US 20200287908A1

(19) **United States**

(12) **Patent Application Publication**

Treleaven

(10) **Pub. No.: US 2020/0287908 A1**

(43) **Pub. Date: Sep. 10, 2020**

(54) **SYSTEM AND METHOD FOR PROTECTING AGAINST E-MAIL-BASED CYBERATTACKS**

(71) Applicant: **Bravatek Solutions, Inc.**, Austin, TX (US)

(72) Inventor: **Ian Anthony Treleaven**, Maple Ridge (CA)

(73) Assignee: **Bravatek Solutions, Inc.**, Austin, TX (US)

(21) Appl. No.: **16/882,726**

(22) Filed: **May 25, 2020**

Related U.S. Application Data

(63) Continuation of application No. 15/246,500, filed on Aug. 24, 2016, now Pat. No. 10,666,659.

(60) Provisional application No. 62/209,055, filed on Aug. 24, 2015.

Publication Classification

(51) **Int. Cl.**

H04L 29/06 (2006.01)

H04L 12/58 (2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/102*** (2013.01); ***H04L 51/08*** (2013.01); ***H04L 51/22*** (2013.01); ***H04L 63/20*** (2013.01)

(57) **ABSTRACT**

A system for dynamically managing email access and content is described, wherein the email system based on email rules and filters may modify emails presented to users or limit access to the email content via a specific architecture.

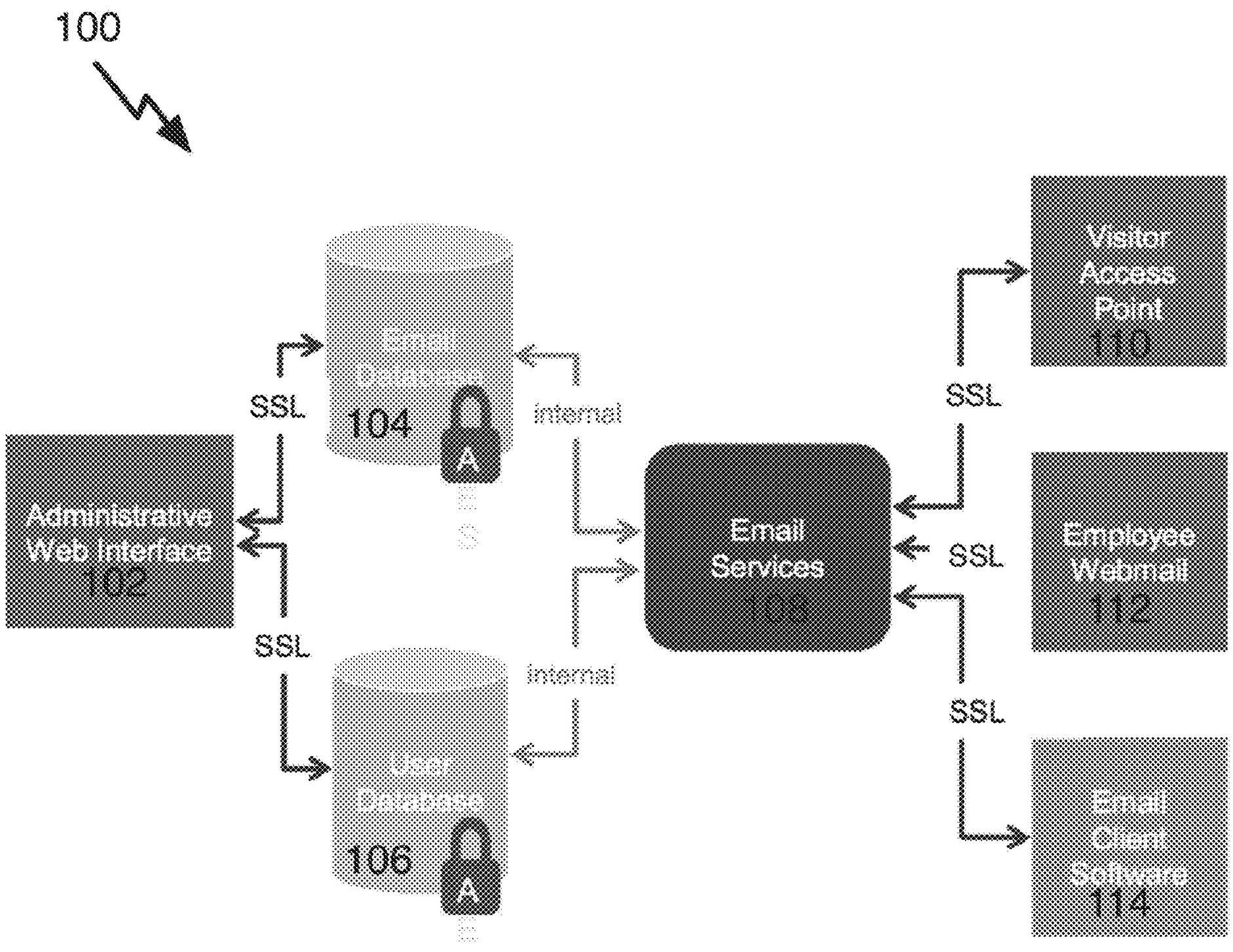


Figure 1

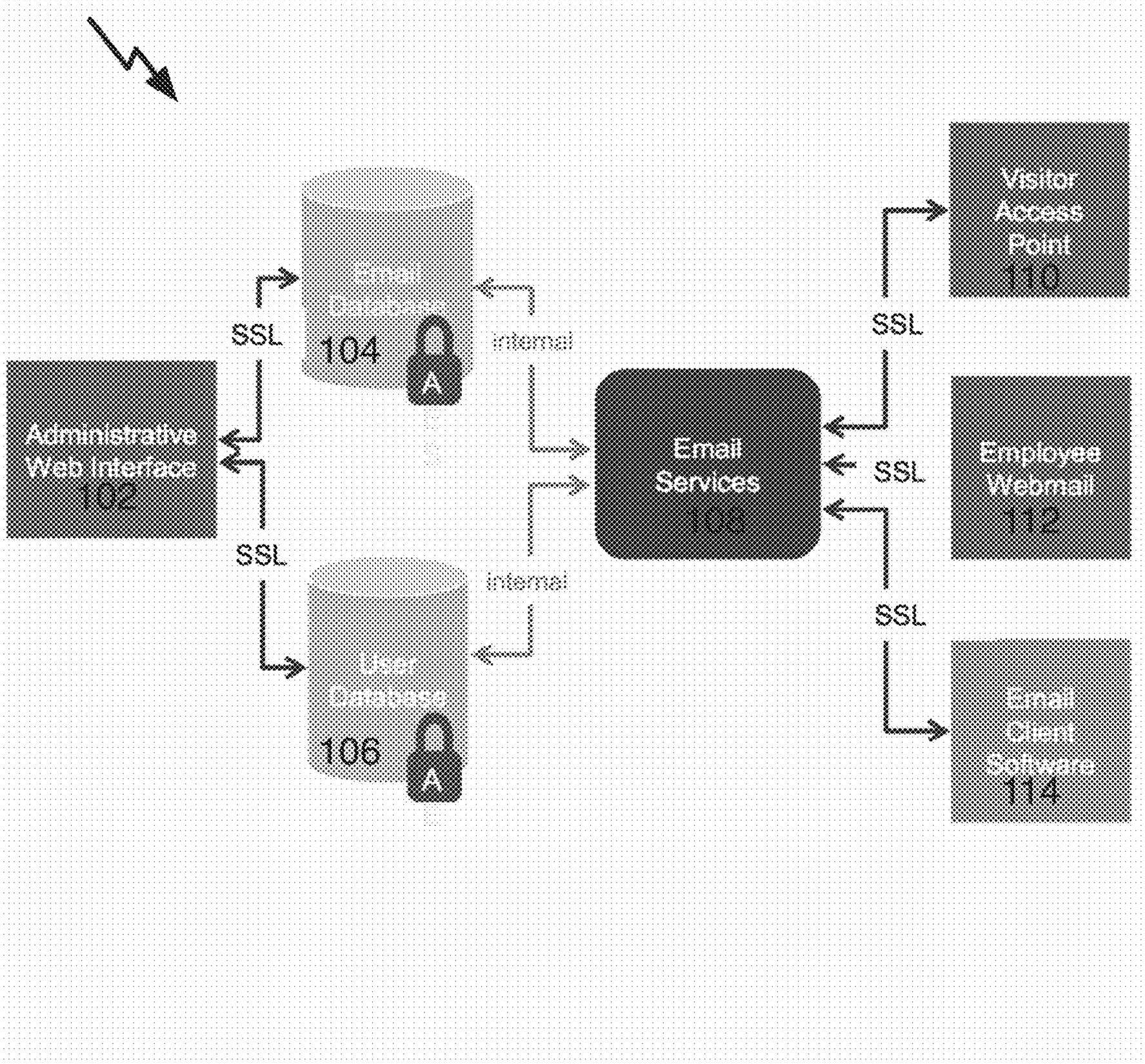

100
Administrative Web Interface 102
SSL
104
A
Internal
Email Services 108
SSL
Visitor Access Point 110
SSL
Employee Webmail 112
SSL
Email Client Software 114
Internal
User Authentication 106
A
SSL

