Comparison Guide

Sendio vs Barracuda

Introduction

You've seen the research and read all the reports, and you likely have experienced dealing with malicious emails.

Now the time has come for you to fortify your defenses with an email security solution that will help stop spam and deal with the rise of cybercriminals who use sophisticated threats such as phishing to compromise your end-users.

In researching vendors that provide the type of protection your company's email systems require, Sendio and Barracuda have likely become possible candidates. Though both are known throughout the industry, there are some important differences between the two solutions that you must be aware of when making the final decision as to which vendor's offering is best suited to your company's needs.

When evaluating the email security systems offered by Sendio and Barracuda, you must consider the minimum criteria today's email security solutions require to effectively defend against the complex threat landscape you face:

Anti-virus protection against known malware delivered via email. One in every 2841 emails contains malware designed to compromise your users and network resources. Your email security system must be able to scan incoming messages for malware and update itself regularly to protect against the most current strains of malicious software.

Email scanning to identify embedded links to known malicious webpages. Just like attachments, malicious hackers have used webpages to compromise computers and accounts. By embedding a link to a malicious webpage, the attacker can send victims to a compromised website that infects visitors with malware or a forged website designed to steal login credentials. The ability for your email security system to identify known malicious links is another mandatory feature.

Protection against email spoofing. Cyberattackers can easily make an email look like the sender is someone trusted or known to the recipient. Look for products that offer protection against both inbound and outbound email spoofing.

Challenge/Response Email Filtering (Greylisting) for Unknown Senders

Email filtering solutions commonly work by blocking any email addresses that are known to be used by spammers and criminals (blacklisting), or by allowing any email that comes from trusted senders to be delivered to the recipient's inbox (whitelisting). Though these solutions are common in email filtering systems, they have some serious shortcomings. Blacklisting may seem like an ideal way to prevent emails that come from IP addresses and domains associated with known spammers. However, when spammers know that they are listed on one of the blacklists, they simply use new, clean domains. Because it costs less than $10 to register domains, they are never in short supply. Blacklists also present a problem to legitimate senders who are accidentally or mistakenly associated with one or more of the blacklists, which happens more frequently than you might expect. When this happens, legitimate emails from those on the blacklist will not find their way to the end-user.

A similar problem comes from relying on whitelisting. If you only allow mail from known, trusted domains and IP addresses, then you run the risk of a high number of false positives from those who are not on the whitelist.

> Greylisting is the answer to these concerns. With this technique, emails are held up for a short time. When this occurs, the sending server will not receive a response, so legitimate email servers will assume that something went wrong and resend the message. Mass mailers don't usually send the follow-up messages because of bandwidth use, so if your security solution doesn't receive the second email, it will know that the message is junk or harmful.

The Ability to Block Attachments by MIME Content-Type

Anti-virus scanning only works if there is a known signature to identify the malicious software or a known attack pattern to raise concerns about a possible zero-day attack. If the attack is completely unique and unknown, it may slip past these two countermeasures.

One way to prevent this is to block file types that are known to carry malware so any email attachments that contain these file types are not permitted. Some email security solutions will handle this by filtering by the file extension; however, this is ineffective because anyone can easily change the file extension to make the attachment look harmless. Instead, the more effective email security solutions block file extensions by their MIME content-type. This scans the file itself to identify its type rather than just the extension.

Two of the more well-known hosted email security solutions come from Barracuda and Sendio.

Choosing the Right Solution

Most vendors will claim that their products rely on the most cutting-edge technologies to stop spam and other types of malicious emails. The truth, however, is that most vendor offerings fall into one of two categories. The first is the group of vendors that rely on ineffective technologies such as content filtering and blacklists as their sole means of protecting the inboxes of the endusers. Content filtering and blacklists are both effective at stopping the low-level threats; they are mostly used by modern solutions to filter out the noise so their products can work to stop the real threats.

The second common type of email security system you may encounter is one that does a great job at identifying and stopping threats but is complicated to manage. These platforms may rely on complex configurations or require you to write up detailed rules to keep malicious email at bay. Often, these companies also offer some sort of certification for those who have mastered their complicated solutions.

