



SR L09 - Messaging Gateway, Encryption and Data Loss Prevention: Three Great Things Even Better Together Hands-On Lab

Description

The messaging gateway has emerged as a key point of control for managing an information risk and security strategy. With its key functions of message filtering and security, the messaging gateway serves as an ideal point on which to build the foundation of a Data Loss Prevention (DLP) and encryption strategy as well. In this hands-on lab, you will take a powerful first step toward a more comprehensive approach of data protection, configuring Symantec Messaging Gateway to work with both PGP Universal Server and Symantec Network Prevent. This configuration takes advantage of the integrated DLP Connect options built into the Messaging Gateway. It also utilizes the advanced content filtering module to enforce actions determined by Symantec DLP.

This lab assumes a prerequisite knowledge of the Symantec Messaging Gateway, Symantec Network Prevent for Email, and Symantec PGP Universal Gateway Server.

At the end of this lab, you should be able to

- Understand the benefits of integrating the Messaging Gateway with PGP and Data Loss Prevention (Network Prevent for Email)
 - Determine the key configuration requirements for integrating the Messaging Gateway, PGP, and Data Loss Prevention (Network Prevent for Email)
 - Properly configure the integration between the Messaging Gateway, PGP, and Data Loss Prevention (Network Prevent for Email)
-
-

Notes

- A brief presentation will introduce this lab session and discuss key concepts.
 - The lab will be directed and provide you with step-by-step walkthroughs of key features.
 - Feel free to follow the lab using the instructions on the following pages. You can optionally perform this lab at your own pace.
 - Be sure to ask your instructor any questions you may have.
 - Thank you for coming to our lab session.
-

About The Virtual Machines

The messaging security environment leverages virtual machines configured to demonstrate the value of the integration and provide a platform for training and testing.

There are four virtual machine images that will be required that are listed below.

Virtual Machines		
Name & Resources	Description	Username and Password
<u>EnforcedemoX64(v11)</u> Disk: 60GB RAM: 4GB	This image runs the Enforce platform and Network Prevent for SMTP. In addition it functions as the external server and mail host. After filtering, the SMG products will relay outbound messages to this host.	OS: Administrator/Protectdemo! Enforce*: Administrator/protect4 Oracle user and Oracle UID and SID: protect Oracle DB user: protect/protect *UI is available via browser favorites and https://enforcedemo64 . Password for all users: protect4
<u>PGP Universal Server</u> Disk: 10GB RAM: 1GB	This image runs the PGP Universal Gateway Server. This server will encrypt messages sent by the Symantec Messaging Gateway	PGP Universal Server UI: Administrator/protect4

<u>Symantec Messaging Gateway</u> Disk: 90GB RAM: 1.3GB	Symantec Messaging Gateway Virtual Edition, this image runs version 9.5 of the appliance software	SMG UI: Administrator/symc4now
<u>Window 7x86(V11)</u> Disk: 16GB RAM: 1GB	This image will be used to send test messages to the Messaging Gateway to trigger the encryption policy. In addition it will be used to verify and retrieve the protected message.	OS: Joe/Protectdemo! Outlook Users: juser@acme.com (internal) & larry@anothercompany.com (external)

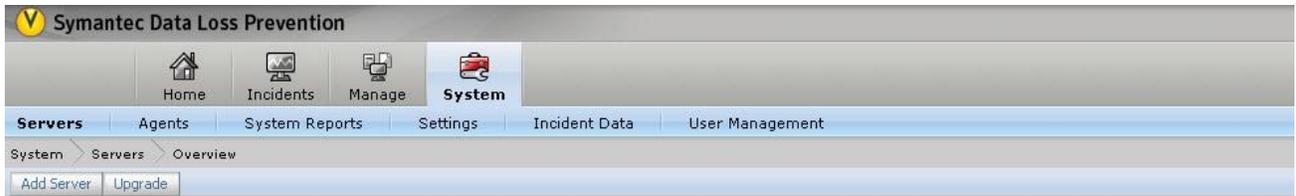
Part 1: Symantec Network Prevent Configuration

Network Prevent Server (Email) monitors and analyzes outbound email traffic and (optionally) blocks, redirects, or modifies email messages as specified in the policies. When integrating with Symantec Messaging Gateway, you should configure Network Prevent to modify the message header and allow SMG to enforce the necessary action. Configuring Network Prevent will require the following two steps:

Task1: Configure Network Prevent for reflecting mode

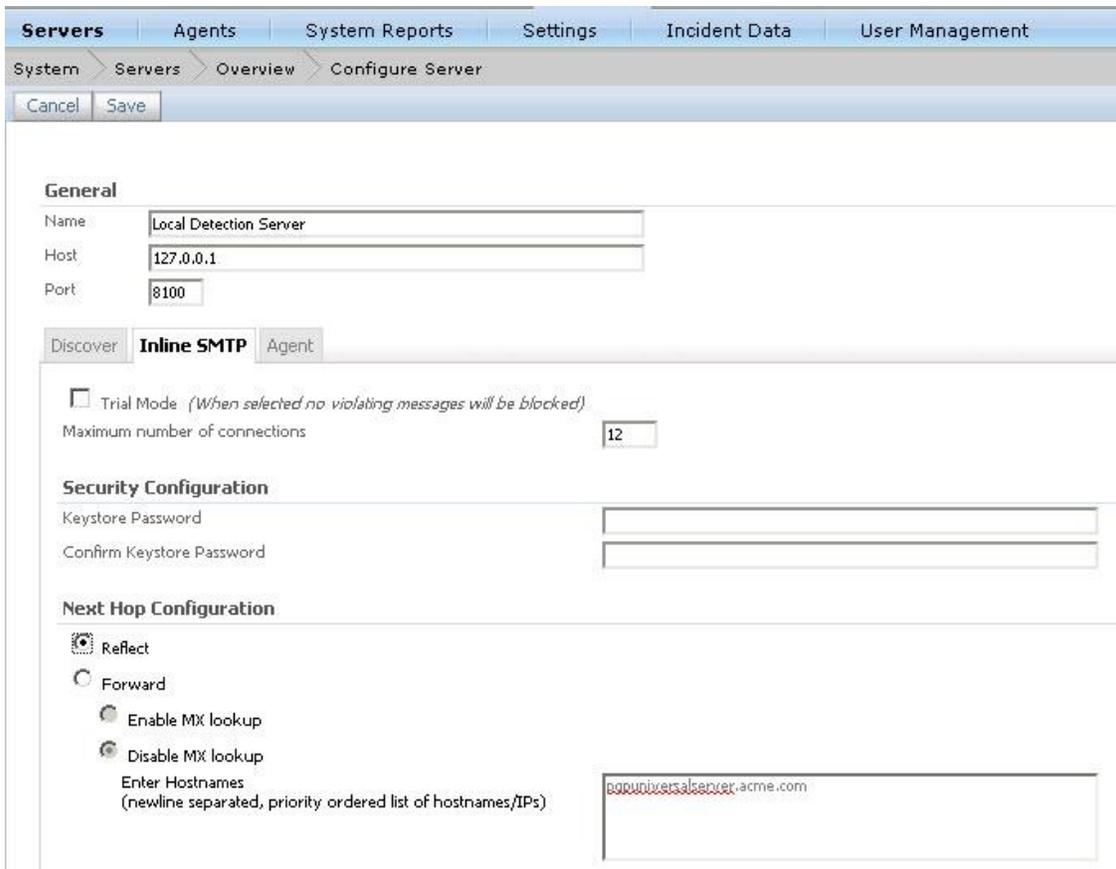
In reflecting mode, the Network Prevent Server (Email) acts as an SMTP proxy. It receives messages from an MTA, analyzes them, and then sends them back to the same MTA.