Figure 2

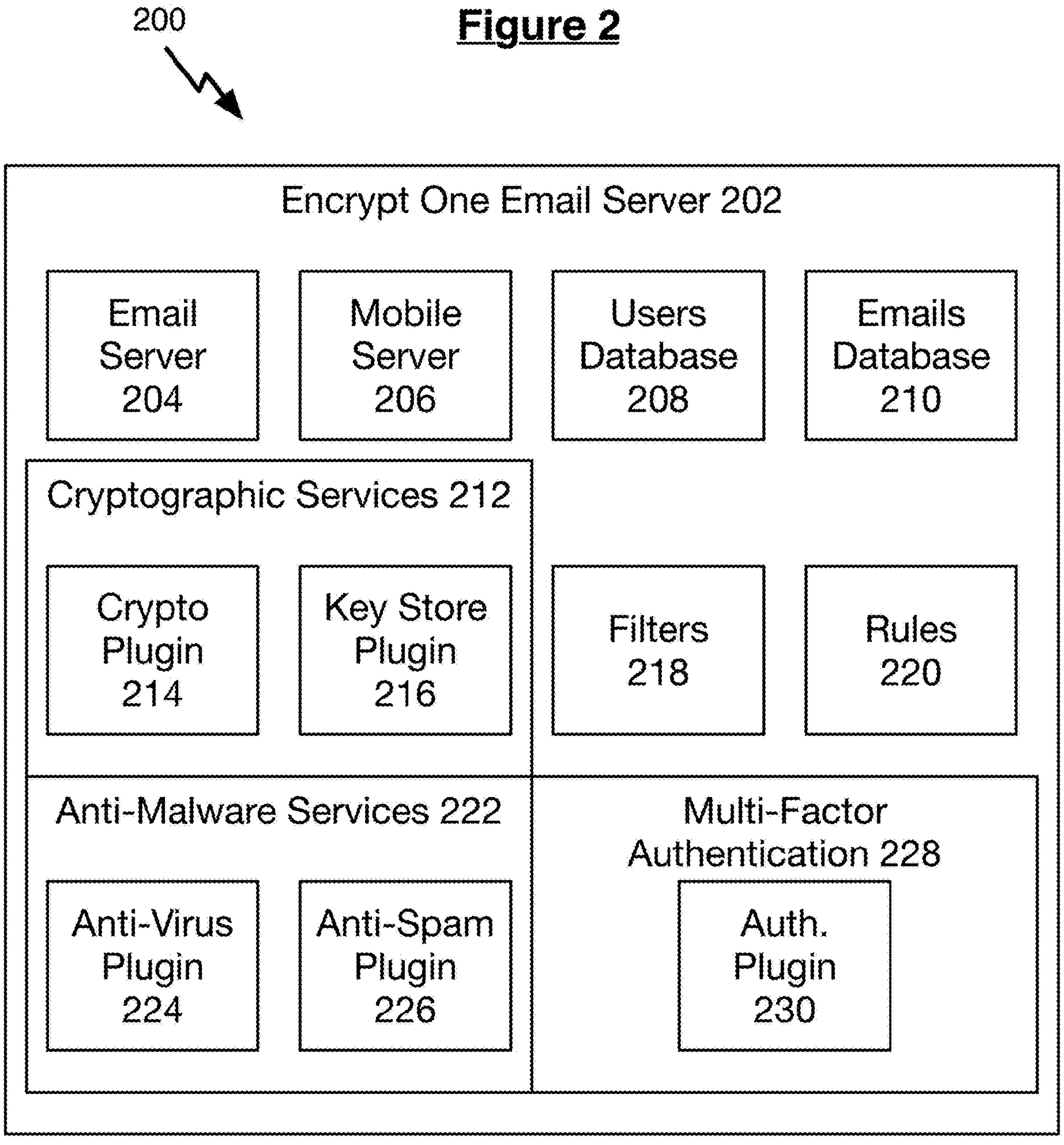

200
Encrypt One Email Server 202
Email Server 204
Mobile Server 206
Users Database 208
Emails Database 210
Cryptographic Services 212
Crypto Plugin 214
Key Store Plugin 216
Filters 218
Rules 220
Anti-Malware Services 222
Anti-Virus Plugin 224
Anti-Spam Plugin 226
Multi-Factor Authentication 228
Auth. Plugin 230

Figure 3

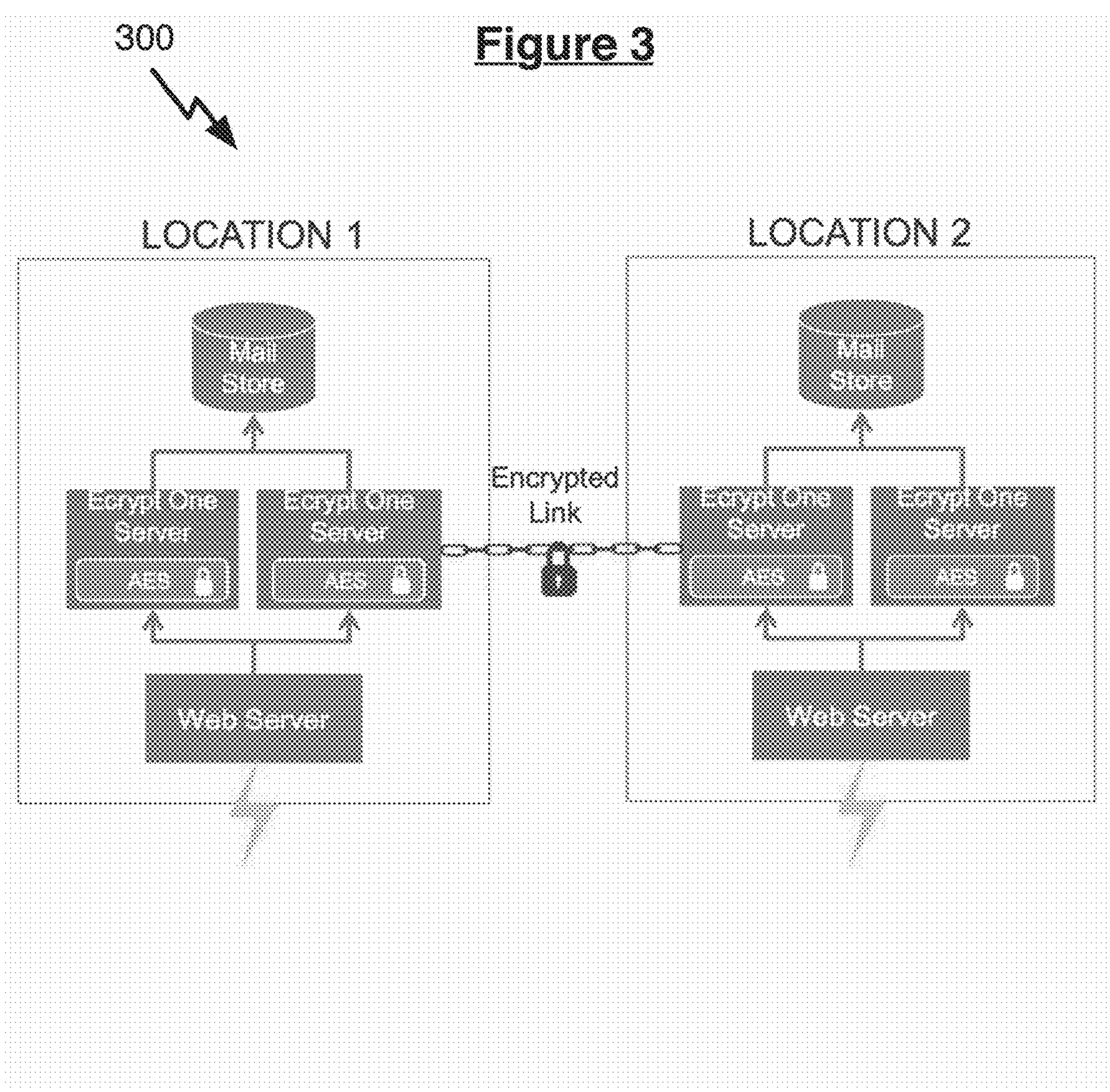

300
LOCATION 1
LOCATION 2
Mail Store
Mail Store
Encrypted Link
Encrypt One Server
AES
Encrypt One Server
AES
Encrypt One Server
AES
Encrypt One Server
AES
Web Server
Web Server