If you want protection without having to study, this type of solution may not be for you, either.

Both products address the deluge of spam that businesses receive on a daily bases, and both work to keep email systems more secure against the myriad of attack methods that threaten them every day—but the two products take different routes to achieve this. Both provide protection using:

- Real-time message scanning
- Content Filtering
- DKIM Filtering
- Personal Quarantines

Barracuda

Spam

To scan messages and filter out spam emails, Barracuda relies on two different methodologies: Bayesian filtering and Realtime Block Lists.

Bayesian filtering is a mathematical technique that relies on probability to identify illicit email messages. Relying on what is known as a bag of words, Bayesian filters look at the words, and sometimes other heuristics, that make up the email message. Based on probability, it makes an assumption as to whether the message is spam or legitimate. For example, the words Viagra, stock, and mortgage are commonly found in spam emails. Keyword filtering would assume that the presence of these words makes the email spam and identifies it as such. However, legitimate emails may have these words as well, so Bayesian filtering takes the process a step further. By analyzing the other words in the content of the email message, it is able to mathematically determine whether an email is spam that should be quarantined or a legitimate email that should be delivered based on a score.

Realtime Block Lists (RBLs) rely on lists domains that are known to be used by spammers and phishers. Domain names or IP addresses are submitted by security professionals and email users alike. If the block list administrators have reason to believe an address should be included, it is added to the list. An email security solution that relies on RBLs will identify messages sent from these domain names/IP addresses as malicious and send them to the junk or spam folder.

Security

Barracuda's Spam and Virus Firewall product addresses the threats posed by attackers who spoof legitimate email addresses and send illegitimate emails that would be identified as spam or phishing attacks.

To prevent email spoofing, Barracuda employs a technology known as DomainKeys Identified Mail (DKIM). This checks the email message headers to identify the tag-value parts. Included in this is a digital signature that the email security solution can verify using the sender's public key. If the signature doesn't validate, or has been tampered with, the recipient's security system is alerted. Because a spoofed email won't have the appropriate digital signature, this countermeasure helps prevent these types of attacks.

Technologies Used

To protect the end-user from spam and malicious emails, Barracuda's email security system relies on the following technologies:

- Content Filtering
- Inbound DKIM Filtering
- Zero-Hour Anti-Virus Protection
- Real-Time Message Scanning
- Personal Quarantines

Barracuda also provides operators with a Web-based management console capable of producing a number of reports and the ability to manage events at both the domain and account levels.

Pros and Cons

Although Barracuda does provide a robust management console and the ability to actively scan messages in real-time for both suspicious content as well as malware, it does rely on older filtering techniques such as Bayesian filtering, which has been known to cause false positives.

Take, for example, the case of Franklin D. Azar & Associates.4 In 2007 the Aurora, Colo., law firm was receiving massive amounts of pornographic spam on a daily basis. To stop the offensive emails, the IT administrator tightened up the controls on its Barracuda Spam Firewall, and the deluge of spam began to drop significantly. Unfortunately, when they made this change, messages from the United States District Court for the District of Colorado were also blocked by the firm's spam filter. Included in these blocked emails was a notice from the court alerting lawyers as to the date of a hearing in a civil lawsuit. Because no one in the firm saw the email notification, no one showed up to court on the assigned date. The judge overseeing the case ordered Azar & Associates to pay attorneys' fees and expenses for the other side and publicly criticized the firm.

PROS

PRO: Barracuda does employ DKIM inbound filtering to verify that the content of the message has not been altered and that the message was, in fact, sent by the owner of the domain

CONS

This is an important step in identifying emails that have a spoofed sender address, but it does little to stop spam because spammers themselves have the ability to set up a DKIM signature for their messages as well.

CON: The absence of DKIM outbound filtering is a cause for concern with the Barracuda Spam Filter because it leaves your email domains susceptible to spoofing. Using public key cryptography, DKIM allows you to digitally sign your emails so when your email filtering service applies this digital signature to your outgoing emails, recipient servers can validate that the email came from the domain it claims to have originated from, and that the content is the same as when the email was originally sent to prevent man-in-the-middle attacks.