1. Log into the **EnforcedemoX64(V11)** console with the following:
 - Username: Acme\Administrator
 - Password: Protectdemo!
2. Open Mozilla Firefox.
3. Go to the Enforce UI, <https://enforcedemox64/ProtectManager/Navigate.do?menuID=default>
4. Log into the Enforce UI with the following:
 - Username: Administrator
 - Password: protect4
5. Select the System tab, under Servers, click on *Local Detection Server*.

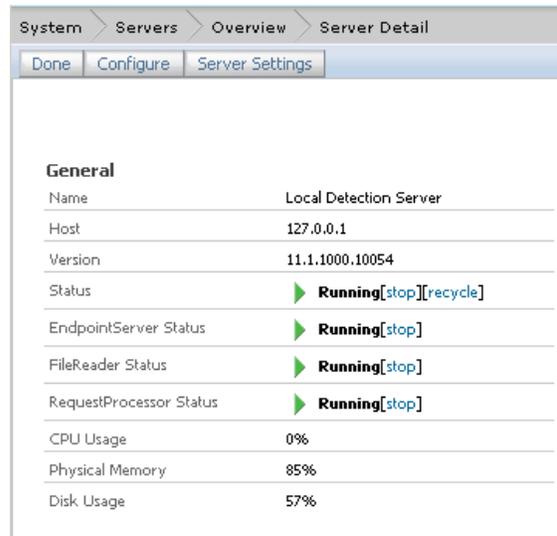


Status	Server	Version	Channels
Running	Enforce Server	11.1.1000.10054	N/A
Running	Local Detection Server	11.1.1000.10054	Network Prevent for E-mail, Endpoint, Network Discover

6. Under Server Detail, click on *Configure*.
7. Under General, select the *Inline SMTP* tab.
8. Under Next Hop Configuration, select the *Reflect* radio button.



9. Select *Save* to continue.
10. From the Overview tab, select *Local Detection Server*.
11. Under General, next to Status, click *recycle* to restart the server.



12. Select *Done* to continue.

Task 2: Configure the Encryption Policy

Network Prevent will be used to identify content that needs to be encrypted. The policies can be as complicated as identifying customer data or as simple as identifying a keyword in the subject line. Regardless of the content that is identified the key action is adding a header in the violating message so that the Message Gateway can enforce the encryption action. To add the header, complete the following:

1. From the **EnforcedemoX64(v11)** console, log into the Enforce UI with the following:
 - Username: Administrator
 - Password: protect4
2. From the Manage Tab, select *Response Rules*.
3. From the Response Rules, select *Add Response Rule*.
4. Under Choose the type of response rule to add, select *Automated Response*.
5. Click *Next* to continue.
6. Configure the rule as follows:

Manage > Policies > Response Rules > Configure Response Rule

Cancel Save

General

Rule Name: Add X-header for PGP encryption

Description: Inserts header for PGP encryption

Used in no active policies.

Conditions Add Condition

Incident Match Count: Is Greater Than or Equals: 1

Actions (executed in the order shown) <choose action type> Add Action

Network Prevent: Modify SMTP Message

Subject: Don't Modify Prepend Append Replace With

Headers:

Header 1 Name	Header 1 Value
X-Encrypt	Yes
Header 2 Name	Header 2 Value
Header 3 Name	Header 3 Value

7. Click *Save* to continue.
8. From the *Manage* Tab, select *Policy List*.
9. From the list click on the policy *Protect Data With Encryption and DLP*.

Home Incidents **Manage** System

Policies Data Profiles Discover Scanning

Manage > Policies > Policy List

Add Policy

Name	Description
*Protect Data With Encryption and DLP	Medium severity (customer data) encrypted, high severity (IP) blocked
Competitor Communications	This policy detects communications with competitors.
Confidential Documents	This policy detects company-confidential documents at risk of exposure.

10. Under *General*, next to *Status*, click on *Suspend*.

Policies | Data Profiles | Discover Scanning

Manage > Policies > Policy List > Configure Policy

Cancel Save

General

Name: *Protect Data With Encryption and DLP

Description: Medium severity (customer data) encrypted, high severity (IP) blocked

Policy Group: General Policy Group

Status: Active [suspend]

Policy Actions:
 Enable Classification Test Mode
 Maximum for Classification Test Mode Events: 100

Last Modified: 12/8/11 4:12 PM by Administrator

11. Click *Save* to continue.
12. From the Policy List, select *Add Policy*.
13. Under Choose a type of policy to add, select *Add a blank policy*.
14. Click *Next* to continue.
15. Configure the policy as follows:

General

Name: Encrypt Using PGP

Description: Identify "Encrypt" within the Subject

Policy Group: General Policy Group

Status: Active [suspend]

Policy Actions:
 Enable Classification Test Mode
 Maximum for Classification Test Mode Events: 100

16. Under Detection, select *Add Rule*.
17. Under Rule Type -> Content, select *Content Matches Keyword*
18. Click *Next* to continue.
19. Configure the rule as follows:

Manage > Policies > Policy List > Configure Policy - Edit Rule

Cancel OK

General

Rule Name: Keyword Search: [Encrypt]

Severity Add Severity

Default: High

Conditions

Content Matches Keyword

Match type: Case Sensitive Case Insensitive

Keyword Separator: Newline Comma

Match any Keyword: [Encrypt]

Keyword Proximity matching
No keyword pairs defined.