Fig. 4

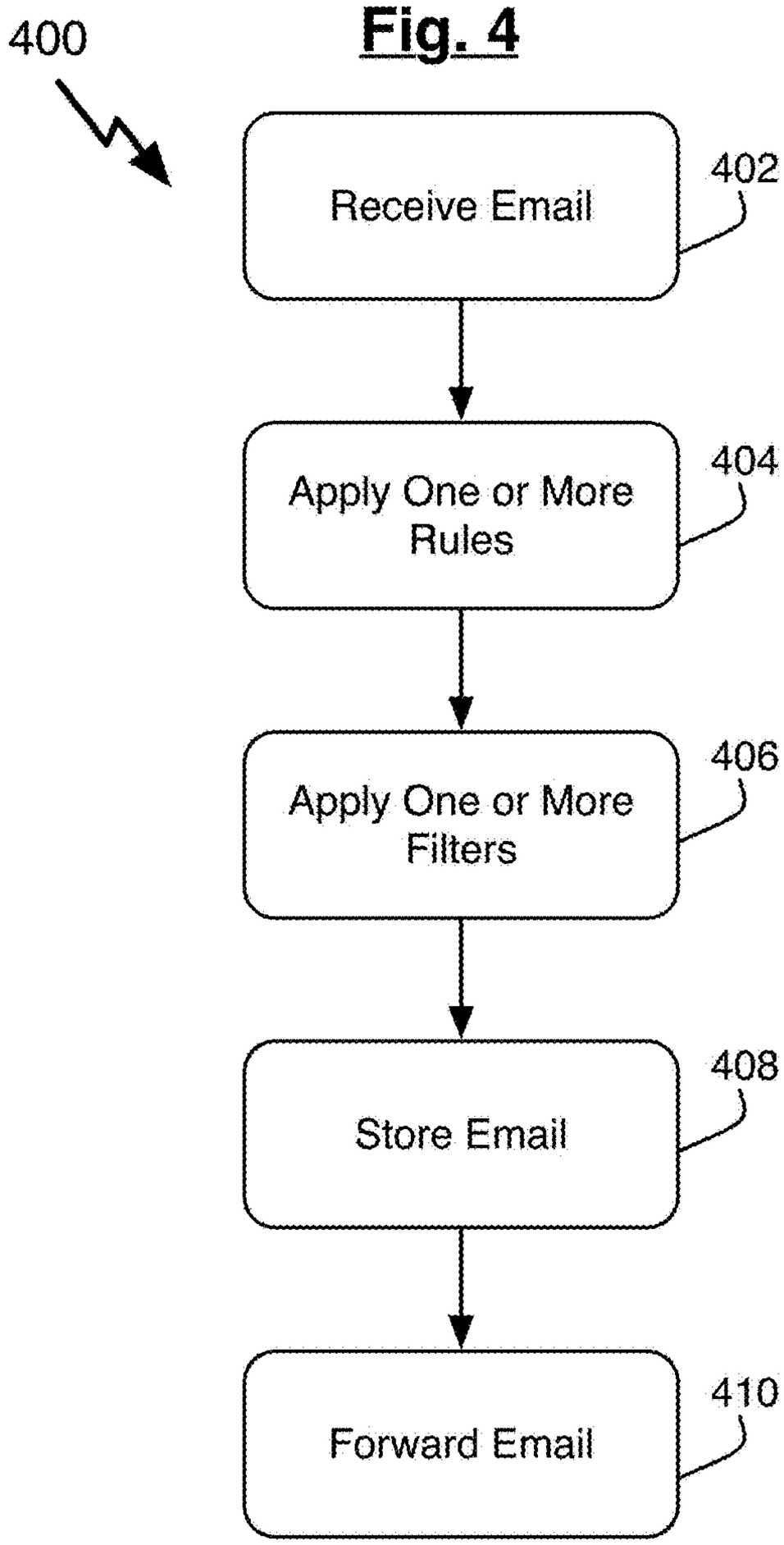

400
Receive Email
402
Apply One or More Rules
404
Apply One or More Filters
406
Store Email
408
Forward Email
410

Figure 5

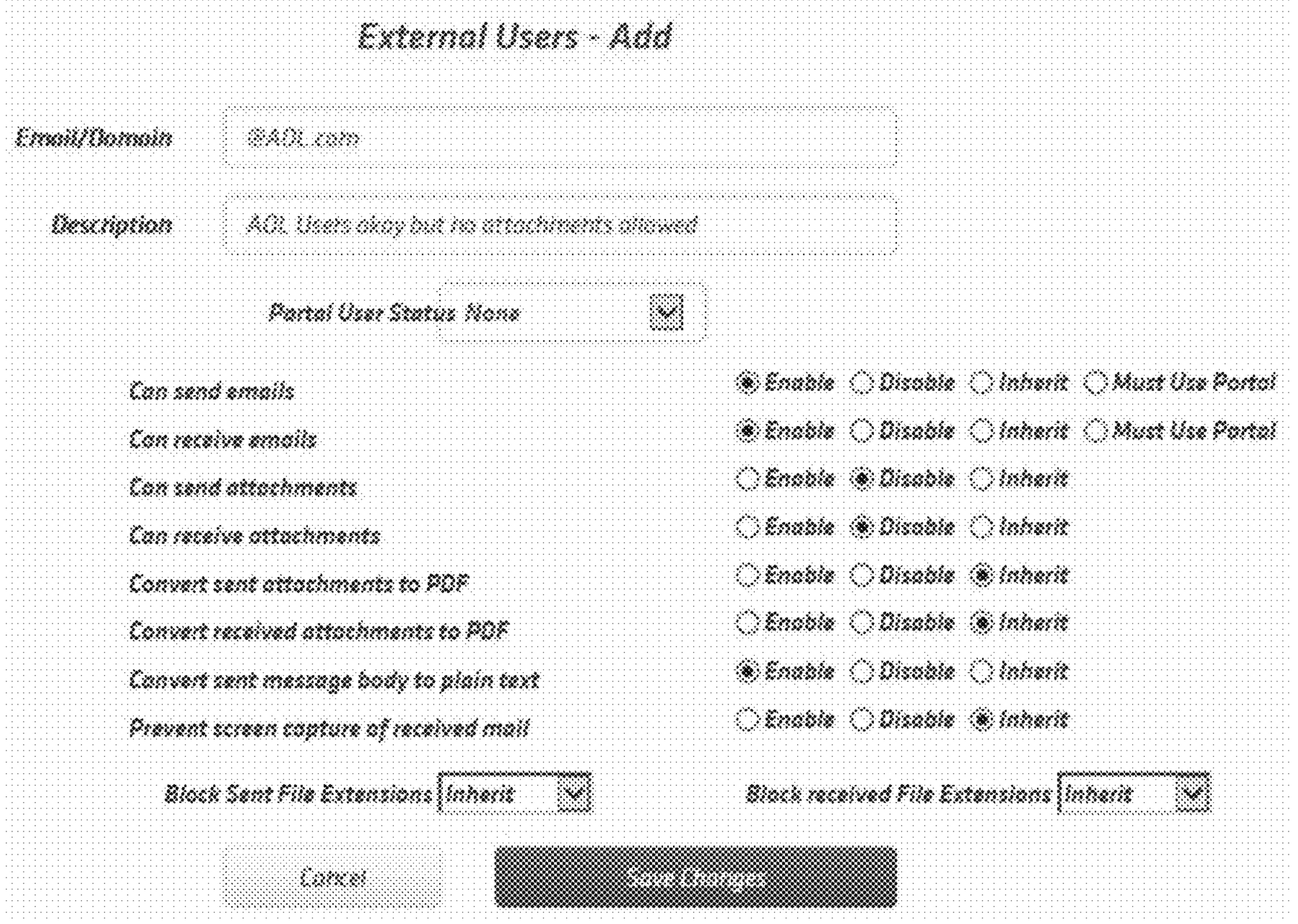

External Users - Add
Email/Domain
@AOL.com
Description
AOL Users okay but no attachments allowed
Portal User Status: None
Can send emails
Enable Disable Inherit Must Use Portal
Can receive emails
Enable Disable Inherit Must Use Portal
Can send attachments
Enable Disable Inherit
Can receive attachments
Enable Disable Inherit
Convert sent attachments to PDF
Enable Disable Inherit
Convert received attachments to PDF
Enable Disable Inherit
Convert sent message body to plain text
Enable Disable Inherit
Prevent screen capture of received mail
Enable Disable Inherit
Block Sent File Extensions
Inherit
Block received File Extensions
Inherit
Cancel
Save Changes

