PGP POLICY MANAGEMENT AGENT FOR SMTP 1.0

Flexible Security Policy Enforcement for Email

PGP® Policy Management Agent for SMTP helps to protect an organization's vital information by enforcing corporate security policies for email communications across internal and external networks. This important component of the PGP Business Security Suite transparently integrates with the desktop to ensure that incoming and outgoing email messages adhere to the policies established for a given corporate site.

Reliable prevention of policy violations

PGP Policy Management Agent works with standard SMTP mail servers, intercepting and checking email to ensure that it conforms with desired security policies. A typical policy established for encryption software, for example, is that encrypted email must also be encrypted to a corporate message recovery key to enable data recovery. Email that adheres to the policy is automatically routed to the intended recipient. Email that fails to adhere to any of the established policies is rejected by the server and sent back to the client with a configurable SMTP error message, depending upon the policy failure.

Built-in reporting capabilities

PGP Policy Management Agent for SMTP provides automatic logging for each request that is processed. IS managers can choose among multiple levels of information, as well as the destination of the output.

Transparent client interaction

Once installed, PGP Policy Management Agent for SMTP performs its functions without any change of client software. All operations are transparent to the client, unless policy is failed. Rejection messages are configurable for each installation and policy violation.

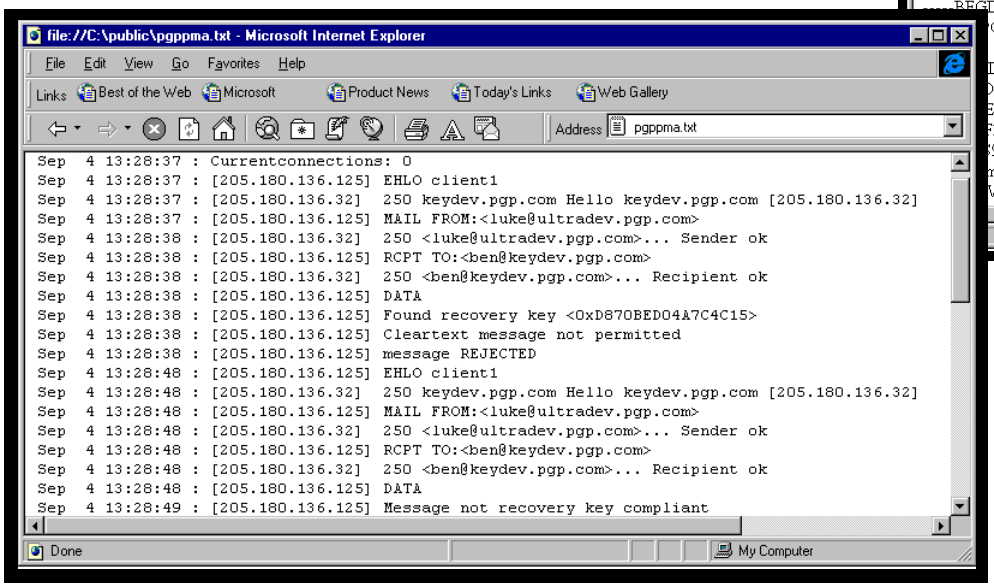
- Policy enforcement for email within intranets and over the Internet
- Automatic enforcement of encryption and corporate message recovery policy
- Support for standard SMTP servers
- Transparent integration with all PGP clients
- Easy installation and operation
- Multiple logging levels
- Configurable error messages for non-conformance to policy

PRETTY GOOD PRIVACY™

PGP POLICY MANAGEMENT AGENT FOR SMTP 1.0

AVAILABLE POLICIES

- **Corporate message recovery: Rejects all encrypted messages which have not also been encrypted to one or more corporate message recovery keys.**
- **Digital signatures: Allows, Disallows, or Requires the use of digital signatures on messages.**
- **Encryption: Determines whether all email and attachments must be encrypted before passing policy requirements.**
- **Conventional encryption: Allows the rejection of all messages that have been encrypted with only conventional encryption. Conventional (also known as symmetric) encryption requires the recipient to have the same passphrase as the sender.**
- **Forbidden keys: Disallows the use of encryption to specific keys.**
- **Specified address: Limits the checking of policies to be enforced for a specified IP address or domain. Through a simple configuration value, which includes wildcard support, policies can be designated for an entire domain, network, subnet, or IP address.**



PGP Policy Management Agent for SMTP maintains a log file of all activities at the server.

SYSTEM REQUIREMENTS

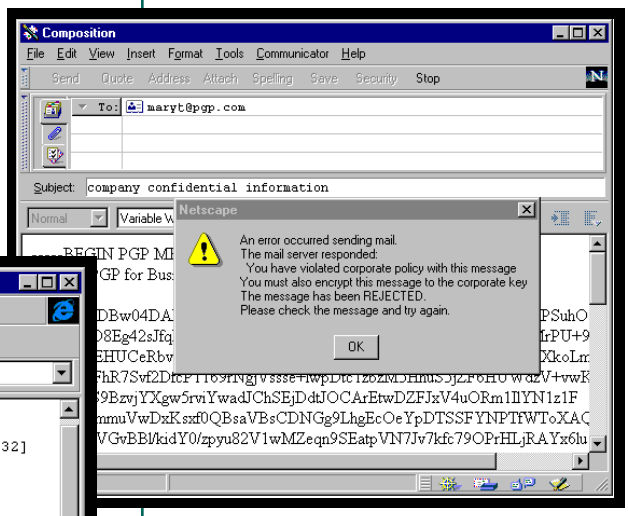
SMTP SERVER CAN BE RUN IN EITHER OF TWO CONFIGURATIONS:

SMTP server that can listen on a port other than 25 (the standard SMTP port) and will only allow connections from its own machine.

SMTP server configured to allow connections only from the server running the Policy Management Agent for SMTP.

OPERATING SYSTEMS SUPPORTED

Sun Solaris (SPARC) 2.5.1 or later, or
Microsoft Windows NT (Intel) 4.0



Email that doesn't adhere to policy is automatically rejected and returned to the sender.

FOR MORE INFORMATION

address: Pretty Good Privacy
2121 S. El Camino Real
San Mateo, CA, 94403
telephone: 602.944.0773
toll free: 888.747.3011
internet: www.pgp.com

PRETTY GOOD PRIVACY™

301-600-000003