Enter in keywords or key phrases, one on each line or separated by commas. (E.g., internal use only, confidential, not for distribution)

Add Pair of Keywords

Match Conditions: On whole words only
 Check for existence (don't count multiple matches)
 Count all matches and only report incidents with at least 1 matches

Match On: Envelope
 Subject
 Body
 Attachments

Also Match: Match... Add

20. Click **OK** to continue.
21. Under **General**, select the *Response* tab.
22. From the drop down box, select the rule, *Add X-header for PGP encryption*

Detection Groups **Response**

<choose response rule> Add Response Rule

<choose response rule>

Add X-header for PGP encryption

Block Copy to Removable Media

Block Email and Send Notify Sender and ITSecurity - Internat

Block Endpoint Threat and Show Pop-up - international

Block Web Communication

Copy Stored File

Endpoint: Block and Show Pop-Up

Endpoint: Block and Show Pop-Up 2

Endpoint: Encrypt confidential data to USB

Endpoint eDAR Zip and Move (Endpoint Flexresponse)

Endpoint Quarantine File

Endpoint User Cancel for Encrypted USB

Endpoint Zip & Move (eFlexresponse)

Network: Block SMTP Email

Network: Route to PGP for encryption

Notify and Resolve

Notify End User

Notify of Critical Incident

Quarantine SMTP Email

23. Click *Add Response Rule* to continue.
24. Click **Save** to continue.

Congratulations, you have completed Part 1!

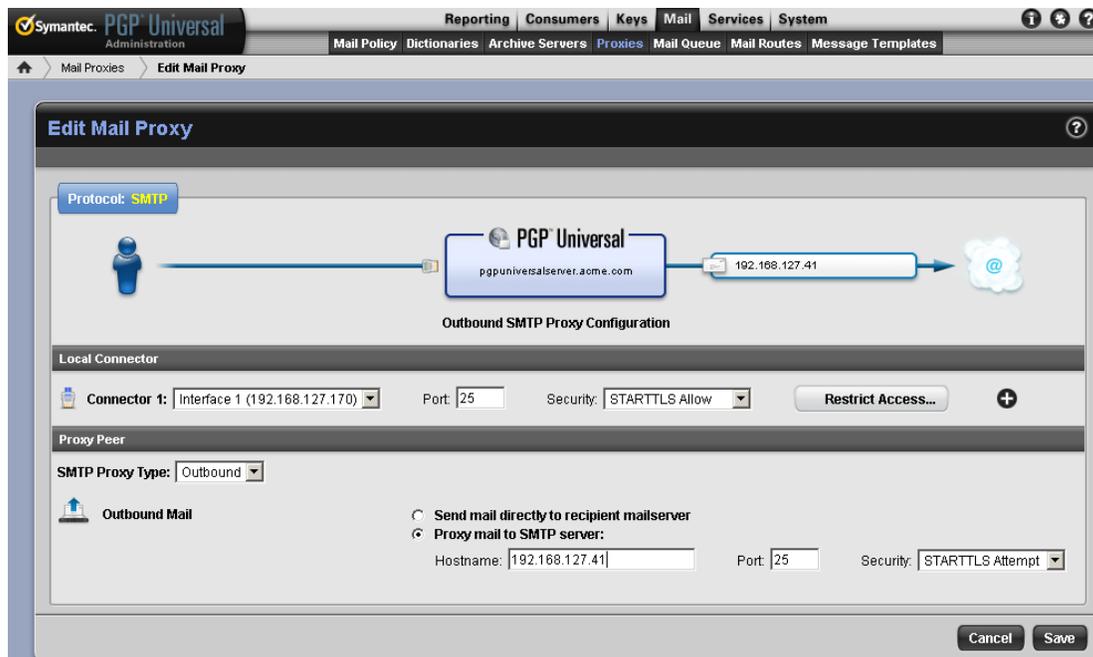
Part 2: Symantec PGP Configuration

In general when integrating SMG, DLP, and PGP, both DLP and PGP should communicate through the Messaging Gateway. Therefore, any messages received by PGP should be encrypted. In addition the Messaging Gateway should act as the primary server to send messages outside of the organization, as a result similar to the DLP configuration, PGP should route any encrypted message or notification through the Messaging Gateway.

Task 1: Configure PGP to Route Outbound Messages through the Messaging Gateway

In order to route messages that PGP receives to the Messaging Gateway, you will need to configure an SMTP proxy within PGP. To configure the proxy settings complete the following:

1. From the **EnforcedemoX64(v11)** console, open Mozilla Firefox.
2. Go to the PGP UI, <https://pgpuniversalserver:9000/omc/GetLoginScreen.uevent>
3. Log into the PGP UI with the following:
 - Username: Administrator
 - Password: protect4
4. From the Mail Tab, select *Proxies*.
5. From the list of Proxies, select *SMTP*.
6. Edit the Mail Proxy as follows:



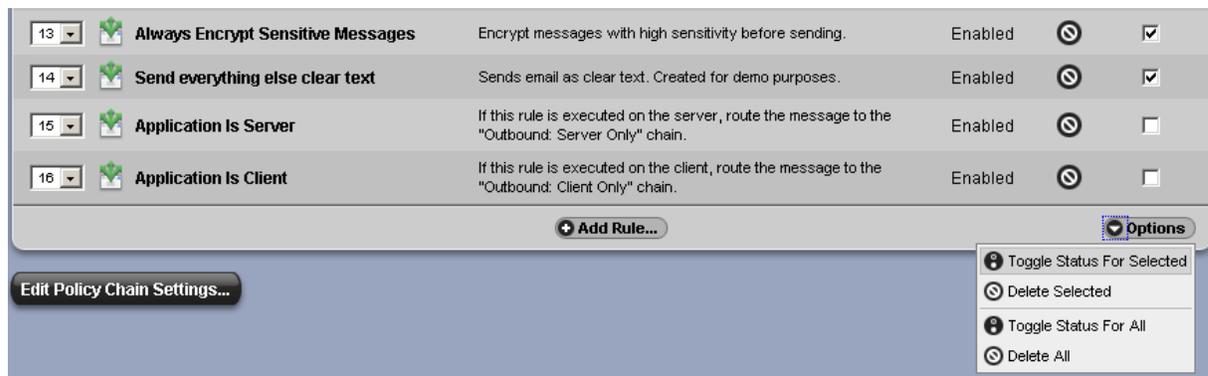
7. Click *Save* to continue.
8. From the Mail Tab, select *Mail Routes*.
9. Select the domain, *anothercompany.com*.
10. Replace the Hostname/IP with *192.168.127.41*.
11. Click *Save* to continue.