Figure 6

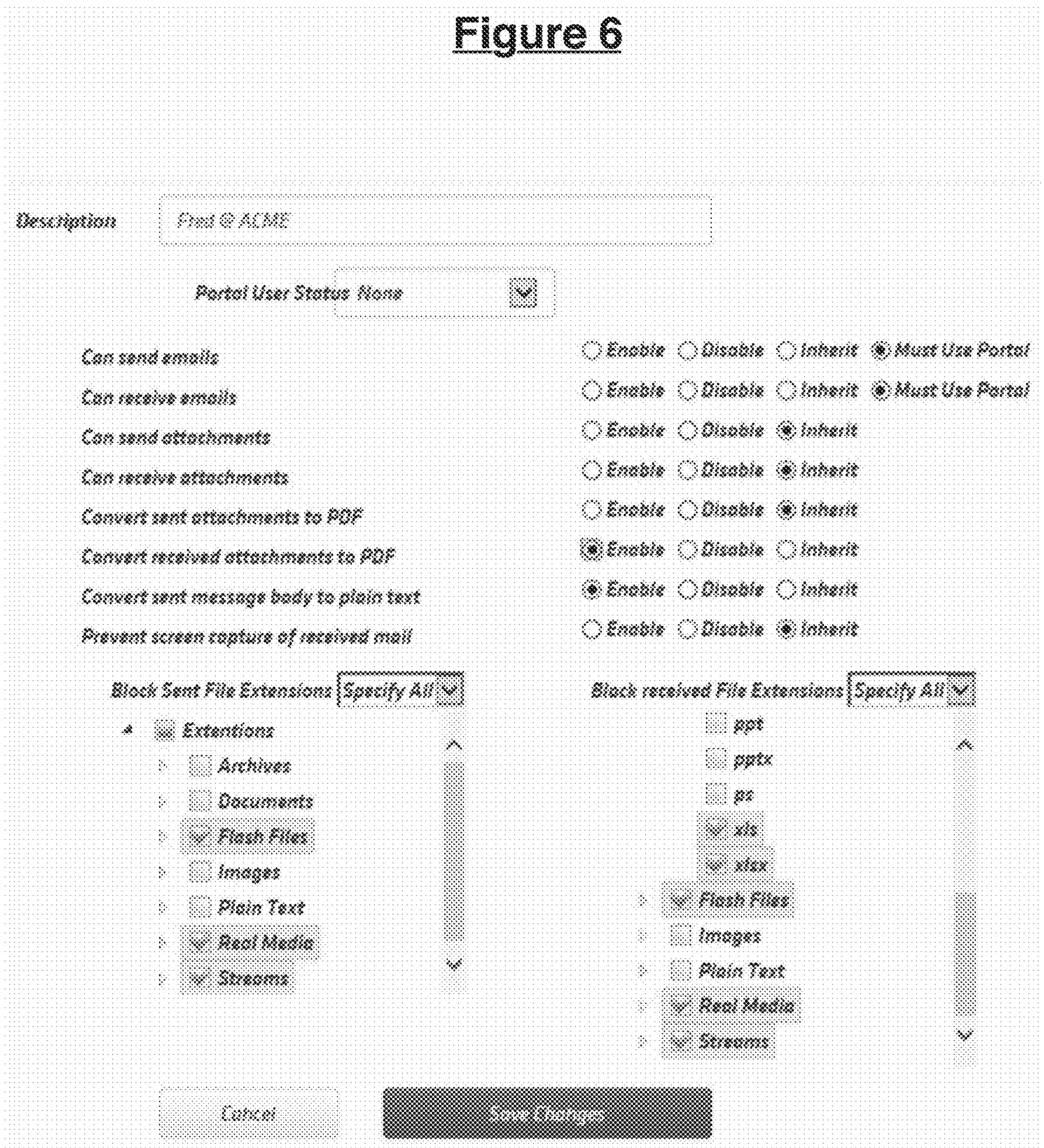

Description
Pixel @ ACME
Portal User Status None
Can send emails
Can receive emails
Can send attachments
Can receive attachments
Convert sent attachments to PDF
Convert received attachments to PDF
Convert sent message body to plain text
Prevent screen capture of received mail
Enable Disable Inherit Must Use Portal
Block Sent File Extensions Specify All
Extensions
Archives
Documents
Flash Files
Images
Plain Text
Real Media
Streams
Block received File Extensions Specify All
ppt
pptx
ps
xls
xlsx
Flash Files
Images
Plain Text
Real Media
Streams
Cancel
Save Changes

Figure 7

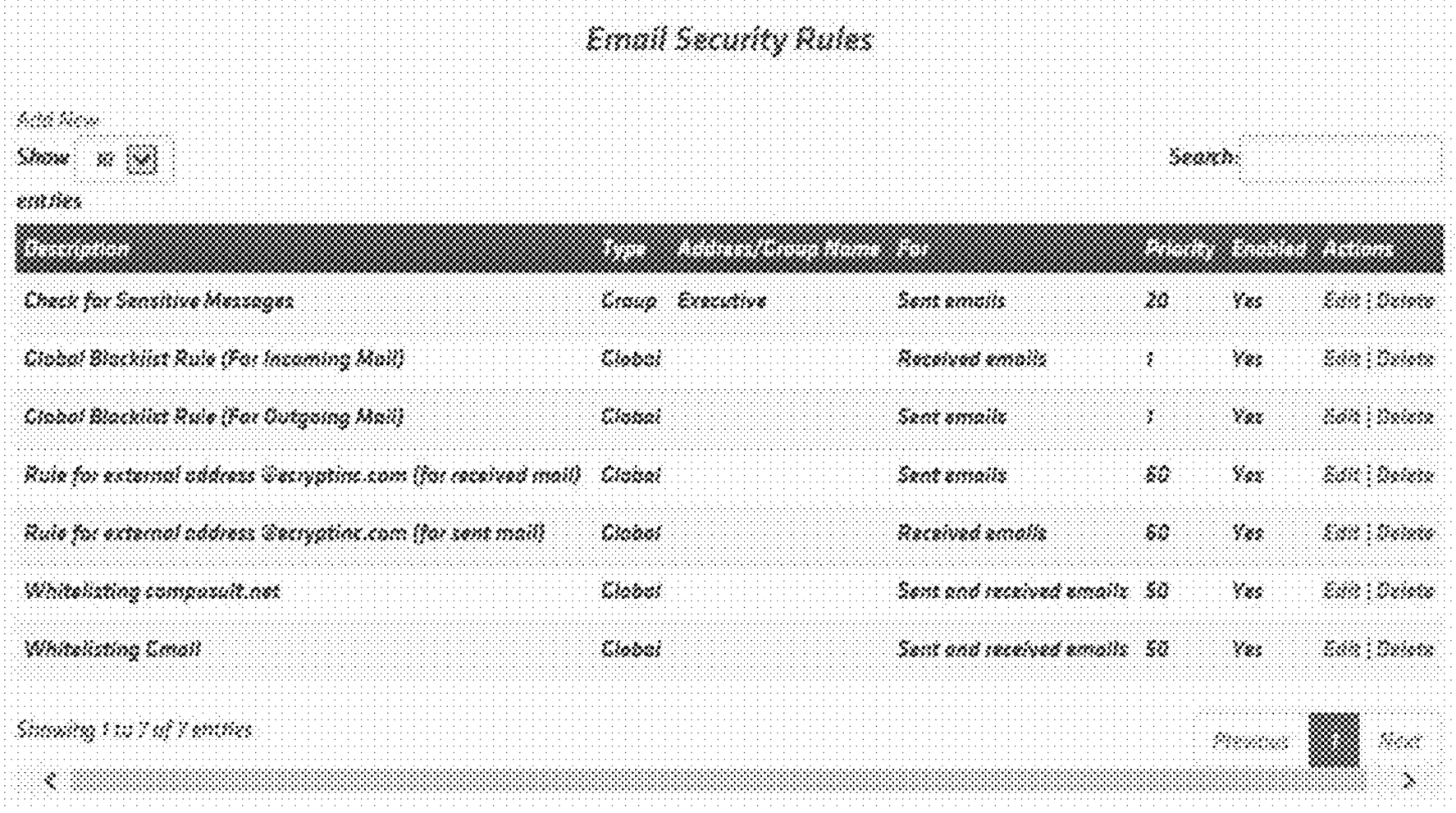

Email Security Rules
Add New
Show 10 entries
Search:
Description
Type
Actions/Group Name
For
Priority
Enabled
Actions
Check for Sensitive Messages
Group
Executive
Sent emails
20
Yes
Edit | Delete
Global Blacklist Rule (For Incoming Mail)
Global
Received emails
1
Yes
Edit | Delete
Global Blacklist Rule (For Outgoing Mail)
Global
Sent emails
1
Yes
Edit | Delete
Rule for external address @encryptinc.com (for received mail)
Global
Sent emails
60
Yes
Edit | Delete
Rule for external address @encryptinc.com (for sent mail)
Global
Received emails
60
Yes
Edit | Delete
Whitelisting compusult.net
Global
Sent and received emails
50
Yes
Edit | Delete
Whitelisting Email
Global
Sent and received emails
50
Yes
Edit | Delete
Showing 1 to 7 of 7 entries
Previous
1
Next

