

SMTP Scanner Creation GWAVA4

Copyright ©2009. GWAVA, Inc. All rights reserved. Content may not be reproduced without permission. <u>http://www.gwava.com</u>

SMTP Scanner

SMTP scanners allow the incoming and outgoing mail to be intercepted, scanned, and filtered completely independent of the mail system. This setup has the distinct advantage of relieving the mail system of unnecessary and unwanted traffic, leaving mail system resources open to function with greater performance and security.

The SMTP interfaces add a layer between the GWIA, or any other mail system's SMTP sending agent, and the internet. Sending mail is forwarded through an SMTP proxy, which then sends the filtered, clean mail to the original recipient. Incoming mail is scanned via the SMTP scanner, which then sends the filtered and clean mail to your mail system, unaltered. These scanners allow GWAVA to act independently of your mail system.

Creating a SMTP Scanner

The SMTP scanner will only work if your MX record points to the GWAVA SMTP interface for mail delivery, and if your domain and mail system SMTP are listed correctly in your GWAVA system.

GWAVA SMTP will then forward the clean mail to the SMTP Gateway specified during server activation. To view or change the domain and SMTP for your Mail system, go to Server/Scanner Management | <Server Name> |Server Management | Configure Server.

GWAVA 4		
Home GWAVA.com Support Help Logout	Server Configuration	
Velcome Recorded webinars	GWAVAMAN root directory Show Advanced Connectivity Settings	/opt/beginfinite/gwava/
Computer based training T Quick install guide G Quarantine manager	Log level Normal V Keep log files for 7 days	
Bookmarks	Default internet domain for this server	gwava.com
System Management	Mail relay agent SMTP Server	192.168.1.101
Server/Scanner Management	Mail relay agent SMTP auth login name	chris
🖃 📁 gwava-iso (Linux)	Mail relay agent SMTP auth login password	
Gerver management Server statue	Administrator e-mail address	admin@gwava.com
Configure server	Administrator Full Name	admin
Appliance control	Show Advanced Message Relay Settings	
GigSpan / PRep agent setup Cogs (Clicensing ⊕ ∠ Wizards ⊕ ∠ Manage scanners	Additional internet domains	Remove Domain
	New domain Destination SMTP host	Add Domain
	Proxy Server Configuration	
	QMS SMTP Authentication Server	192.168.1.101
	 Enable QMS data pruning 	
	Days to retain messages in QMS	30 days
	Prune stored messages	
	Prune database entries	
	Backup and maintenance time	02:00
	Show Auvanced QMS Seconds	

The Mail relay agent SMTP Server and Default domain MUST be Correct for your system. If you have multiple domains, list the additional domains. GWAVA will only accept mail for the listed domain(s).

The Scanner creation wizards, (found under Server/Scanner Management | <Server name>| Wizards | Install/create new scanner), walk through the steps and information required to install the different scanners for your system. Select the SMTP Interface scanner and follow the instructions to install the scanner.



To install a SMTP scanner, select the SMTP scanner option from the wizard and click next.

The SMTP scanner creation wizard informs you of the information you must know to successfully create the scanner.

*	Create new SMTP scanner
	Welcome to the SMTP scanner creation wizard.
	To ensure a smooth installation of this interface, some information about your mail system needs to be supplied. You may also undertake some of these steps manually after the GWAVA network has been configured if you wish to maintain control of the process yourself.
	Prerequisites:
	 Configure your network or MX records so that the GWAVA SMTP interface receives your SMTP mail. Configure your outbound SMTP mail to point to the GWAVA SMTP interface (for outbound mail scanning). Know the IP or DNS address of your SMTP server. Know the internet domains that GWAVA will be handling mail for. Know the internal/external IP addresses to determine inbound/outbound mail flow.
	Post install:
	There are no post installation requirements.
	Continue

The **Scanner Name** is whatever you wish the scanner to be named in the GWAVA server.

The **IP listen address** is the address of the GWAVA Appliance. This should also be listed on the MX record for your domain.

Allowed relay addresses are the source addresses

*	Create new SMTP scanner		
	Scanner Name		
	Install on this server	gwava-iso (Linux)	
	IP listen address@	0.0.0.0	
	Allowed relay addresses @	127.0.0.1	×
		192.168.*.*	×
		172.16.*.*	×
		10.*.*.*	×
		[add another address/range]	
	Perform IP reputation test@		
	Perform RBL drop at connection@		
	Perform SPF drop at connection@	\checkmark	
		Continue	

which are allowed to send mail through the GWAVA SMTP scanner. Your mail system SMTP address should be listed here, as well as any other mail sending source for your domain. Mail coming from these addresses will be treated as outbound mail. No source but these listed addresses will be allowed to send mail through the SMTP interface.