Task 2: Disable the Outbound Policies

The PGP image used provides flexibility in integrating directly with DLP for demo purposes. However, as a general rule SMG will manage which messages should be encrypted and relay only those messages to

PGP. Therefore any message received by PGP should be encrypted. To avoid policy confusion, the PGP content policies should be disabled. To disable the content policies complete the following:

1. Go to the PGP UI, <https://pgpuniversalserver:9000/omc/GetLoginScreen.uevent>
2. Log into the PGP UI with the following:
 - Username: Administrator
 - Password: protect4
3. From the Mail Tab, select *Mail Policy*.
4. From the list of Mail Policies, select *Outbound*.
5. Disable the following 3 policies:
 - a) Encrypt based on DLP header
 - b) Always Encrypt Sensitive Messages
 - c) Send everything else clear text
6. To disable the policies, select the check box next to each policy.
7. Towards the bottom part of the page, select the *Options* drop-down box.
8. Select *Toggle Status for Selected*

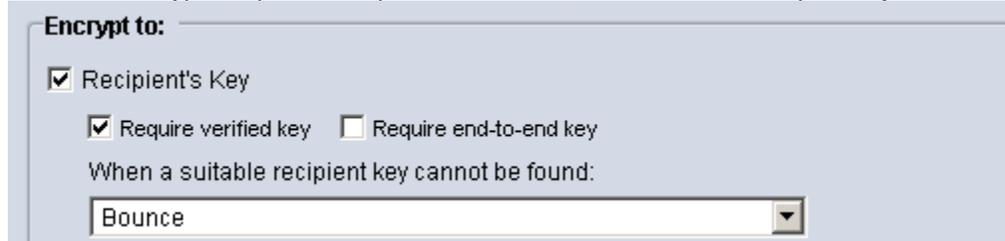


9. Click *Ok* to continue.

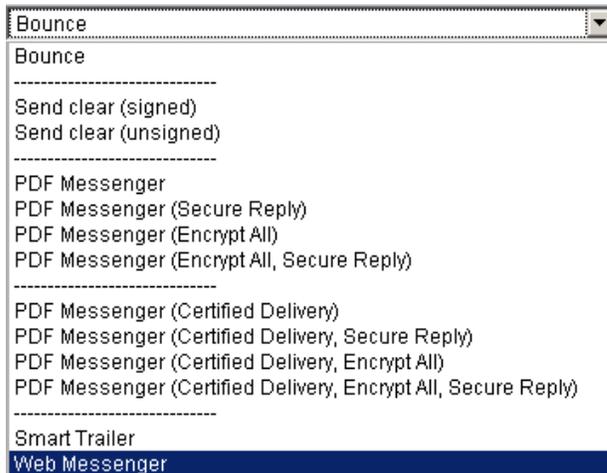
Task 3: Edit the Outbound Server policy

By default you will want any message received by PGP to be encrypted. In addition to disabling the Outbound policies, you will need to allow the ability to encrypt any message where the user does not have a key. To allow this, complete the following:

1. From the PGP UI, go to the *Mail* Tab.
2. Select Mail Policy, and from the policy list select *Outbound: Server Only*
3. Click on the rule, *Send Message*.
4. Select the *Actions* Tab.
5. Under *Encrypt to*, open the drop-down box under, *When a suitable recipient key cannot be found*



6. Open the drop-down box and select *Web Messenger*.



7. Click **Save** to continue.

Congratulations, you have completed Part 2!

Part 3: Symantec Messaging Gateway Configuration

The Messaging Gateway is used to manage routing of all messages destined to either the DLP or PGP servers. In addition as a good best practice it should be the main email gateway that sends messages to the Internet. The Messaging Gateway is designed for direct integration with DLP and users can enable the DLP Connect option to route all outbound messages automatically. However when integrating with PGP, users will need to configure policy routes leveraging the advanced content filtering engine within SMG. To complete the integration we will need to enable the DLP Connect option and configure content filtering policies by referencing information in Part 1 and 2.

Task1: Enable DLP Connect

When enabling DLP Connect, all outbound messages will be routed to the Network Prevent server. To enable DLP connect complete the following tasks.

1. From the **EnforcedemoX64(v11)** console, open Mozilla Firefox.
2. Go to the SMG UI, <https://192.168.127.40/brightmail>
3. Log into the SMG UI with the following:
 - Username: admin
 - Password: symc4now
4. From the Content Tab, under Settings, select *DLP Connect*.
5. Edit the DLP Connect settings as follows:

Symantec Data Loss Prevention Setup

Connect the Symantec Messaging Gateway with a Symantec Data Loss Prevention (DLP) deployment. Enable and configure DLP for one or more outbound Scanners. To configure different settings for different Scanners, enable and save settings for each Scanner separately.

Connection Settings

Enable DLP for the outbound Scanner host: Local Host

Route Outbound Mail to DLP Servers

Route outbound mail to the following IP addresses or hostnames for DLP filtering:

<input type="checkbox"/> Host or IP Address	Port	MX Lookup	Preference (1-100)
<input type="checkbox"/> 192.168.127.130	10025	<input type="checkbox"/>	10

Enable bypass when all DLP servers are unreachable

Accept Scanned Mail from DLP Servers

Accept outbound mail from the following DLP server IP addresses.

<input type="checkbox"/> IP Address
<input type="checkbox"/> 192.168.127.130

Apply to all outbound Scanner hosts

Save Cancel

6. Click Save continue.

Task2: Create a Policy to Route Messages to PGP

For outbound filtering, leveraging SMG, DLP and PGP two policies will be required. Since all outbound mail is automatically routed to Network Prevent, you will not need to create a policy to route mail to Network Prevent. However, when the message is sent back from Network Prevent, the Messaging Gateway will need to enforce the action determined by Network Prevent. In this case if the header that we configured in Part 1 is inserted into the message, SMG will need to route that message to PGP for encryption. In order to create the policy, complete the following:

1. Go to the SMG UI, <https://192.168.127.40/brightmail>
2. Log into the SMG UI with the following:
 - Username: admin
 - Password: symc4now
3. From the Content Tab, under Policies, select *Email*.
4. Under Email Content Filtering Policies, select *Add*.
5. Under Content Filtering Police Templates, select *Blank* and click *Select* to continue.
6. Edit the first part of the Email Content Filtering Policy as follows:

Add Email Content Filtering Policy

Configure an Email Content Filtering Policy.

