SPAMjadoo

Never See another SPAM again

(along with FAQ)

Overview

Spamjadoo offers complete protection to prevent spam from entering your email server. Based on a unique Privacy paradigm, it is vastly superior to content-filter based products.

Other products encourage spammers to try new ways to sneak into your mailbox. The result ? More spam, more threats, more attacks, more effort by network admin and users.

Spamjadoo is the only antispam product that actively discourages spammers. Our ESP technology spreads a privacy layer around your mailbox that results in spammers taking you off their database and the amount of spam targeted at you reducing with time.. Other anti-spam products check the mail AFTER receiving it – this encourages spammers to try harder, which results in more spam, more traffic, more server loads

The multiple checks that are run includes DHA, SPF, SMTP Auth, reverse DNS, blacklist/white list check, Senders Domain MX check, Blocking of specific attachments, and many more along with its proprietary ways to stop spam.

Features

ESP (Eliminate Spam at Protocol level):

SpamJadoo uses the revolutionary ESP technology to build an unbreakable, fool-proof privacy layer around your mailbox. ESP allows Spamjadoo to stop spam before they enter into the email server.

Directory Harvest prevention:

Spamjadoo tracks email spammers with invalid emails and count them automatically. Spamjadoo is capable to diagnose these attacks automatically and the moment it diagnoses the attack, it stops the response for that particular IP address immediately. It all happens automatically without any administrator's intervention... magically!

Email Traffic Control (Rate limit) :

Spamjadoo has Ip based, Domain based rate controls and also limits the Maximum number of simultaneous sessions allowed from each unique IP and Senders email id.

Virus protection:

Spamjadoo has integrated antivirus engine which detects viruses, worms and trojans, including Microsoft Office macro viruses, mobile malware, and other threats. built-in support for various archive formats, including Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS and others . Extra file extension blocking facility for know suspicious extensions.

Spamjadoo content analaysis:

Spamjadoo content filter inspects each and every email and declares an email as a spam on the bases of score , phrase and special links .

SPF: Senders Policy Framework

Spamjadoo has inbuilt e-mail authentication protocol that verifies the origin of the e-mail and prevents forged mail from entering an organization. In essence, Spamjadoo using Sender ID framework asks a question: Has this e-mail message been spoofed If the answer is Yes, it has been spoofed, the Spamjadoo rejects the message immediately. If the answer is ? No, we can confirm the sender´s authenticity,? the message is assigned a SPF status and gets accepted for further checking by Spamjadoo.

SMTP Auth: Authenticate before SMTP

SMTP-AUTH extends SMTP to include an authentication step through which the client (outlook / thunderbird) effectively logs in to the mail server during the process of sending mail. Servers which support SMTP-AUTH can usually be configured to require clients to use this extension, ensuring the true identity of the sender is known. Spamjadoo follows the SMTP-AUTH as defined in RFC 2554. Server Administrator may use this to avoid phising and unwanted email traffic from his organisations own network.

Reverse DNS , MX /A record check :

Spamjadoo uses Reverse DNS lookups for IPV4 addresses through special domain in-addr.arpa. An IPv4 address is represented in the in-addr.arpa domain by a sequence of bytes in reverse order, represented as decimal numbers, separated by dots with the suffix .in-addr.arpa. While receiving email from a specific domain, Spamjadoo is capable to check whether the sender domain has a valid DNS record

having A or MX entry, and in case it does not have, spamjadoo can block it. This setting may be configured by administrator and can be applied for all the domain configured on the server. The also happens at protocol level... magically !!.

Challenge-Response

As integral part of ESP, automated challenge-response system is another highlight of ESP – genuine (but as yet unknown) senders can validate themselves with a couple of clicks and keystrokes. This works transparently to the recipient, and cannot be performed by spam engines.

JMail accounts

The JMail sub-system is another unique, revolutionary and thoughful feature of ESP. It allows custom JMail accounts to be created as programmable extensions to your mail account, and rules to be assigned to each such account. You can then invite trusted senders into your mailbox without compromising your privacy. Even if a trusted sender's computer is hacked, or address book data (including your JMail id) is stolen, the JMail account is not accessible to anyone else without your permission. And the JMail accounts can be configured by you in a variety of ways to support common usage scenarios – newsletter subscription and online shopping are just two examples.

Spamjado spam-quarantine: Safe hold place for spam mails, manageable by users and administrator. It gives Email Tagging, Quarantine and Blocking facility.

