

GWAVA 4.5



GWAVACon

GWAVA 4.5: Protecting GroupWise from the inside out...

Robert Quintero
Director, Technical Support
robertq@gwava.com

GWAVA 4.5 Goals



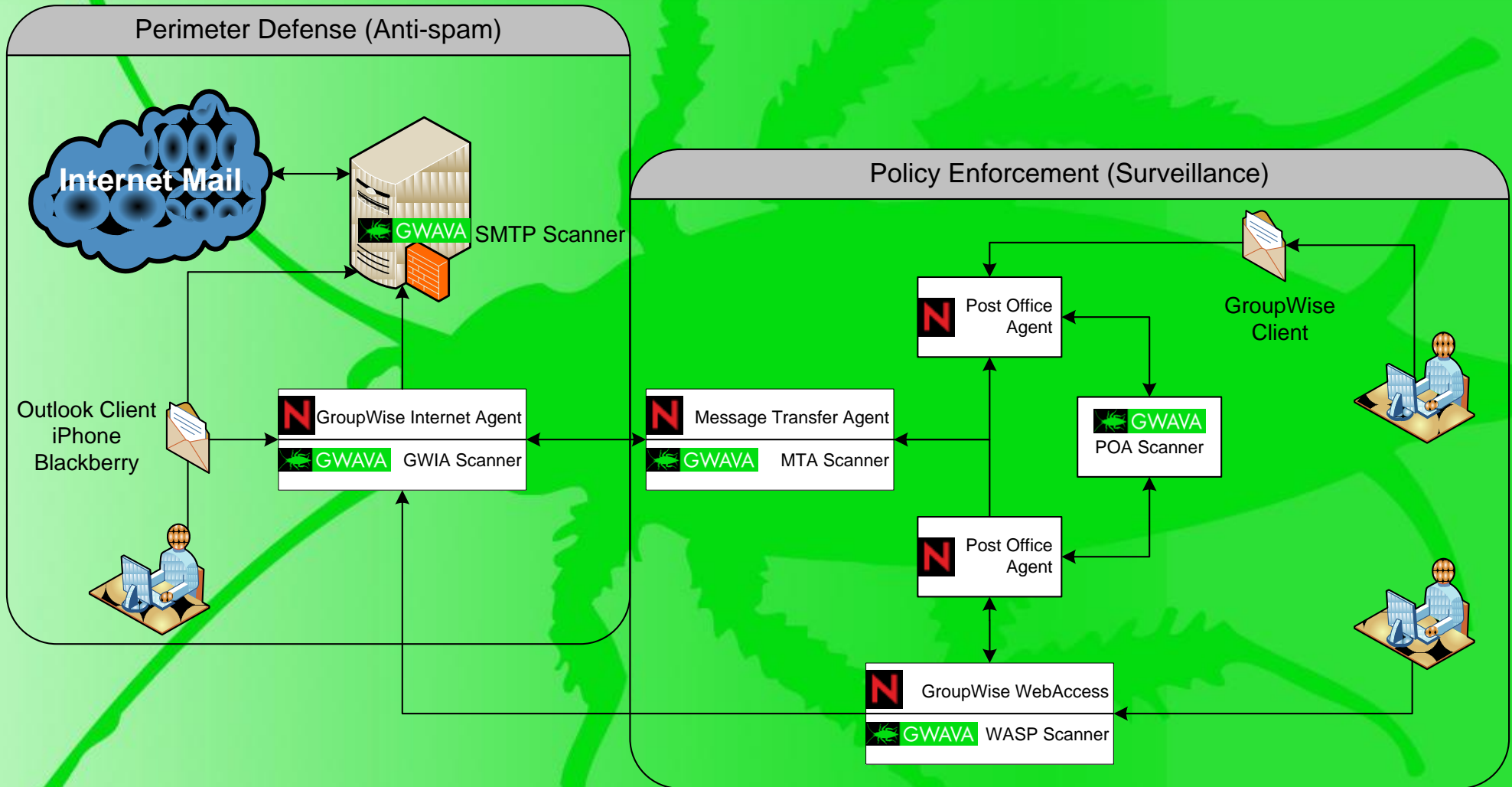
GWAVACon

- 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)

Mail Flow Overview



GWAVACon



Signature Spam Engine



GWAVACon

- **NO TRAINING**
 - Less resource utilization
 - Reduces administrator burden
- **Real-time signatures updated constantly**
 - No scheduling required
- **Provides practically zero false positives**
 - Functions much like a virus scanner
 - No need for large lists of exceptions
- **Provides 0-day virus scanning**



- SMTP scanner can work with any email backend
 - Works as a proxy
- Stop mail before it enters your mail system
 - Enables easier allocation of resources
- Provides connection level access for GWAVA services

Connection Dropping



GWAVACon

- 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



- **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



- 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”

Lab 1: Dropping



GWAVACon

- **Goals**
 - Drop connections from unknown IP addresses
 - Drop spoofed email



- **Recommended Scans**
 - Antivirus
 - Attachment/fingerprinting (mp3, mov, mpg, etc)
 - Content Filters
- **Possible Actions**
 - Block (delete)
 - Quarantine
 - Notifications
 - BCC



- **Tightly integrates with the WebAccess Application**
- **Scans the message before it is sent**

Lab 2:



GWAVACon

- **Goals**
 - **Demonstrate sample configuration**
 - **Send sample messages and verify block result**



- Scan uses IMAP and a trusted application key
- Scans mail after it has been received
 - Can pull mail out of the existing mailbox
- Example setup
 - Delete any viruses already in post office
 - Detect messages with disallowed words
 - Notify administrator of message
 - BCC a copy to a mailbox (quarantine possibly)
 - Delete copy out of the user's mailbox

Lab 3:



- **Goals**
 - **Configure POA scanner for only a few users**
 - **Remove unwanted attachments**
 - **Remove inappropriate email from mailboxes and then quarantine it for later review**

Quarantine



GWAVACon

- **Suspect email in Digest**
 - False Positive email can be released from digest
- **User Quarantine**
 - Log in as user and see your mail in real-time

Central Quarantine



GWAVACon

- One place to check for blocked messages even if you have multiple scanners on different servers
- Master server
 - Houses all mail and sends digests
- Slave server
 - Sends mail to the master

Lab 4:



- **Goals**
 - Create digest for all previously blocked messages
 - Log in to QMS as user to review real-time messages

Questions



GWAVACon