Email Content Filtering Policy

Policy name:

Track violations of this policy in the dashboard and reports

Conditions

Apply to:

Which of the following conditions must be met:

7. Under Conditions, click *Add* to customize the condition builder.
8. Based on Part 1, edit the Content Filtering Policy Condition as follows:

Content Filtering Policy Condition

Text in the Subject, Body or Attachments:

Contains or more words from dictionary:

matches regular expression

matches pattern

Matches data in the Record Resource:

View:

Minimum number of occurrences required:

Text in this specific part of the message:

Header name:

The message header:

contains or more occurrences of

starts with

matches regular expression

matches pattern

Text in the specific part of the message header:

from dictionary:

from dictionary:

Message size is equal to bytes

File Metadata:

Is in the Attachment List:

Has a filename containing:

Is MIME type:

contains a filename from dictionary:

contains a file extension from dictionary:

For all messages

9. Click *Add Condition* to continue.
10. Under Actions, click *Add* to add an action.
11. From the drop-down box, select *Route the Message*
12. Edit the action to route the message to the PGP server, as follows:

13. Click *Add Action* to continue.
14. Under Apply to the following policy groups, select *Default*
15. Click *Save* to create the policy.
16. Move the newly created policy to the top of the list.

Email Content Filtering Policies				
Manage content filter policies for your organization.				
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/>				
<input type="checkbox"/>	Email Content Filtering Policies	Enabled	Applied To	Number of Groups
<input type="checkbox"/>	Protect Message with PGP	✓	Outbound only	1
<input type="checkbox"/>	Delete Executable Files Violations	✓	Outbound only	0
<input type="checkbox"/>	Delete Email Policy Violations	✓	Outbound only	0
<input type="checkbox"/>	Legal Disclaimer	✓	Outbound only	0

Task3: Create a Policy to Prevent a Mail Loop with PGP

The second policy is required to prevent a mail loop with PGP. In a typical production scenario all messages should be routed to the Messaging Gateway for final delivery to the Internet. When a message is routed from SMG to PGP, PGP will either generate a notification that a message has been encrypted or encrypt the original message and send it to the Messaging Gateway. In this scenario SMG may detect that the message contains the original header of X-Encrypt and resend that message back to PGP. To ensure that messages received by PGP are not sent back, create the following policy:

1. Go to the SMG UI, <https://192.168.127.40/brightmail>
2. Log into the SMG UI with the following:
 - Username: admin
 - Password: symc4now
3. From the Content Tab, under Policies, select *Email*.
4. Under Email Content Filtering Policies, select *Add*.
5. Under Content Filtering Police Templates, select *Blank* and click *Select* to continue.
6. Edit the first part of the Email Content Filtering Policy as follows:

Add Email Content Filtering Policy

Configure an Email Content Filtering Policy.

Email Content Filtering Policy

Policy name:

PGP Loop Prevention

Track violations of this policy in the dashboard and reports

Conditions

Apply to:

Inbound and outbound messages

Which of the following conditions must be met:

Any

7. Under Conditions, click *Add* to customize the condition builder.
8. Edit the Content Filtering Policy Condition as follows:

Content Filtering Policy Condition

Text in the Subject, Body or Attachments:

Contains or more words from dictionary:

ABA Routing Number Keywords (Premiu

matches regular expression

matches pattern

Matches data in the Record Resource:

View:

Minimum number of occurrences required:

1

Text in this specific part of the message:

Header name:

The message header:

contains 1 or more occurrences of

starts with

matches regular expression

matches pattern

Message header

Received

exists

192.168.127.170

Credit Card (Basic)

Text in the specific part of the message header:

contains Email address from dictionary:

Envelope recipient

ABA Routing Number Keywords (Premiu

Message size

is equal to

bytes

File Metadata:

Is in the Attachment List:

Has a filename containing:

Is MIME type:

contains a filename from dictionary:

contains a file extension from dictionary:

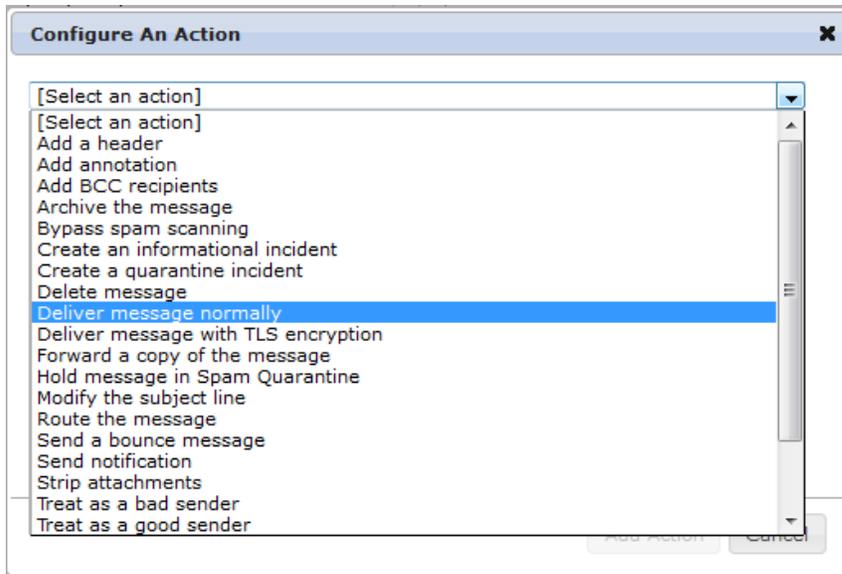
Archive Files

ABA Routing Number Keywords (Premiu

ABA Routing Number Keywords (Premiu

For all messages

9. Click *Add Condition* to continue.
10. Under Actions, click *Add* to add an action.
11. From the drop-down box, select *Deliver the Message Normally*



12. Click *Add Action* to continue.
13. Under Apply to the following policy groups, select *Default*
14. Click *Save* to create the policy.
15. Move the newly created policy to the top of the list (Make sure it is the first policy listed).

Email Content Filtering Policies

✔ The policy precedence has been changed.

Manage content filter policies for your organization.

