million strong global network of users that submit feedback on good and junk mail constantly. We are continuously growing this global base and are in the process of rolling out new technology to the SMART Network to enable submission of information to help with new outbreaks.
- SonicWALL Content Filtering has been granted a patent due to its unique Adversarial Bayesian technology that specifically handles spammers' attempts at trickery. We retrain this system regularly with updated data.
- SonicWALL Reputation is the only hierarchical reputation system that goes beyond IP address reputation to also provide reputation on domains, senders, messages, and message components.

In addition to these, SonicWALL has unique technologies for fighting phishing, viruses, DHA and DoS attacks. SonicWALL is also constantly investing in new technologies and has developed and deployed Image Thumprinting, Auto-Junking, and Stock Ticker Dictionaries.

Why do I get the same message in my inbox over and over, even if I submit it?

Messages frequently look identical, but are actually unique. For example, an image spam may blur, tilt, slightly discolor, or cut into pieces the image within. All of these are too subtle for the human eye, but do make each one unique. Text messages often look identical but will also have slight variants. Spammers intentionally make each message unique to avoid filters.

What do I do if a spam or phishing message is missed by the filter?

Submit your messages to SonicWALL by sending them to junk@sonicwall.org (for spam) and junk@sonicwall.org (for fraud/phishing.) These must be sent as attachments for us to be able to use them.

Why does Outlook or another filter catch messages that are missed by SonicWALL?

Different vendors use different technologies to catch attacks. The system that is installed as the first filter will catch the majority of the spam, but the system downstream, even if very basic, will catch a few messages. While this may make it seem like a good idea to stack multiple vendor systems in a row, the result of this will typically be only a few extra spam caught, but a doubling of the good mail mistakenly caught, and increased complexity of management.

What about spoofed spam?

The new Anti-Spoofing set of features are SPF check (domain centric SPF enforcement), DKIM judgment and DMARC settings.

Sender Policy Framework (SPF) is an email validation system designed to prevent email spam by detecting email spoofing by verifying sender IP addresses. SPF records, which are published in the DNS records, contain descriptions of the attributes of valid IP addresses. SPF is then able to validate against these records if a mail message is sent from an authorized source. If a message does not register as an authorized source, the message 'fails.' You can configure the actions against messages that 'fail.'

There are two types of SPF Fails:

- SPF SoftFail - This occurs when the SPF record has designated the host as NOT being allowed to send messages, but the message is still allowed through to the recipient.
- SPF HardFail - This occurs when the SPF has designated the host as NOT being allowed to send messages and does not allow messages through to the recipient.

What is DKIM?

Domain Keys Identified Mail (DKIM) uses a secure digital signature to verify that the sender of a message is who it claims to be and that the contents of the message have not been altered in transit. A valid DKIM signature is a strong indicator of a message's authenticity, while an invalid DKIM signature is a strong indicator that the sender is attempting to fake his identity. For some commonly phished domains, the absence of a DKIM signature can also be a strong indicator that the message is fraudulent. The benefit of DKIM is it verifies legitimate messages and prevents against phishing.