Dashboard (GUI): Enable configurable login for better control on email account against spam emails. Full featured GUI with multi-level (user/domain/server) login accounts and capable of secure web based remote administration. SNMP MIB Provides detailed analysis and system status that shows the administrator the health and information statistics of hardware and resources

Complete logging and detailed stats: powerful logging enables administrators and support persons to track each and every email and to quick answer to end-users "exactly what happened with the email".

Parameters

Server Level (will be applicable to all domains globally)

Mail Size (MB) :
If mail size is more than specified size than mail will be rejected.
Config : Parameter in Serverconfig.txt - Admin Access

Max Recipients:
if recipients are more than specified numbers than mail will be rejected.
Config: Parameter in Serverconfig.txt – Admin Access

Mail Queue Period (Days):
Spamjadoo will try to deliver mail till specified days after specified days it will bounce mail to sender.
Config: Parameter in Serverconfig.txt – Admin Access

Reverse MX checking of Sender IP:
If selected "YES" & sender server IP is not having reverse MX setting then mail will be rejected.
Config : Web Dashboard – Server Level Settings

Reverse Domain checking:
if selected "YES" & sender domain's A or MX record not found then mail will be rejected.
Config: Parameter in Serverconfig.txt – Admin Access

Virus Checking (ClamAV):
If "YES" & virus found in mail then all content of mail will be removed
Config: Parameter in Serverconfig.txt – Admin Access

Virus Notification Mail to Recipient:
If Virus found in any email recipient will be notified.
Config: Parameter in Serverconfig.txt – Admin Access

Daily notification mail of Unknown Sender:
If parameter value is set to 1 than all the users on the server will get Unknown Senders notification email. Which means user will be know about the senders list, whose emails have been rejected.
Config: Parameter in Serverconfig.txt – Admin Access

Quarantine list mail time interval (from 00:00 Hrs):
Define the time of interval in between two quarantine email alerts sent to user.
Config: Parameter in Serverconfig.txt – Admin Access

Sence Directory Attack (DHA):
If Spamjadoo identifies directory attack on the server, *all incoming communication from that IP will be stopped. Exception - only local users having SMTP-AUTH can send mail.*
Config: Parameter in Serverconfig.txt – Admin Access

DHA Shelf Life:
Once Spamjadoo puts any ip in DHA block list, after the specified Shelf Life only the connections from that IP will be accepted.
Config: Parameter in Serverconfig.txt – Admin Access

MAXSESSION :
If Maxsession parameter value is set to 1. Spamjadoo will not accept simultaneous emails from the same userid + IP .
Config: Parameter in Serverconfig.txt – Admin Access

SMTP Auth :

If set to "ON" then local users not using SMTP-AUTH in their email client will not be able to send email.

Config: Parameter in Serverconfig.txt – Admin Access

Black List IP:

Put an IP address or range of IP address in the blacklistIP.txt to permanently block connections from these IP addresses.

Config: Parameter in BlacklistIP.txt – Admin Access

White List IP:

Put an IP address or range of IP address in the WhitelistIP.txt file to permanently accept connections and emails from these IP addresses.

Config: Parameter in WhitelistIP.txt – Admin Access

Black List Domains:

Put Domain name or domain names in the blacklistdomain.txt to permanently block email from these domains.

Config: Parameter in Blacklistdomain.txt – Admin Access

White List Domains:

Put Domain name or domain names in the whitelistdomain.txt to permanently accept email from these domains.

Config: Parameter in WhitelistDomain.txt – Admin Access

Host Allowed IP :

Enter List of internal host IPs in hostallowed.txt , from where you would like to accept mail without SMTP-Auth. (normally web servers or your e-billing / news servers)

Config :Parameter in HostAllowed.txt – Admin Access

Internal Relay :

If parameter switched on than Spamjadoo will allow mail-from external domain if sender ip is internal and SMTP Auth is enabled.

Config: Parameter in Serverconfig.txt – Admin Access

DNSBL:

DNS based block listing services may be integrated with Spamjadoo by setting this parameter and configuring zone.txt file.

Config: Parameter in Serverconfig.txt – zone.txt

Email transfer rate limit:

Email transfer rate limit on the basis of Sender server IP address.Control the email traffic from each server IP.