<input type="checkbox"/>	Email Content Filtering Policies	Enabled	Applied To	Number of Groups
<input type="checkbox"/>	PGP Loop Prevention	✔	Inbound and Outbound	1
<input type="checkbox"/>	Protect Message with PGP	✔	Outbound only	1
<input type="checkbox"/>	Delete Executable Files Violations	✔	Outbound only	0
<input type="checkbox"/>	Delete Email Policy Violations	✔	Outbound only	0
<input type="checkbox"/>	Legal Disclaimer	✔	Outbound only	0

Congratulations, you have completed Part 3!

Part 4: Testing the Integration

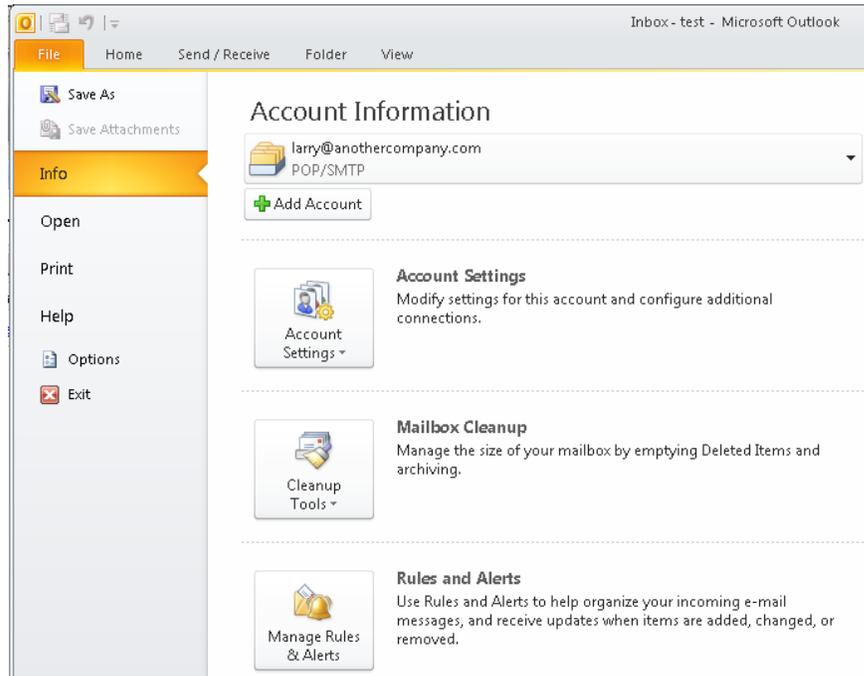
Now that you have configured the integration, test to confirm that each component is operating properly. You will be able to view the details in both the Message Audit Logs of the Messaging Gateway, the Incident reports of the Enforce platform, and the MTA logs of the PGP server. Finally as an end-user you will be able to review the message by access the encrypted message from the PGP portal.

Task 1: Configure Outlook

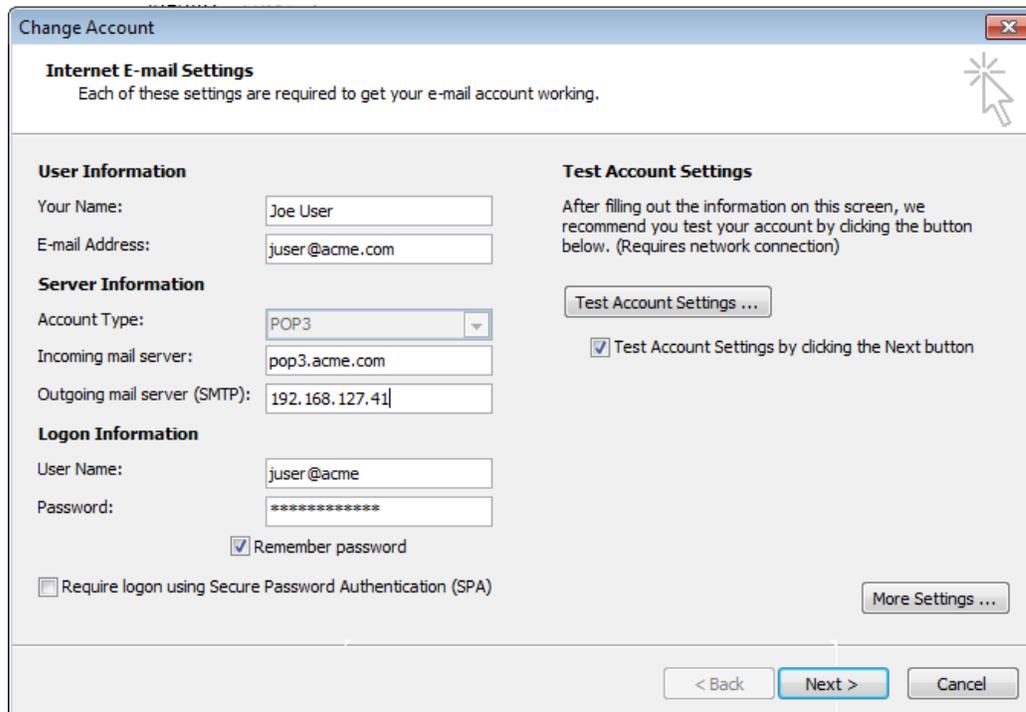
Before testing that the Network Prevent policy works, you will need to configure Outlook to relay outbound messages through the Messaging Gateway. Complete the following steps to re-route messages:

1. From the **Windows 7x86(v11)** Image, log-in using the following::
 - Username: Joe
 - Password: Protectdemo!

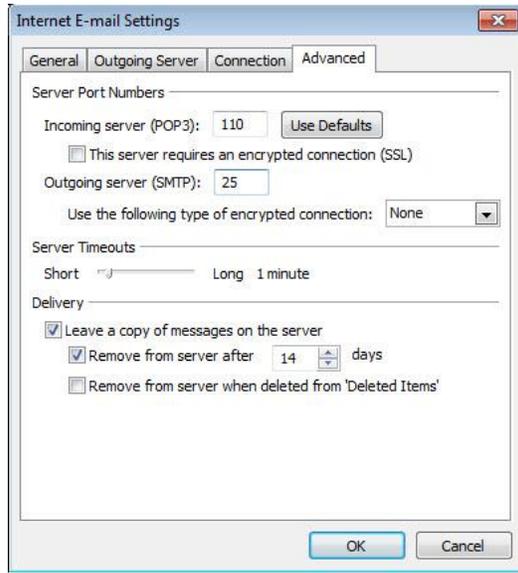
2. Open Microsoft Outlook.
3. Select the *File* tab.
4. Within the Info section, open the drop-down box for Account Settings and select *Account Settings*.



