

GWAVA Certified Engineer

GWACon EMEA 2009

Introduction



Course Objectives

We want you to walk away familiar with:

What GWAVA is and how it can help your organization

Using the SMTP scanner

WASP & POA scanners

Stopping SPAM

Manage your QMS

Setting up a GWAVA network

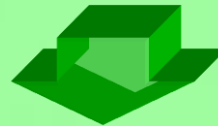


What is GWAVA?

SPAM-Blocker Technology

Advanced Anti-Virus Protection

E-mail Surveillance and
Administrative Capabilities



GroupWise Anti-Virus Agent



What is GWAVA?

Goals for GWAVA 4.5 are:

- Reduce administrative burden
 - Improve spam catch accuracy
 - Reduce false positives
- Reduce server load and still provide scalability for increasing email loads
- Provide greater virus protection via KAV and the new “0-day virus scanner”
- Centralized quarantine for all scanners
- Stop spoofed messages for your domain and others (backscatter/spam undeliverables)



What is GWAVA?

New features in GWAVA 4.5:

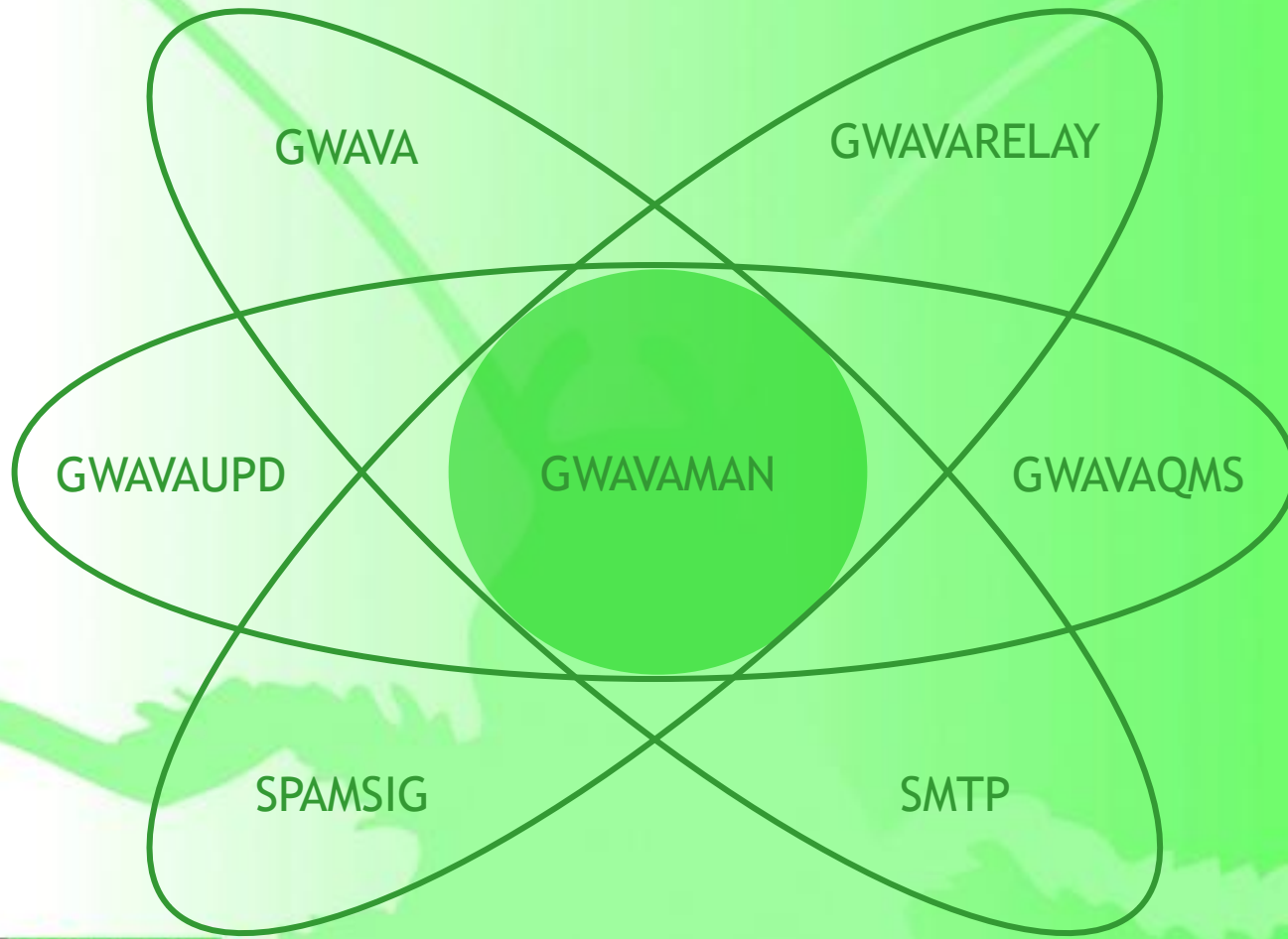
- Appliance install
 - Quick install with no extra overhead from the OS (SLES 10) components
 - Requires no Linux knowledge
- SMTP scanner
 - Can work with any email backend
 - Stop mail before it enters your system
 - Provides connection-level access for GWAVA services
- Connection Dropping
 - Dramatically reduce server load
 - Can be based on RBL, IP Reputation, or SPF
- SPAM Signature Engine
 - No training needed
 - 0-hour virus scanner