Figure 8

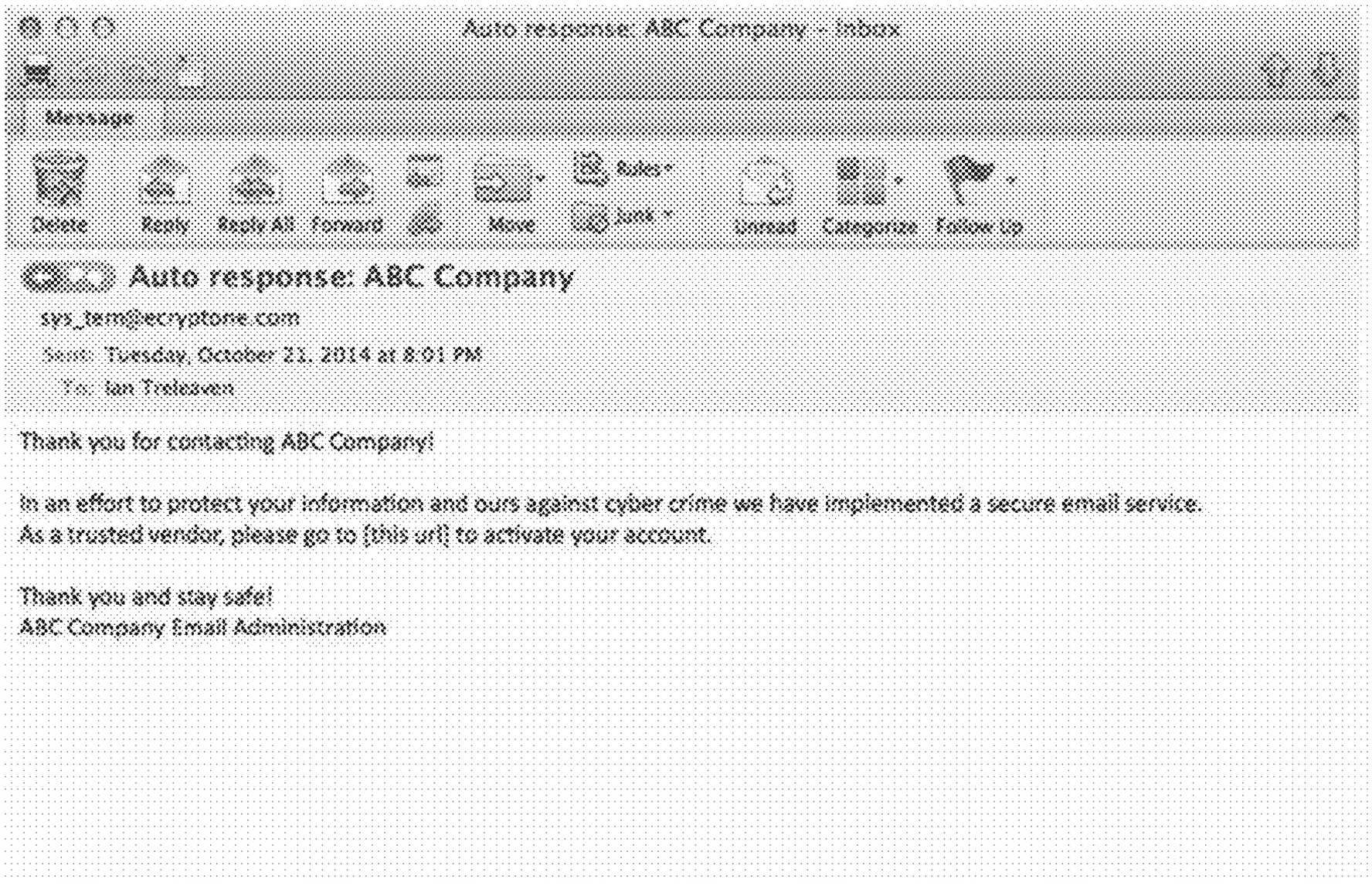

Auto response: ABC Company - Inbox
Message
Delete
Reply
Reply All
Forward
Move
Rules
Junk
Unread
Categorize
Follow Up
Auto response: ABC Company
sys_term@ecryptone.com
Sent: Tuesday, October 21, 2014 at 8:01 PM
To: Ian Trolleven
Thank you for contacting ABC Company!
In an effort to protect your information and ours against cyber crime we have implemented a secure email service.
As a trusted vendor, please go to {this url} to activate your account.
Thank you and stay safe!
ABC Company Email Administration

Figure 9

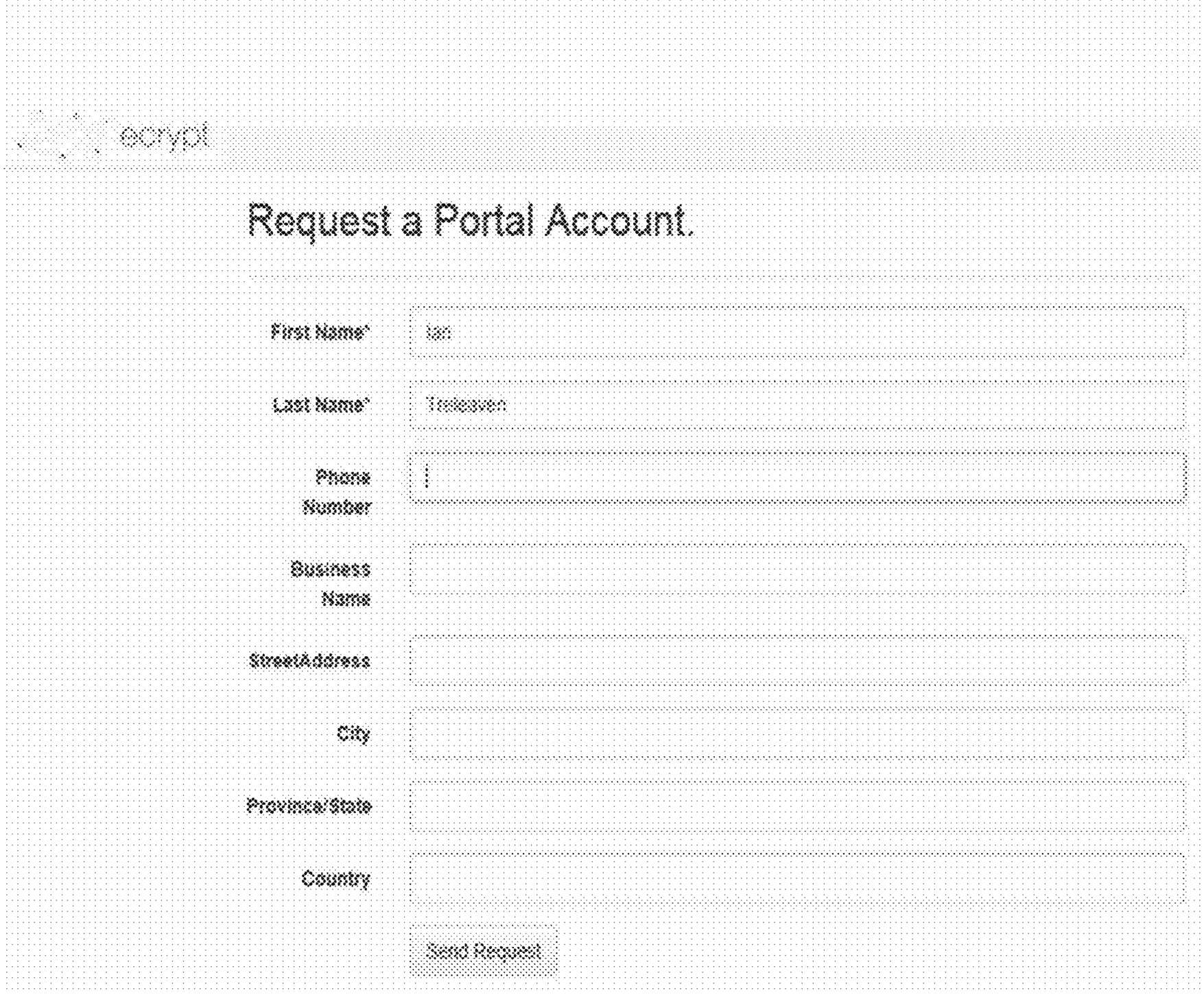

ecrypt
Request a Portal Account.
First Name*
Last Name*
Phone Number
Business Name
StreetAddress
City
Province/State
Country
Send Request