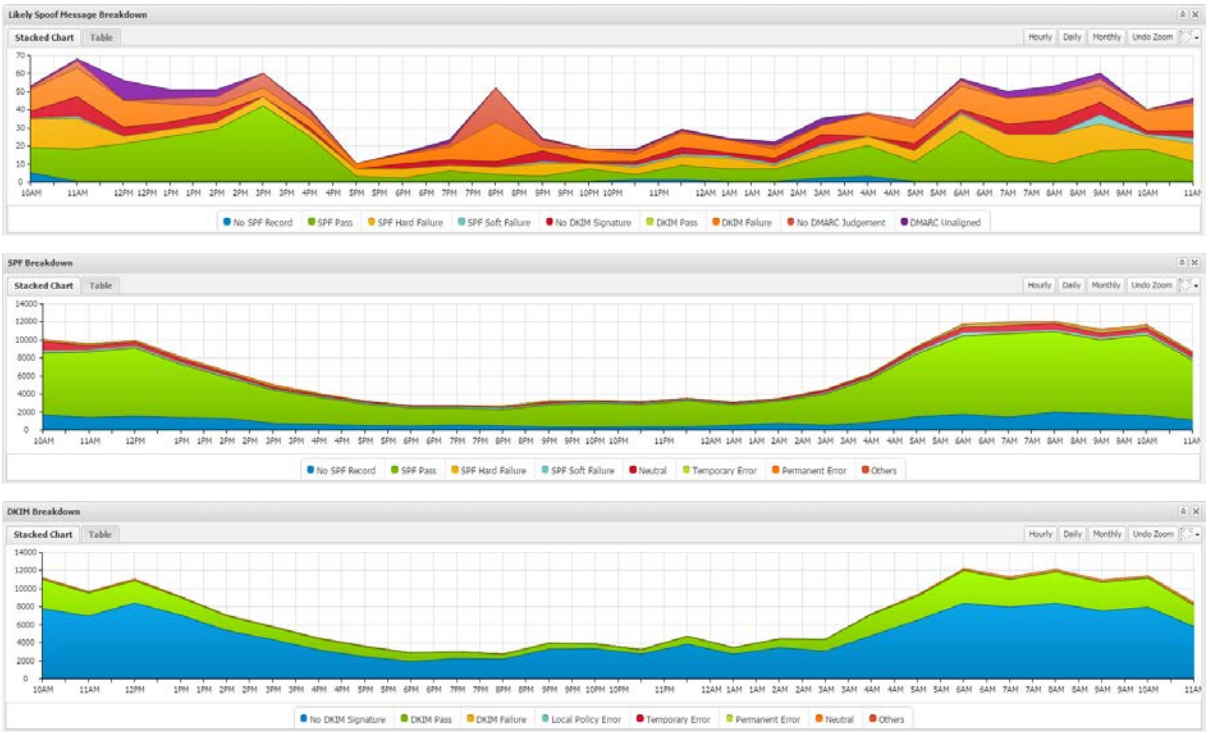
NOTE: DKIM does not prevent spam - proper measures should still be taken against fraudulent content.

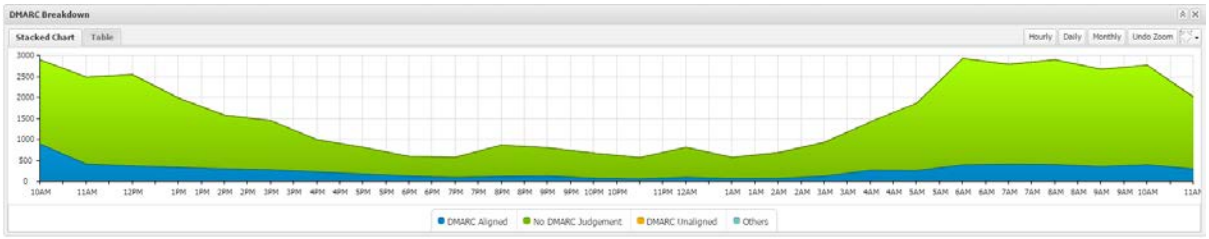
What is DMARC?

Domain-based Message Authentication, Reporting & Conformance (DMARC) is a policy that works in tandem with SPF and DKIM to fully authenticate incoming and outgoing email messages. A DMARC policy allows a sender to indicate that his emails are protected by SPF and/or DKIM, and also tells a receiver what to do if neither of those authentication methods passes, such as junk or reject the message. By default, the DMARC feature is enabled. You can specify the exact domain names to exclude from DMARC Policy Enforcement. The DMARC feature also allows you to specify domains for Incoming and Outgoing message reports.

Anti-Spoofing feature set reports

The charts below show the anti-spoofing features sets, such as spoof message breakdown, SPF, DKIM and DMARC.





What about image spam?

Spammers have recently started to use images in their spam to bypass filters. SonicWALL Email Security has added Image Thumbprinting, which considers image identifiers in the evaluation of messages. These image thumbprints are created by the SonicWALL SMART Network (over 1 million users worldwide) and through AutoJunking technology on SonicWALL honeypots and spamfeeds. SonicWALL Email Security pulls these thumbprints from SonicWALL datacenters to catch these image spams.

What about stock ticker spam?

Spammers are using “pump-and-dump” spam techniques to raise the value of penny stocks by spamming about their forecast increase in value, then quickly dumping them as their value increases. In SonicWALL Email Security, sliding the “Get Rich Quick” slider on the Anti-Spam > Anti-Spam Aggressiveness page to the highest setting “5”, will cause the system to strongly clamp down on stock ticker spam.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit http://www.software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call 1-949-754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to http://support.software.dell.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to http://software.dell.com/trials.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Last updated: 3/28/2016

232-003208-00 Rev A