CON: The lack of SPF and DMARC should cause further concern because without them, your spam filter does not offer fully layered protection against emailborne attacks in which the threat has spoofed a legitimate email address or domain. SPF technology allows domain owners to publish the IP addresses that are allowed to send emails from specific domains. Spammers and phishers can easily make a sender address look like it comes from anyone they want. The absence of SPF technology leaves the spam filter without the ability to perform a basic check to ensure that an email originates from the sending domain it claims to be from.

CON: Without integrated DMARC technology, your email spam filter won't know what to do with SPF and DKIM failures. Email spam filters that leverage DMARC allow domain owners to publish policies that receiving email servers consider when handling SPF and DKIM failures. The information these recipient servers send back to the sender positions them to take action if there is a problem with their sending postures or if their domains are used in emails that are spoofed.

CON: Another area where this spam filtering comes up short is due to the enduser being left out of the equation. When relying purely on technical controls, there is the likelihood that harmful emails will be improperly identified as legitimate, known as a false negative, or a legitimate email will be identified as spam, known as a false positive. This happens when the threshold for the spam identification score is set too high or too low. Without a highly trained, experienced administrator to manage the email security solution, it takes time for everything to be set just right. This process of trial and error also puts a company at risk for some potential problems.

Sendio

Spam

To spot low-level spam, Sendio does actively scan the content of incoming messages for junk emails; however, its protection against illegitimate email goes much further than that. Rather than relying on Bayesian filtering and RBLs, Sendio's protection comes from the layers of protection offered by its large feature set along with its reliance on a unique email community paradigm.

A community is built by exporting all of the contacts from the mail server and then loading them into Sendio. Next, the contacts from your company's CRM solution and accounting system undergo the same process. Finally, the personal contacts of your users are added. After the initial setup, the community is self-managed by the user. If an email is sent to a person not included in the community, that email address is added to the user's individual community. If someone sends a message to a user that is not in the recipient's community, the message is put in a queue and the sender is invited to join that user's community. Messages from verified community members will always make it through to the recipient's inbox.

In addition to its community, Sendio also relies on a challenge/response technology called Server Recon as well as Sender Address Verification to ensure that emails arriving from unknown senders who are not in the community are actually sent by real mail servers and people instead of spambots. Because this technology requires action by senders to verify their authenticity, social engineering and automated threats are almost completely eliminated.

Security

Like other email security systems, Sendio actively scans emails for malware and frequently updates its anti-virus database to ensure it is able to spot even the most recent malware signatures. However, it takes malware protection even further by allowing the operator to block emails with attachments known to house malware. Yet because criminals can easily change the file attachment's extension to make it look harmless, Sendio also checks the S/MIME content to see the exact file type of the attachment. If it is one that should be blocked, it will not be delivered—even if the extension claims that the file is safe.

To protect against email spoofing, Sendio uses a layered approach relying on inbound and outbound SPF and DKIM technologies not only to ensure that incoming mails are not spoofed, but also to protect your reputation by stopping criminals from spoofing your domain.
To fill in the gaps, DMARC technology is also used to help your servers, as well as others, easily authenticate email messages.

Technologies Used

The Opt-Inbox and Email Security Gateway combination protects the mail systems using:

- Content Filtering
- Personal Quarantines for Users
- Both Inbound and Outbound SPF Protection Against Email Spoofing
- Inbound DKIM Filtering
- A Greylisting Technology Using SMTP Challenge Filters (Known as Silverlisting)
- Zero-Hour Anti-Virus Protection
- Challenge Response Email Verification
- DMARC Protection
- End-User Whitelisting and Blacklisting
- Real-Time Message Scanning
- Message History

Pros and Cons

Sendio's email security system offers a much more robust, multi-layered approach to protecting the inbox from harmful email messages.

PROS

PRO: With an easy-to-manage console, false positives are reduced, and the use of communities even further protects against legitimate emails being accidentally labeled as spam. The inclusion of end-users provides an added layer of protection and encourages them to participate in your organization's security.