Config: Parameter in Serverconfig.txt – LimitOnIP

Configuration Settings : Domain Level (will be applicable to individual domain)

Number of days to keep quarantine mails:
Define number of days after that quarantine emails will be deleted automatically.
Config : Web Dashboard – Domain Level Settings

Number of days to keep unknown senders list:
Define number of days after that Unknown senders list will be deleted automatically.
Config : Web Dashboard – Domain Level Settings

Unknown sender's mail append text :
When Spamjadoo receives an Email from an unknown sender, it can dynamically add the Specified word into the subject of the email.
Config : Web Dashboard – Domain Level Settings

Number of Maximum users in a domain:
After reaching at limit no more local user will be added to dashboard hence its address book will not be generate but mails incoming & outgoing will be continue for those users.
Config : Web Dashboard – Domain Level Settings

SPF (Sender Policy Frame) checking:
If enabled and based on the settings , SPF check will be applied on each email and response will be given by Spamjadoo accordingly.
Config : Web Dashboard – Domain Level Settings

Allow External :
If Spamjadoo is set to *allow internet domain emails from external IPs, than only an internal user from external network using SMPT AUTH will be able to send emails. Any IP which is not configured in hostallowed.txt is considered as External.*
Config : Web Dashboard – Domain Level Settings

Validation Method : SMTP ,Bounce, Forward
How do you want to handle email that is sent to an address that is not present on Spamjadoo Mail Server?

> **SMTP. Attempt to validate the destination email address against the incoming POP3 server specified above. If the POP3 server will accept the address, then accept the incoming email, otherwise reject the incoming email with a "no such user" error message.**
>
> **Bounce. Reject the incoming email with a "no such user" error message.**
>
> **Forward. Perform no further checks and unconditionally forward the email to the POP3 server**

Config : Web Dashboard – Domain Level Settings

Grey List Period:
If Greylist / Medium mode is on and unknown sender sends an email. 450 (mailbox temporarily unavailable) response to the senders server, if sender server retries after specified minutes , the

email will be received and delivered to recipient.
Config : Web Dashboard – Domain Level Settings

Attachment Type Block *e.g. exe, pif, scr*
Emails having attachment with Specified extensions will be blocked.
Config : Web Dashboard – Domain Level Settings – Advanced Settings

Auto Add Users :
If you want users to be configured on Spamjadoo automatically, you can set this feature on.
Config : Web Dashboard – Domain Level Settings – Advanced Settings

LDAP Integration:
Spamjadoo can communicate with LDAP to verify the internet users validity before receiving email.
Config : Web Dashboard – Domain Level Settings – Advanced Settings

Disable Dashboard Login:
If you want to disable users from login into the dashboard, you may set the value to Yes.
Config : Web Dashboard – Domain Level Settings – Add / Edit users

Configuration Settings : User Level (will be applicable to individual User)

WhiteList :
User can add known senders emails address in his white list . All mails will be allowed in his inbox from these ids. While adding, you can define the emails as Spamjadoo and unknown too.
Config : Web Dashboard – User Level Settings – Add to Whitelist

Bulk Import address book :
If you have a address book list in CSV format , you can directly import the list of email ids and define them as Friend, Spammer or Unknown.
Config : Web Dashboard – User Level Settings – Import

Email Alias :
User can create virtual email address attached to their parent email id. Example: If parent id is Sonia@spamjadoo.com , the alias may be Sonia.web@spamjadoo.com .
Config : Web Dashboard – User Level Settings – Add Alias

Jmail :
Programmable and Disposable Email address may be created attached to their parent email id. *User can create Jmail ids with its own policies.*
Config : Web Dashboard – User Level Settings – Add Jmail

Status :
User can configure his account status himself and let Spamjadoo work according to the settings done by him for his account / email id. He can choose, High – Medium – Low – Learning – None , as per his choice.

FAQ *: to solve some of your questions you may have*

Q1. What category does Spamjadoo fit into ? Does it filter ? Is it challenge-response ? Is it disposable mailboxes?

Ans. It is a completely new approach to spam elimintation, based on the provacy principle. Its innovative **ESP** (**E**liminate **S**pam at **P**rotocol level) technology incorporates some traditional methods, but it should be seen as of a completely different genre – let's just say it is a new class of anti-spam products.

Q2. How is this different and better than everything else out there?

Ans. Spamjadoo is the only product that works at the SMTP protocol level, and hence can block spam even before it can be sent ! It is the only product that provides you the best of all worlds – you get no spam, you never lose a mail from a trusted sender, and you need to make virtually no effort.

Q3. Will this work with my email software like Outlook, Eudora or Entourage?

Ans. YES! SPAMJadoo works with ANY email client because it runs at the mail server level which also means that you don't have to install any software on your PC.

Q4. What is a JMail box?

Ans. It's a virtual email box that looks and works like any other mailbox, except that you decide how it can be used by assigning rules to it.

Q5. How does it work?

Ans. A JMail address is a rule bound email address which lets you make rules on who can send you email. Any sender that violates your rules is not allowed to send email to you.

Q6. Is a JMail account complicated to use?