What is GWAVA?



What is GWAVA?



Spam Signatures

- Each mail has a unique signature
- A list of signatures is stored on an external server
- Very very very very few false positives
- No setup from your end
- Provides 0-day virus scanning



Connection Dropping

- **Block messages before the message is even received**
 - Dramatically reduces server load
 - Server can now handle much more mail
 - Based on RBL, IP Reputation, SPF

IP Reputation

- Determine the validity of a sender based on IP address
- Intelligent greylisting
 - Known spammers are denied
 - Possible spammers are told to try again later
 - Good mail senders are allowed in
- Unknown spammers cannot get through
- “0-day spam protection”

IP Reputation: 3 Functions

Blacklist

Whitelist

Greylist

IP Reputation: Blacklist

Black lists are kept of known spammers' IP addresses, much like RBL lists

If you
have
SMTP
scanning

- Blacklisted senders can be dropped immediately
- A 5xx level error is returned to the sending server

If you
don't

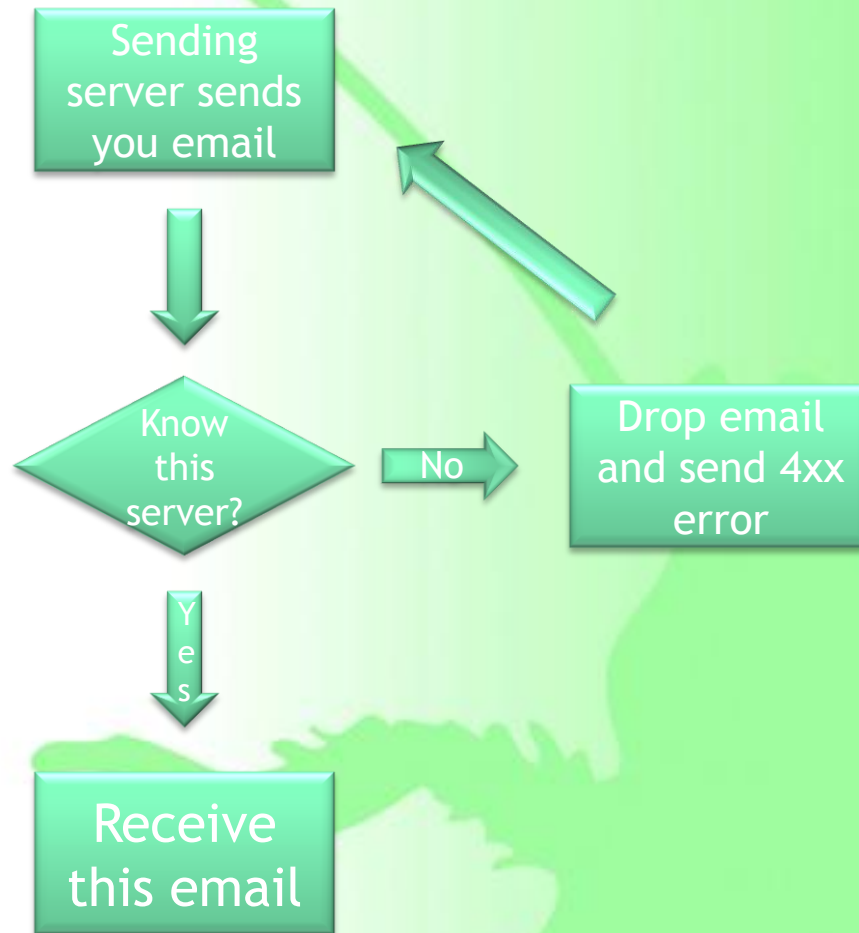
- The header lines can be scanned for blacklisted IP addresses
- These emails can be blocked/quarantined