Figure 10

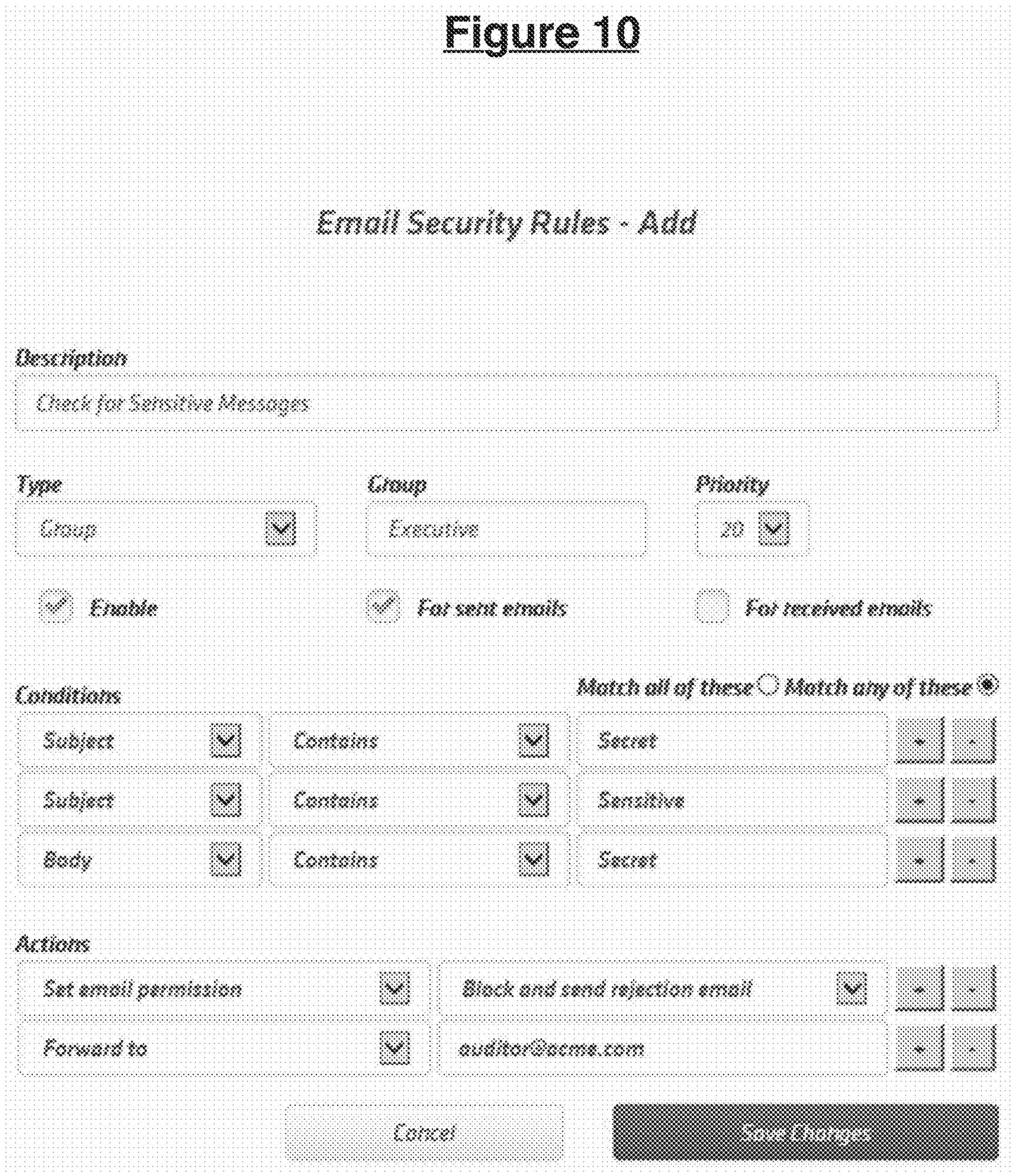
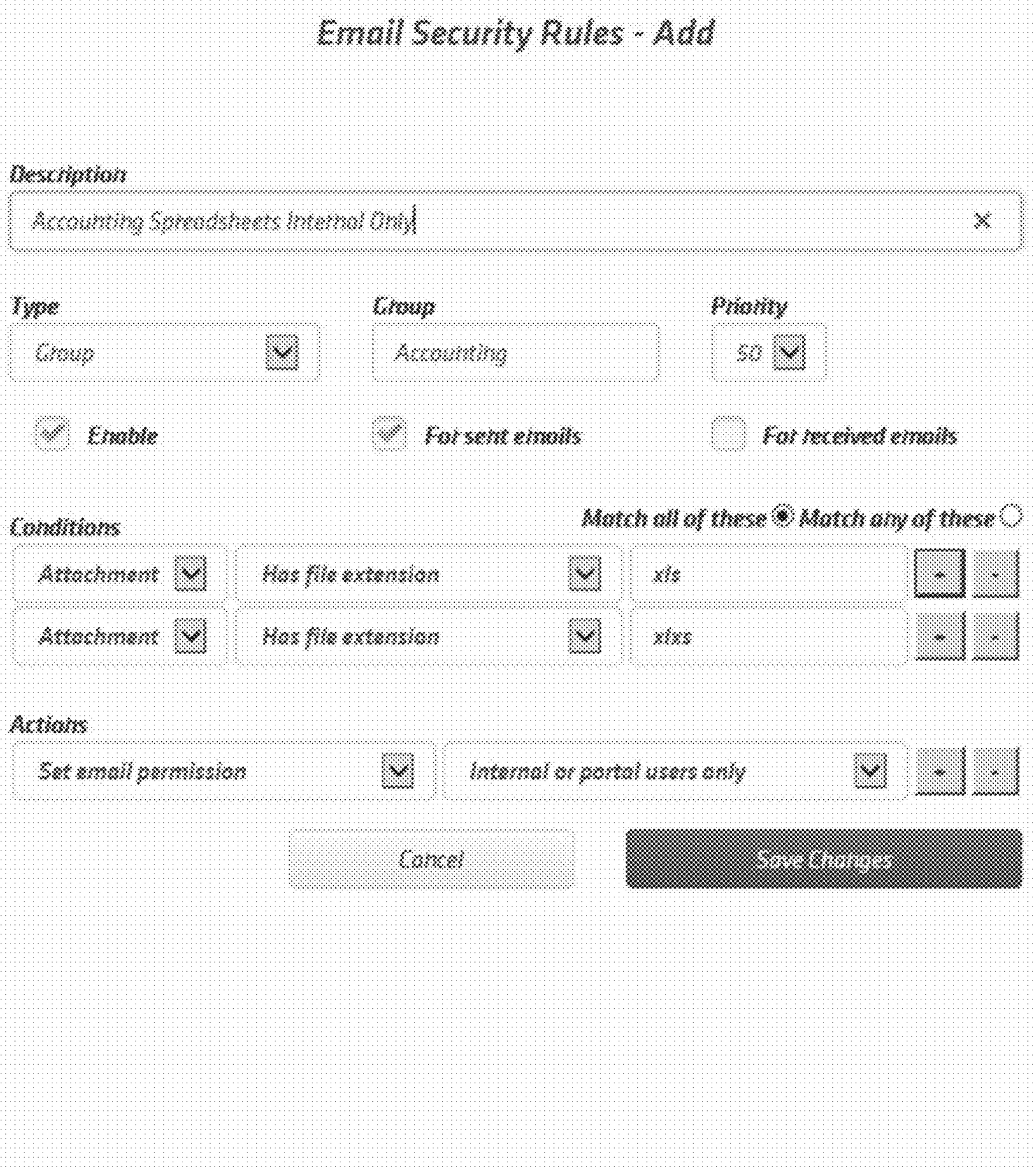

Email Security Rules - Add
Description
Check for Sensitive Messages
Type
Group
Group
Executive
Priority
20
Enable
For sent emails
For received emails
Conditions
Match all of these
Match any of these
Subject
Contains
Secret
Subject
Contains
Sensitive
Body
Contains
Secret
Actions
Set email permission
Block and send rejection email
Forward to
auditor@acme.com
Cancel
Save Changes

Figure 11


Email Security Rules - Add
Description
Accounting Spreadsheets Internal Only
Type
Group
Group
Accounting
Priority
50
Enable
For sent emails
For received emails
Conditions
Match all of these
Match any of these
Attachment
Has file extension
xls
Attachment
Has file extension
xlsx
Actions
Set email permission
Internal or portal users only
Cancel
Save Changes

SYSTEM AND METHOD FOR PROTECTING AGAINST E-MAIL-BASED CYBERATTACKS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. patent application Ser. No. 15/246,500, filed on Aug. 24, 2016, which claims the benefit of, and priority to, U.S. Provisional Patent Application Ser. No. 62/209,055, filed on Aug. 24, 2015, the entireties of which are hereby incorporated herein by reference.