5. Under Name, select juser@acme.com, and from the menu icons click *Change*.
6. Under Server Information, edit the Outgoing mail server (SMTP) option as follows:



7. Click *More Settings*.
8. Select the *Advanced* tab.
9. Next to Outgoing server (SMTP), enter 25.

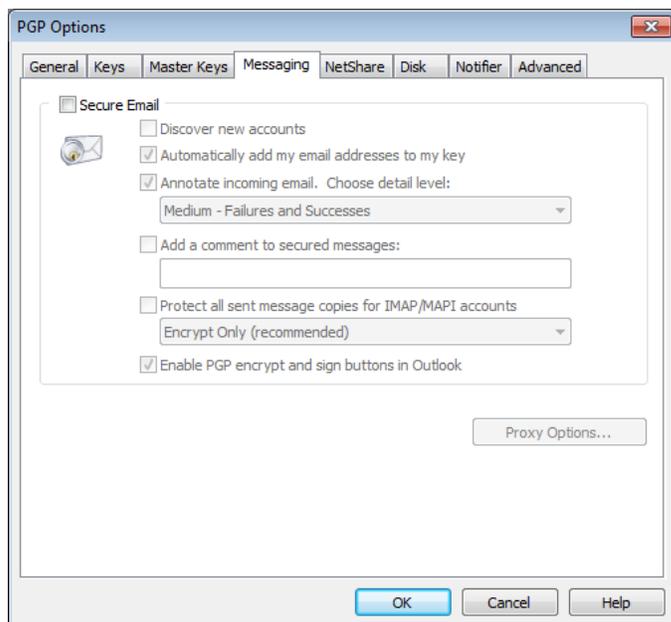


10. Click *Next* to continue.
11. Click *Finish* to continue, and close the Account Settings pop-up.

Task 2: Disable PGP Secure Desktop Email

The images currently used are configured to allow testing of other PGP solutions. For the purpose of the lab you will need to disable the PGP Secure Email Proxying. Remember if you intend to leverage the same image to demonstrate PGP desktop features, turn the Secure Email option on after completing the lab. To disable the Secure Email on the desktop complete the following:

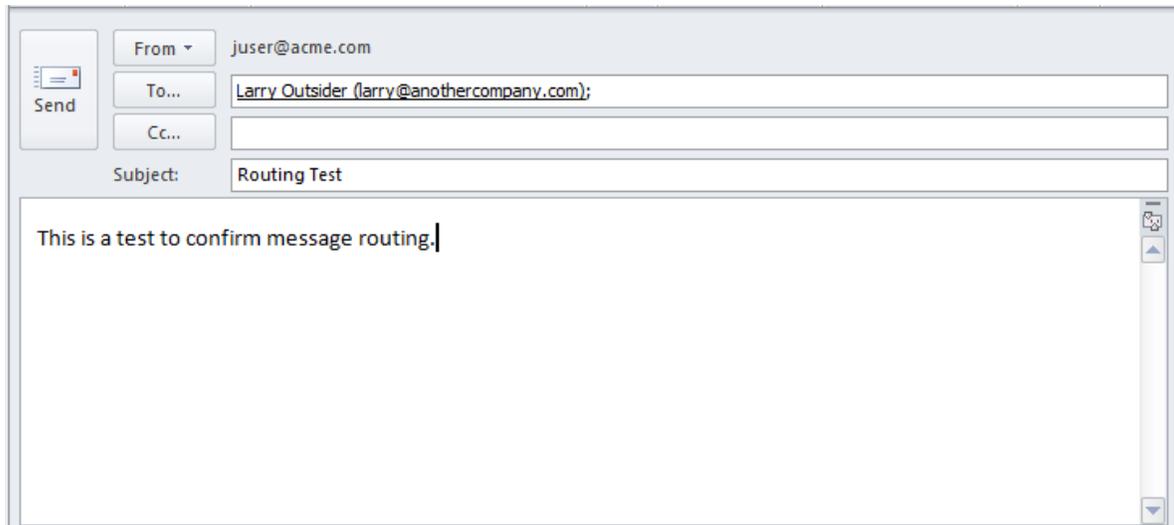
1. From the **Windows 7x86(v11)** Image, open the *Start Menu*.
2. Select *PGP Desktop*.
3. From the Menu Bar, select *Tools*, and go to *Options*.
4. Select the *Messaging* Tab.
5. Uncheck the box next to *Secure Email*.
6. Click *OK* and close PGP Desktop.



Task 3: Message Route Test

You should be able to send a message to test that mail is relayed through the Messaging Gateway. Using Microsoft Outlook and the user Joe Kerr, send a test message to larry@anothercompany.com. This test is intended to simulate outbound mail going where jkerr@acme.com is the internal user and larry@anothercompany.com is the external user. Complete this task as follows:

1. From the Microsoft Outlook, click *New E-mail*.
2. Edit the email as follows:



3. Click *Send* to continue.
4. You have two options to help verify that the message was routed properly:
 - a) From Microsoft Outlook.
 - i. Go to larry@anothercompany.com's Inbox
 - ii. From the ribbon click on *Send/Receive All Folders*.
The message should arrive in the inbox.
 - b) From the Messaging Gateway Console
 - i. From the Status tab, under SMTP, select *Message Audit Logs*
 - ii. Under Search Criteria, Select Recipient and search for larry@anothercompany.com.
 - iii. You should see a list of entries. Select the most recent entry and review the Delivery and Verdict details.
Leveraging the Message Audit Logs is a good way to help troubleshoot issues related to message delivery.

Message Audit Logs

Find messages using custom search criteria. You must enter a value in the Mandatory Type and Value fields.