IP Reputation: Whitelist

- List contains IP addresses of legitimate senders
- Common sources of email will not be delayed by the greylisting feature
- Common senders include gmail, yahoo, and hotmail



IP Reputation: Greylist



- Only available when using a SMTP scanner with connection dropping turned on
- 99% of legitimate email servers will try again later if they receive this error
- Usually spammers won't try to send again

SPF

- Validate the sender address via the DNS SPF record
- SPF record simply has a list of server IP addresses who can send mail for your domain
- Stops common spoofed messages (credit cards, banks)
- Stop spammers from sending you mail with the same sender and recipient
- Set up your own SPF record

Installation Appliance



Installation Appliance

```
N SUSE Linux Enterprise Server
2025 11:00:00 AM

##### Final Setup Step (1/7) #####
##### Keyboard Setup #####

Please enter the desired keyboard layout.

0: English US          1: English UK
2: German              3: German with deadkeys
4: German Switzerland 5: French
6: French Switzerland 7: French Canada
8: Canadian Multilingual 9: Spanish
10: Spanish Latin America 11: Spanish CP 850
12: Italian            13: Portuguese
14: Portuguese Brazil  15: Portuguese Brazil -- US accents
16: Greek              17: Dutch
18: Danish             19: Norwegian
20: Swedish            21: Finnish
22: Czech              23: Czech qwerty
24: Slovak             25: Slovak qwerty
26: Slovene           27: Hungarian
28: Polish             29: Russian
30: Serbian            31: Estonian
32: Lithuanian         33: Turkish
34: Croatian           35: Japanese
36: Belgian            37: Dvorak
38: Icelandic          39: Ukrainian
40: Khmer
Enter Selection: _
```



Installation Appliance

```
N SUSE Linux Enterprise Server
2025 11/03/2025 10:10:10

##### Final Setup Step (2/7) #####
##### Network Setup #####

Please enter the correct values for your network.
The current value or previously entered value appears in parentheses.
If nothing is entered the value in parentheses will be used.

IP address (example: 192.168.137.132): 192.168.137.22
Subnet Mask (example: 255.255.255.0):
Gateway (example: 192.168.137.1):
Primary DNS (example: 192.168.137.1):
Secondary DNS (example: 192.168.137.1):
Domain (example: localdomain): brainstorminc.com
Server Name (example: linux-dqol.site): gwava-master2

Please verify that these values are correct:
IP address: 192.168.137.22
Subnet Mask: 255.255.255.0
Gateway: 192.168.137.1
Primary DNS: 192.168.137.1
Secondary DNS: 192.168.137.1
Domain: brainstorminc.com
Server Name: gwava-master2

Finish setting up the server with these values? (y\n): y_
```