BACKGROUND

Field of the Invention

[0002] The present disclosure is related to effective, efficient, and economical methods and systems for improvements in the processing of email, particularly in respect to controlling access to emails and modifying said emails to meet security conditions.

Description of the Related Art

[0003] While the Internet has popularized email as a modern form of communication, email systems were largely designed using an unsecure store-and-forward architecture. Accordingly, emails can often by read by any person who has access to network traffic, intermediary servers, email storage, etc. Various methods have been proposed to resolve the unsecure nature of email communication, such as encryption of emails or network connections. However, these solutions only prevent access to emails at various points in the storage or transit of emails. Further improvements are required to provide secure and controlled access to emails at all times and locations.

SUMMARY

[0004] An example of a system for securely managing email access and content is described. The system may be comprised of an email database for storing emails and email attachments; a user database; and an email server, wherein the content of the email is restricted or modified according to a set of rules profiles. In some embodiments, the set of rules profiles includes instructions for converting email attachments to a different form of media. In some embodiments, each rules profile is applied based on a user's email address or domain. In some embodiments, the set of rules profiles further includes instructions that the email or email attachments may only be accessed via a webmail server. In some embodiments, a subset of the rules profiles is applied based on a user's assigned grouping.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] FIG. **1** illustrates an example of a system for implementing an enhanced email system.

[0006] FIG. **2** illustrates another example of a system for implementing an enhanced email system.

[0007] FIG. **3** illustrates an example of how multiple instances of an enhanced email system may be implemented.

[0008] FIG. **4** illustrates an example of a method for handling emails that are received by the enhanced email system.

[0009] FIG. **5** illustrates an example of a rules profile that may be used with the enhanced email system.

[0010] FIG. **6** illustrates further examples of additional rules that may be contained in a rules profile.

[0011] FIG. **7** illustrates an example of a list of rules profiles.

[0012] FIG. **8** illustrates an example of a request to use a visitor access point.

[0013] FIG. **9** illustrates an example of registration request.

[0014] FIG. **10** illustrates an example of a rules profile further containing email filters.

[0015] FIG. **11** illustrates another example of a rules profile further containing email filters.

DETAILED DESCRIPTION

[0016] Although the invention will be described in connection with certain preferred embodiments, it will be understood that the invention is not limited to those particular embodiments. On the contrary, the invention is intended to cover all alternatives, modifications, and equivalent arrangements as may be included within the spirit and scope of the invention as defined by the appended claims.

[0017] With respect to FIG. **1**, an example of a system for implementing an enhanced email system **100** is shown. Administrative Web Interface **102** may be used to configure the elements of system **100**, including Administrative Web Interface **102**. Email Database **104** may be used to maintain a database of emails and related documents. User Database **106** may be used to maintain a database of user records and may also maintain their associations with respect to the emails located in Email Database **104**. Email Services **108** may perform in the role of an email server as known in the art and may further perform the methods described herein. Visitor Access Point **110** may be a webmail server or other email interface for use with outside users, such as non-employees. Employee Webmail **112** may be a webmail server or other email interface for use with internal users, such as employees. Email Client Software **114** may be email software, such as Microsoft Outlook, Apple Mail, etc.

[0018] In some embodiments, System **100** may only be composed of a subset of the above elements. For example, an embodiment of System **100** may only be composed of Email Database **104**, User Database **106**, and Email Services **108**. System **100** may be implemented using any variety of computer-based technologies, such as computers, servers, cloud-based computing, etc. For example, Email Database **104**, User Database **106**, and Email Services **108** may reside on one or more servers located within a network that then communicate, such as through secure connections (e.g., Secure Sockets Layer), to other computers that implement Administrative Web Interface **102**, Visitor Access Point **110**, Employee Webmail **112**, Email Client Software **114**, etc.

[0019] With respect to FIG. **2**, another example of a system for implementing an enhanced email system **200** is shown. Email Server **202** may be composed of an Email Server **204** (e.g., Internet Message Access Protocol server), a Mobile Server **206** that may perform the synchronization of email, contacts, calendar, tasks, and notes from a messaging server to a smartphone or other mobile devices (e.g., a Microsoft ActivSync Server), a Users Database **208** for maintaining user accounts, and an Emails Database **210** for maintaining email documents.

[0020] System **200** may also contain a Cryptographic Services Component **212**, which may provide cryptographic services relating to the methods described herein. Cryptographic Services Component **212** may also support plugins, such as Crypto Plugin **214** that allows for different forms of encryption to be supported by Cryptographic Services Component **212**, such as public key-encryption (e.g., RSA) or private-key encryption. Cryptographic Services Component **212** may also support a Key Store Plugin **216** for secure management of cryptographic keys.

[0021] System **200** may also contain a Filters Component **218** that may contain email filters as described herein and may be used by System **200** to filter emails handled by System **200**. System **200** may also contain a Rules Component **220** that may contain email rules as described herein and may be used by System **200** to process emails handled by System **200**.

[0022] System **200** may also contain an Anti-Malware Services Component **222** for managing malicious emails (e.g., emails containing spam, viruses, malware, etc.). Anti-Malware Services Component **222** may also support plugins, such as Anti-Virus Plugin **224** that may allow for different forms of anti-virus protection to be supported by Anti-Malware Services Component **222**. Anti-Malware Services Component **222** may also support an Anti-Spam Plugin **226** that may allow for different forms of anti-virus protection to be supported by Anti-Malware Services Component **222**. System **200** may also contain a Multi-Factor Authentication Component **228** for further managing access to System **200** based on two or more authentication requirements (e.g., a user password and a RSA SecurID Token). Multi-Factor Authentication Component **228** may also contain plug-ins to extend its functionality, such as an Authentication Plug-in **230**.

[0023] With respect to FIG. **3**, an example is shown of how multiple instances of System **100** or System **200** may be implemented. For example, Location **1** may contain two instances of System **200** to provide redundant or quicker services to users accessing Location **1**. In addition, Location **2** may contain two instances of System **200** to provide redundant or quicker services to users accessing Location **2**. Further, Location **1** and Location **2** may be connected via an encrypted link over a network or private line, thereby allowing for any necessary synchronization to maintain redundant or quicker services between the various instances of System **200**. For example, the instances may exchange email records, user records, email filters, email rules, etc. to improve redundancy or provide quicker service to users of any instance of System **200**.

[0024] With respect to FIG. **4**, an example of a method **400** is shown for handling emails that are received by the enhanced email system. At step **402**, the system may receive an email, which may contain attachments, data, metadata, etc. At step **404**, the system may apply one or more rules to determine how emails should be processed, which may include modifying the email, metadata, or data attached to the email. In some embodiments, the system may have a global set of rules that apply to all email or group rules that only apply to an email based on selected criteria (e.g., domain name, specific sender or receiver email address, user groupings, keywords). At step **406**, the system may apply one or more filters to determine how emails should be processed, which may also include modifying the email, metadata, or data attached to the email. Further examples of email rules and email filters that may be used to within steps **404** and **406** are described below.

[0025] At step **408**, the system may store the email. In some embodiments, the system may store only the modified email after processing a received email according to steps **404** or **406**. In other embodiments, the system may store the email as it was received, but then perform step **404**, step **406**, or both to modify the mail when asked to retrieve or forward an email in step **410**. In such an embodiment, retaining the original email may allow users to not have emails resent after email filters or rules are adjusted. For example, a user may request that an email rule be changed. After changing the rule, the user may then be able to sync their email client, thereby receiving the original emails in place of the previously modified emails it received from the system. In some embodiments, the system may also store both original and modified emails, such as when it is desired to minimize processing burden over the issue of storage requirements. At step **410**, the system may forward an email to a recipient or recipients.

[0026] With respect to FIG. **5**, an example is shown of a rules profile that may be used with the enhanced email system. A rules profile may be created for any characteristic of an email, such as a specific email address, a subset of that email address (e.g., a domain name), specific types of email content, etc. In some embodiments, rules profiles may also have parent/child relationships. For example, a rules profile for a domain name (e.g., aol.com) may act as a parent rules profile for any rules profile of a specific user whose email address contains such a domain name (e.g., bob@aol.com).