PRO: Rather than simple blacklisting and whitelisting, Sendio relies on a greylisting technology it calls Server Recon. Server Recon is a challenge/response check that holds back the delivery of an email message. If the sending server notices that the delivery failed and resends the message, Sendio knows that this may have come from a legitimate email server and sends it on for further processing. If no second email is sent, then the sender is assumed to be a spammer.

PRO: Rather than whitelisting, Sendio relies on communities of known legitimate senders. Contacts from the CRM solution, accounting software, and individual user contact lists are added to a safe community. Emails verified to have come from these senders are always let through, and anyone not in the community is given the opportunity to join using Sender Address Verification (SAV), in which an email is generated asking senders to click a link in the reply to verify who they are.

CONS

CON: Some do see this as a drawback because the users must be trained on how to spot malicious emails, and you do have to get them to actually use these features to make Sendio's protection even better. However, if you are able to successfully train users on how to spot suspicious emails, and then reinforce this learning, your end-users will be less likely to fall victim to social engineering and phishing attacks because they will know what to look for and how to deal with it.

Central DuPage Hospital Case Study

One company that saw the benefits of Sendio's Server Recon and SAV technologies was Central DuPage Hospital. With more than 4,000 end-users, this suburban Chicago-based hospital's IT director, Glen Malan, described the amount of spam received on a daily basis as "astronomical."

The need to block these unwanted messages was compounded by the need to ensure that legitimate emails were not designated as spam. Being a healthcare provider, this presented a unique problem. As Malan explained, "We were concerned that filters would not be able to differentiate between fake 'Viagra' emails and valid email with 'Viagra' in the subject."

Citing Sendio's Sender Address Verification and Server Recon as the most prominent features, Malan claims that the inflow of spam email has now dropped to an undetectable level.

Additional Information

Migrating Security Solutions

Migrating to a new vendor or solution is usually a large step to take, requiring a great deal of project planning, dedicated resources, and buy-in from the rest of your company. On the technical side of things, this process includes:

- Configuring the new solution so that your email and users see no loss in protection
- Reconfiguring your network so that inbound and outbound emails are routed through the new solution
- Testing to ensure that emails are being delivered and sent
- Reviewing emails to ensure that false positives and false negatives are within acceptable levels

To help manage these processes, consider the following tips:

Get the right people trained on the management console for your new solution. Make sure they are familiar with the user interface and the steps required to successfully implement this migration. Even if you are using a hosted security solution, someone in your company must understand how things are being set up and configured.

Identify all domain and email server parameters you will need to configure the inbound and outbound paths between your email servers and your new security solution. This will likely include your A records necessary to map hostnames to IP addresses, and MX records to map domain names to the mail transfer agents for that domain.

Test everything by sending emails internally, once you have configured your servers and the new security solution, and also send emails from your company email address to an outside free email service as well. If the audit logs show the email as delivered, and the email is successfully delivered, then you know outbound delivery is working. Next, send an email from that same free account to your company email to see if inbound email is working as well.

Adjust your email security solution to meet the security requirements of your company. Be sure to set filters appropriately, confirm that anti-virus components update frequently, set up email spoofing protections, and make sure that whitelisting and greylisting is configured so that legitimate emails are delivered appropriately.

Keep an eye on everything. Even though things might be working, there are no anomalies or settings that may prevent legitimate emails from reaching their destination inbox.

Keeping the End-User Informed

Though the technical tips may help you make sure that everything is configured correctly, keeping the end-user up to date about these changes is the most important step you can take to ensure the project's success. By training users on what changes to expect, how to use the new features of the solution and how this change will benefit them helps keep them engaged in the process. As they grow more comfortable with these changes, they will eventually become champions for your new security system.

Over the past 10 years, Sendio's Opt-Inbox and Email Security Gateway have helped many companies eliminate their spam problems without the worry of marking legitimate emails as harmful. To see how these products can help your company better protect the inbox and effectively deal with spam, sign up for a demonstration and get your spam problem under control.

[1] "What's in Your Inbox ?" What's in Your Inbox ? 7Safe, 18 June 2015. Web. 7 Sept. 2015.