Ans. Not at all. You just use email the way you normally do. Except you can create different JMail addresses. And give these out when you need to, for example when a Web site asks for your address. Now you're in control.

Q7. How does it prevent companies from selling my email address?

Ans. It doesn't prevent them from selling your address, but it makes your JMail address worthless to the company that paid for it. This is because you can create a JMail and specify as it rule : "this can be only used by the company I give it to". And it won't work for any company that violates that rule.

Q8. How does SPAMJadoo know if someone is violating my conditions or not?

Ans. JMail addresses are smart as their usage is tracked by a database and anyone that uses the email address, is compared against those that have already used it. Your policies are applied against this collection to determine whether or not the email should be accepted.

Q9. What can I do if I start getting unwanted email?

Ans. That's really up to you. Lets say for instance you subscribed to a newsletter that did not respect your subsequent request to unsubscribe. All you do then is simply disable that JMail and they are gone. If that JMail is being used by many other people or company that you don't want to affect, you can just disable the JMail for that one company. If you created a "wide open" JMail, you can just lock it, and the people that used it can continue to use it, but no one else can.

Q10. How do I protect my existing email address?

Ans. You decide and can change your mind anytime. If you have an old email address that gets a lot of spam, you can request that anyone you don't know first prove they are person and not a mass-email program before they can send you mail.

If you have a new email address that does not get spam but you want to protect yourself against future spam and unwanted email, you can continue using your regular email address alongside new JMail addresses you create for various reasons.

Q11. Why is this better than aliases or "disposable" email addresses?

Ans. You can't assign a usage policy to an alias. Aliases don't enforce your policy by bouncing violating email. You can't stop someone from using an alias. But you can do all these things with a JMail address.

The problem with disposable addresses is that the only thing you can do is dispose them. And when you do that, you stop getting all the good email that is normally sent to that address !

You can use a JMail address just like a disposable, except that when it gets tainted you don't have to dispose it off. In fact, you continue controlling who can use it, when, and how, via policies. This

means that if a JMailbox starts getting unwanted mail, you can lock it down and stop unwanted mail yet continue receiving mails from senders you trust.

Q12. How do I subscribe to newsletters and order confirmations?

Ans. Easy. Just provide a JMailbox address to the newsletter or ecommerce web site – if you want to use a new Jmail address, first create it using the web dashboard interface. Newsletters and order confirmations flow straight to your inbox. You don't have to know their email address in advance or anything.

Q13. Can I get email from legitimate people I don't know without forcing them to use Challenge/Response?

Ans. Of course! Just give out your appropriate JMail address. Else, set the spam control setting to a more tolerant level.

Q14. How many JMail Addresses can I have?

Ans. As many as you want. There’s no limit.

Q15. What kinds of policies can I assign to my JMail Address?

Ans. There's a lot of variations. Basically you can make a JMail work for a given company only, a given person only, a number of companies, or a number of people. And you can "lock" a JMail which only lets in those that used it already (and no one else), disable a JMail so that no one can use it, or disable a JMail after a certain number of days.

Q16. How does Spamjadoo stop spam before it's even sent?

Ans. Email is sent in two steps: In step one, the sender connects to your email server and tells it your address and their address. In step two, your email server allows the sender to transmit the email contents. SPAMJadoo never lets spammers (or anyone else that doesn't respect your policies) get past step 1.

Q17. What happens when spammers get a hold of my JMail Address?

Ans. That depends on the policy you have in effect. For example if that JMail has a policy to be used only by the organization you gave it to, then spammers can't do anything with it.

If you have an "wide open" policy on that JMail, then when you do receive your first spam, you can change the policy on your JMail making it unspammable. For example, you can "lock" it so

that only those that have already used it can continue to use it. Or if you want to be a little more flexible, you can require that new senders prove they are a person.

Of course, you can always disable it, but you don't have to be that severe because you have a lot more control than ever before.

Q18. How does this install in our network?

Ans. SPAMJadoo becomes your organization's primary MX and then it relays clean incoming email to your existing email servers. Outgoing mail has to pass through SPAMJadoo which then relays it through your existing email server for final delivery.

Q19. Do all our users have to use it?

Ans. NO! Each user can make their own decision if they want to stop spam or not. And each user also gets to decide how to stop spam. You can have as few as one, or as many as all of the users within a given domain.

Q20. How do users get started?

Ans. Users self-subscribe via a Web interface. We supply utilities that allow them to upload their white list of known senders. Users are advised usually to use SPAMJadoo in a "passive" mode that shows them which email will get rejected and which mail will come through without actually acting on it. Once the user feels comfortable that SPAMJadoo is doing its job, they flip a switch and spam is gone forever.