The red 'X' removes listed address ranges and the blue 'add...' link provides an extra address/range box.

IP Reputation and **RBL** drop at connection settings are recommended as default. This dumps any incoming message that fails these initial incoming tests, saving bandwidth and performance.

RBL

The Real-time Blackhole List scanner searches the header of incoming message files to see if their source address is listed on an RBL. When enabled to drop on connection, a positive RBL event will cause the SMTP scanner to terminate the connection to the sending server for the offending message as soon as the event occurs. The RBL scanner utilizes real-time blackhole lists hosted on the servers listed under the RBL configuration page. RBL servers may be added or removed from the configuration. This is a strict pass or fail engine, and an offending ip address listed on the RBL will not be allowed to send mail to your system. Take time to verify that the RBL servers listed in the configuration are the desired list servers. The default list servers for RBL are, sbl-xbl.spamhaus.org and bl.spamcop.net.

IP Reputation

IP Reputation works much like the RBL scanner does, in that it uses a black list, but also has a white list for common mail sources. When used with the SMTP scanner, IP Reputation will also temporarily fail messages from sources not found on either list. The temporary fail will allow the sending SMTP gateway to retry, and it will eventually get through. This catches one-time spam bursts from sources not found on the black list, while enabling good mail to still be delivered to the system. The black and white lists are maintained and updated online, but are cached on the local machine as they are used.

SPF

Sender Policy Framework can be used with the GWIA and SMTP scanners. Sender Policy Framework, (SPF) attempts to verify the sender of each email message, which can eliminate spoofed email and most

backscatter attacks. For SPF to work correctly, the sending domain must have an updated SPF record set up in DNS. If the sending domain does not have a SPF record set in their DNS, then their mail will not be blocked. Setting up a correct SPF record will block messages from spammers who are pretending to be you, to your system.

To use SPF on a GWIA scanner, you must correctly specify which line in the header of mail messages is to be used. If the mail system is using a relay or proxy which adds a line to the message, then you should set SPF to use the second line (2), otherwise, the line used should be set to one (1), which is the default.

SPF is not enabled by default, but can be a powerful tool to keep spam from entering your system.

Select your preferences, and click 'Continue'.

2 <u>1</u> 29	Set	up Wizard
	You	can quickly setup the scanner with some of the most common default security options
	~	Stop Viruses
		This server will use Kaspersky AV engine to scan for viruses
		Enabling virus scanning includes enabling virus sanner services and detecting file types that frequently include viruses with attachment type scanning (i.e. *.vbs, *.pif, *.exe etc) and fingerprinting of attachments.
		⊕ advanced settings
	~	Stop Spam
		Enabling spam detection includes enabling the heuristic detection system and the SURBL and RBL features in GWAVA.
		advanced settings
		Continue

Set the default actions for viruses and spam. These settings can be changed after scanner creation.

Click 'Continue'.

Review and confirm your settings. If you wish to make changes, use the '**back**' button on your browser, correct the information, and continue.

*	Create new SMTP scan	ner
	The requisite information has be is correct, press the install butto	een collected and is ready to be deployed. If you are satisfied that the installation information on to commit the installation procedure to the GWAVA network.
	Scanner name	SMTP Scanner
	Install to server	gwava-iso (Linux)
	IP listen address	192.168.1.104
	Outbound SMTP sources	127.0.0.1 192.168.*.* 172.16.*.* 10.*.*.*
	IP Reputation	enabled
	Greylisting	disabled
	RBL connection drop	enabled
	SPF connection drop	enabled
	Stop Viruses	Yes
	Stop Spam	Yes
		Install

Click 'Install' to continue.

3	Installing SMTP scanner
	Installation tasks are now being performed. On completion, you will be able to continue to configure the scanner services to start protecting your messaging system.
	DO NOT change pages during this procedure or the installation will not complete. Please wait until you are taken to the completion response page.

Wait while the installation completes.

¥	SMTP scanner installation finished
	Activating virus scanning
	Activating Attachment Blocking
	Setting up Fingerprinting
	Setting up Spam System
	Setup of Antispam system complete.
	Scanner 'SMTP Scanner' was created successfully.
	You should now refresh your servers view for the server that this scanner was connected to for configuration options.

Once installation is complete, refresh the Server/Scanner Management | <Server Name> | Manage scanners folder to view your new SMTP scanner.

Your SMTP scanner is now created and ready to configure.

As soon as the MX record pointing to the GWAVA SMTP is active, the SMTP scanner will begin filtering mail.