[0027] As shown in FIG. **5**, a rules profile is shown for a specific domain (e.g., aol.com). As part of the rules profile, an informative description may be entered summarizing the rules profile. Such a rules profile may than set rules specific to the characteristic of the email (e.g., domain name) that is associated with the rules profile. For example, as shown in FIG. **5**, rules may be set with respect to whether emails from a domain can send emails, can receive emails, or can send attachments. In addition, rules may be selected that convert sent attachments to another form (e.g., PDF, JPG), convert received attachments to another form, convert sent message body to a specific text format (e.g., plain text, text that complies pre-determined font settings), or that disallow screen capture of received mail (e.g., when a user is accessing the system via a webmail interface or email client that provides such an ability). In addition, rules may also be set to block sent or received file extensions.

[0028] Depending on the rule, the system may provide different choices on how the rule should applied. For example, if the rule is Enabled than the rule may always be applied; if the rule is Disabled than it may never be applied; if the rule is Inherit, than the relevant setting from a parent rules profile is inherited into that profile (e.g., if a rules profile for bob@aol.com for "can send emails" is set to Inherent and its aol.com parent rules profile is set to Disable on that function, than the rules profile for bob@aol.com will use Disable for "can send emails").

[0029] As another example of rules profiles, users may be assigned to various groupings (e.g., sales, HR, engineering, shipping). These groupings may then be stored in the user records and also may be used to create rules profiles based on such groupings. For example, rather than using a domain name-based rules profile as parent profile, a specific email address rules profile may have a sales group parent profile.

Such an approach may be used with respect to the system where it is desirable to prohibit certain groups of individuals from sending emails of certain types (e.g., users may be temporarily assigned to an delinquent grouping who are prohibited by that parent rules profile from sending attachments due to misuse of the email system).

[0030] With respect to FIG. **6**, further examples of additional rules that may be contained in a rules profile are shown. As shown in FIG. **6**, Fred@ACME may be a rules profile created for a specific user who is part of an ACME grouping. As shown in FIG. **6**, the rules profile may allow for selection of particular data that are blocked in the sending or receiving of an email by Fred@ACME. For instance, the rules profile may allow for a user to not receive or send emails that contain archives, documents, flash files, images, plain text, real media, streams, ppt, pptx, ps, xls, xlsx, flash files, etc. Such selections may be based on data type, file extensions, metadata identifiers, etc.

[0031] With respect to FIG. **7**, an example of a list of rules profiles is shown. Each rules profile in the list may be presented with a description, type, Address/Group Name, affected emails (e.g., "For"), Priority (e.g., to determine which rules take precedence), whether such a rule is enabled, and selectable actions with respect to each rule (e.g., edit, delete).

[0032] In some embodiments, the rules may specific constraints normally not allowed by an email system. For example, it may be desired that external users must use a webmail interface (e.g., visitor access point) for interacting with email in certain circumstances. For example, if an email contains attachments, the rules profile relating to that email may specify that recipient must use a webmail interface to view that attachment. In such embodiments, recipient (s) may only access such an email from a webmail interface when rules profile requires that as a condition to access the email. In further embodiments, the system may send an email to the recipient(s) indicating that an email is available via a web interface.

[0033] If a recipient has not previously used such a webmail interface, the system may provide them with an email informing them of how they can create account to use with the webmail interface as shown in FIG. **8**. A recipient may then request a webmail account (e.g., portal account) as shown in FIG. **9**. In accordance with these embodiments, access to a company's email system may be restricted such that external users can access only emails sent to them via the company's webmail server (which may impose various restrictions, such as a prohibition on forwarding, screen captures, etc.), as opposed to external email servers where the company has no ability to control the handling of emails.

[0034] With respect to FIG. **10**, an example is shown of a rules profile further containing email filters. For example, conditions may set to determine if an email satisfies a filter, such as if the subject, body, recipient, etc. contains certain keywords. If a filter determines that an email meets a condition, than a rules profile may specify actions to be taken with such an email, such as rejecting the email, sending a reply notice informing the sender of the rejection, and forwarding it to another user for review. Another example of a rules profile further containing email filters is shown in FIG. **11**. Rules profiles may use any email filter conditions known in the art and may also use actions for emails that satisfy such conditions that are known in the art or as described herein.

[0035] Based on the rules profiles, the system and methods described herein can disable Internet-based email for some all or users, while allowing access for external users via a webmail server controlled by the system (e.g., visitor access point). It may also apply white-listing or black-listing of emails based on certain conditions as described above.

[0036] The system described above may also provide others features. The system may provide persistent email and database encryption. Two-Factor Authentication may be required by the system, such as when an external user accesses a visitor access point. The system may support mobile syncing (e.g., Exchange ActiveSync) over SSL only. The system may support IMAP over SSL only. The system may entirely disable access via POP. The system may allow web access over SSL only. The system may disable direct server access to certain users or networks. The system may provide malware protection.

[0037] In some embodiments, the system may provide further protection of encryption keys. Rather than always storing such encryption keys in memory, the system may store such encryption keys in an encrypted drive and associate a special identifier with the encrypted drive. When the encryption key is not needed, the system may unmount the encrypted drive, thereby preventing access to the encryption keys by a malicious user. When access to an encryption key is desired, the system upon receiving the special identifier may temporarily mount the encrypted drive and retrieve the requested encryption keys. In such embodiment, a malicious user will likely not be able to locate any encryption keys when they are not required, as the encrypted drive will not be present on the system. Further, when the encrypted drive is present, a malicious user will likely not be able to retrieve any encryption keys, if the malicious user does not have access to the special identifier. In such embodiments, the special identifier may be changed or otherwise modified (e.g., moved to a different memory location) with each storage or retrieval of an encryption key, thereby making to difficult to determine the form of the special identifier.

[0038] While particular embodiments and applications of the present invention have been illustrated and described, it is to be understood that the invention is not limited to the precise construction and compositions disclosed herein and that various modifications, changes, and variations can be apparent from the foregoing descriptions without departing from the spirit and scope of the invention as defined in the appended claims.

[0039] All references cited are hereby expressly incorporated herein by reference.

What is claimed is:

1. A system for securely managing email access and content comprising:

one or more memory devices; and

one or more processors configured to provide:

an email database for storing emails and email attachments;

a user database;

a rules profile database containing a set of rules profiles, wherein each rules profile is individually associated with an entity or a group of entities;

a web server capable of providing a webmail client; and

an email server capable of receiving or retrieving an email and any associated email attachments, identifying a subset of rules profiles from the set of rules profiles based on one or more entities or one or more

groups of entities detected in the email or the email attachments, modifying the email and the email attachments according to the subset of rules profiles, determining based on the subset of rules profiles whether the email requires restricted access, forwarding the email to one or more recipients of the email if restricted access is not required, and if restricted access is required only providing access to the email by the one or more recipients via the webmail client.

2. The system of claim **1**, wherein the email server is further capable of sending a notification email to the one or more recipients that the email must be accessed by the webmail client.

3. The system of claim **2**, wherein the set of rules profiles is capable of including instructions for converting email attachments to a different form of media.

4. The system of claim **3**, wherein each group of entities is based on a domain name or a set of email addresses.

5. The system of claim **3**, wherein the email system does not maintain encryption keys in memory or other mounted storage media when such encryption keys are not required.

6. The system of claim **1**, wherein the webmail client is further capable of restricting the recipients from obtaining screen captures.

7. A computer-implemented method for securely managing email access and content comprising:

storing emails and email attachments;

providing access to a user database;

providing a rules profile database containing a set of rules profiles, wherein each rules profile is individually associated with an entity or a group of entities;

providing a webmail client via a webmail server;

receiving or retrieving an email and any associated email attachments;

identifying a subset of rules profiles from the set of rules profiles based on one or more entities or one or more groups of entities detected in the email or the email attachments;

modifying the email and the email attachments according to the subset of rules profiles;

determining if based on the subset of rules profiles whether the email requires restricted access;

forwarding the email to one or more recipients of the email if restricted access is not required; and

if restricted access is required only providing access to the email by the one or more recipients via the webmail client.

8. The computer-implemented method of claim **7**, further comprising the step of sending a notification email to the one or more recipients that the email must be accessed by the webmail client.

9. The computer-implemented method of claim **8**, wherein the set of rules profiles is capable of including instructions for converting email attachments to a different form of media.

10. The computer-implemented method of claim **9**, wherein each group of entities is based on a domain name or a set of email addresses.

11. The computer-implemented method of claim **10**, further comprising the step of not maintaining encryption keys in memory or other mounted storage media when such encryption keys are not required.

12. The computer-implemented method of claim **7**, further comprising the step of restricting the recipients from obtaining screen captures.

* * * * *