Q21. How do users control the product?

Ans. Spamjadoo is controlled by a Web interface that supports end-user, domain administrators, and server administrators. Practically everything is run from the Web. Most of the control, however, is automatic, as SPAMJadoo builds its database from user policies and email sent and received.

Q22. Can Spamjadoo stop Viruses and Worms too?

Ans. Spamjadoo can integrate with any SMTP level antivirus or command line virus scanner like CLAM and stop the viruses before it gets into the email server.

Q23. Can I talk to few customers and take their feedback about Spamjadoo?

Ans. Yes, we will be happy to align you with desired customers and you are free to talk and take

feedback. You may also see testimonials section for your satisfaction.

Q24. Do you have any industry recognitions for Spamjadoo?

Ans. Yes, IBM has showcased Spamjadoo in all industry verticals on IBM Site.

See at http://www-304.ibm.com/jct09002c/gsdod/solutiondetails.do?solutionId=22958&lc=en on IBM site.

You may also like to visit news and articles sections for latest news..

Q25. What is the maximum numbers of emails per day Spamjadoo can handle and has been tested?

Ans. Spamjadoo has been tested and running live to handle more than 2 million emails per day with over one lac (100000) users.

Q26. What is the hardware configuration required for five lac emails per day?

Ans. To handle approx. five lac (500000) emails per day with an average size of 100KB per mail, server class machine with DUAL CPU XEON / PIV with 2 GB RAM will be sufficient.

Q27. Do you provide email / telephonic support?

Ans. Yes, we do provide 8 hours standard hours support FREE to all our customers and after that if you desired 24x7, its available with additional cost and contract.

Q28. Can spamjadoo block emails having unwanted attachments like EXE or PIF ?

Ans. Yes, If you do not want emails with some attachments like PIF or SCR extension, Spamjadoo can block emails with those specified attachments.

Q29. Do you provide hosted antispam service also?

Ans. Yes, contact us, we will provide you the hosted antispam solution.

Q30. Can I block emails having specific keywords into the message?

Ans. Yes, Spamjadoo also has filtering engine, and can stop the messages before they successfully

get received by Spamjadoo for delivery to Inbox. The settings can be done by domain administrator.

Q31. Do we get latest filtering technology like Bayesian with Spamjadoo.

Ans. Yes, Spamjadoo comes fully integrated with Bayesian filtering technology. This Bayesian filtering engine is fully integrated with Spamjadoo and works just before the email is about to deliver to Inbox.

Q32. We are hosting multiple domains for emails and we want to control the traffic of emails for each domain. No email server provides the rate control facility. Can we do the rate limits to control the traffic for any domain?

Ans. Yes, We call it traffic control feature into Spamjadoo. You can set a domain level setting and configure Spamjadoo to receive only limited number of emails for the specific domain in a particular day/hour/minute.

Q33. We don't want to receive unlimited number of emails from a particular IP addresses. We want to control that how many emails one unique IP can send to us. Can we control this?

Ans : Yes, you can control number of emails to be received in a particular minute from unique IP address. Server can automatically keep control over the traffic each IP and if traffic is more, Spamjadoo can force the sending IP to queue at their level and resend after predefined interval. This is great feature in ISP and Hosting Company like scenario.

Q34. We don't want to allow unlimited number of emails sent from an internal user. We want to control that how many emails every email address can send to others. Can we control this?

Example: My internal domain is mydomain.com and my users like users@mydomain.com should not be allowed to send more than 200 emails a day**.**

Ans. Yes, you can control number of emails to be sent by every internal email address. Spamjadoo gets notified by its uniquely designed log-parser-plugin for the count of emails sent by the outbound SMTP and Spamjadoo uses that notification to block the further sendig of the emails. This is great feature in ISP and Hosting Company like scenario, where users start using the service provider SMTP servers for unlimited spam.

Q35. We don't want to allow emails to be sent by unauthenticated users. We want them to authenticate and then only they should be allowed to send the email. Can we block emails which are sent by unauthenticated users.

Ans. Yes, just enable "Allow External" on domain settings using dashboard control panel for your domain and enable SMTPUTH in Server Configuration file. All the emails sent by yourdomail.com will be subject to authentication from SMTP server. SMTP-AUTH supports PLAIN LOGIN and secured password authentication using CRAM-MD5, DIGEST-MD5, NTLM . SPAMJADOO IS UNIQUE ANTISPAM TO OFFER CRAM-MD5 , DIGEST-MD5, NTLM for outbound emails.