Filter

Host: Time range:
Mandatory filter: *Searches spanning multiple days may cause longer search times
Mandatory filter value:
Optional filter:
Optional filter value:

File Encoding: CSV Delimiter: Entries per page: Display: of 5

Time	From	To	Original Subject	Verdict	Actions
Wednesday, Dec 21, 2011 03:04:22 PM PST	juser@acme.com	larry@anothercompany.com	routing test	None	Deliver message normally

Task 4: Policy Violation Test

Similar to the previous task you will send a message, but this message should contain content that will trigger the DLP policy and cause the message to be routed to PGP. Finally you should be able to review the message through the PGP portal. Complete the following steps to test the full integration:

1. From the Microsoft Outlook, click *New E-mail*.
2. Edit the email as follows, remember the subject must contain the term "[Encrypt]":

From:

To:

Cc:

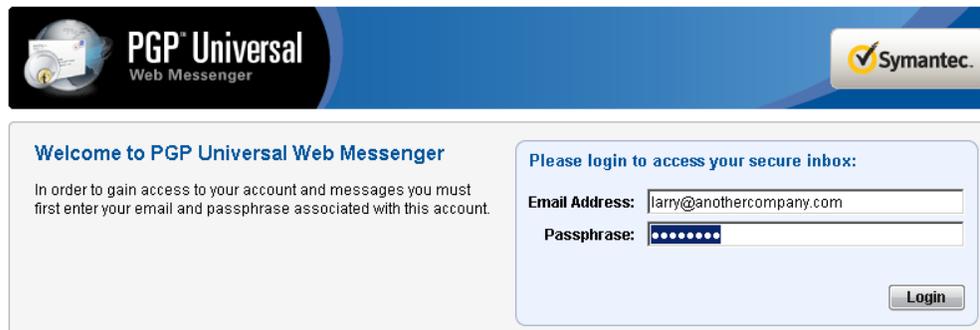
Subject:

This information I type is intended to trigger the encryption rule.
Thanks,
J

3. Click *Send* to send the message.
4. Go to larry@anothercompany.com's inbox.
5. From the ribbon click on *Send/Receive All Folders*.
The notification should have been delivered, indicating that a secured message is available for review.
6. Click on the URL within the message.



7. You should be redirected to the web browser.
8. Log into the portal with the following username and password:
 - Username: larry@anothercompany.com
 - Password: protect4



9. To view the message, select the Subject.



Task 5: Reviewing Logs

In addition if you would like to better understand the routing flow, and review the entries recorded with SMG, DLP, and PGP, complete the following:

Reviewing SMG Entries

1. From the EnforcedemoX64(v11) console, go to the SMG UI, <https://192.168.127.40/brightmail>
2. Log into the SMG UI with the following:
 - Username: admin
 - Password: symc4now

- From the Status tab, under SMTP, select *Message Audit Logs*
- Under Search Criteria, Select Recipient and search for larry@anothercompany.com.
- You should see the following three entries related to the test:

Message Audit Logs

Find messages using custom search criteria. You must enter a value in the Mandatory Type and Value fields.

Filter

Host: Time range:
 Mandatory filter: *Searches spanning multiple days may cause longer search times
 Mandatory filter value:
 Optional filter:
 Optional filter value:

File Encoding: CSV Delimiter: Entries per page: Display: of 6

Time ▼	From	To	Original Subject	Verdict	Actions
Wednesday, Dec 21, 2011 03:25:36 PM PST	juser@acme.com	larry@anothercompany.com	pgp universal secured m...	Content Filtering violati...	Deliver message normally
Wednesday, Dec 21, 2011 03:25:35 PM PST	juser@acme.com	larry@anothercompany.com	(none)		Abort message
Wednesday, Dec 21, 2011 03:25:17 PM PST	juser@acme.com	larry@anothercompany.com	[encrypt] important inf...	Content Filtering violati...	Route the message

- The entries should be read from bottom to top.
- The first entry denotes that the message was first routed to DLP, the header was inserted by Network Prevent and the message was routed to PGP.

Recipient Data

Intended recipient: larry@anothercompany.com

Verdict: [Details](#)

Verdict	Filter Policy	Policy Group	Details	Message Part	Matching Text
Content Filtering violation: Protect Message with PGP	protect message with pgp	default	None	header — x-encrypt	yes

Tracker: [Details](#)

Actions taken: Route the message

Delivery: [Details](#)

Delivered To	Delivered with TLS	Delivery Time	Recipient
192.168.127.130:10025	No	Wednesday, Dec 21, 2011 03:25:26 PM PST	larry@anothercompany.com
192.168.127.170:25	No	Wednesday, Dec 21, 2011 03:25:36 PM PST	larry@anothercompany.com

- The second entry regarding the “Abort Message” action can be ignored.
- The third entry denotes that the Web Messenger notification triggered the loop prevention policy and was routed to the final recipient.

Reviewing DLP Entries

- Log into the **DLP console**.
- Select the Incidents Tab, and click on *Network*.
- Under Network Reports, select *Incidents – New*.
- The policy violation should be listed.

Incidents Manage System

Network Endpoint Discover Classification

Save Send Export Delete Report

Filter

Status: Equals New Severity: High Low Medium Info Apply

Date: Last 30 Days

Advanced Filters & Summarization

Applied Filters

Status Equals New Date Last 30 Days Severity Is Any Of High(5), Medium(0), Low(0), Info(0)

Incident Actions 1-5 of 5 Show All Select All

Type	Subject / Sender / Recipient(s)	Sent	ID / Policy	Matches	Severity	Status
<input type="checkbox"/>	Subject: [Encrypt] Important Information Sender: juser@acme.com Recipient: larry@anothercompany.com	12/21/11 2:31 PM	00001564 Encrypt Using PGP	1	High	New
<input type="checkbox"/>	Subject: [Encrypt] Important Information Sender: juser@acme.com Recipient: larry@anothercompany.com	12/21/11 2:17 PM	00001563 Encrypt Using PGP	1	High	New

5. Click on the current violation to review its details.

Reviewing PGP Entries

1. Log into the **PGP console**.
2. Select the Reporting Tab, and click on *Logs*.
3. You should see log entries similar to the following, which indicate that a message from the Messaging Gateway was received, the message triggered a policy, and that the Web Messenger notification was sent.

Symantec PGP Universal Administration

Reporting Consumers Keys Mail Services System

Overview Graphs Logs

System Logs

System Logs Refresh

Log: Mail Search: Search

Display: Information Regular expressions advanced

Wed Dec 21, 2011 at 2:32:14 PM 1 page

Message	Time
SMTP-00002: connection from 192.168.127.41:42453 closed	Wed Dec 21, 2011 at 2:32:14 PM -08:00
SMTP-00002: recipient 1/1 (larry@anothercompany.com): sending Web Messenger message	Wed Dec 21, 2011 at 2:32:09 PM -08:00
SMTP-00002: recipient larry@anothercompany.com: policy rule match: chain: "Outbound: Server Only", rule: "Send Message"	Wed Dec 21, 2011 at 2:32:09 PM -08:00
SMTP-00002: recipient larry@anothercompany.com: policy rule match: chain: "Outbound", rule: "Application Is Server"	Wed Dec 21, 2011 at 2:32:09 PM -08:00
SMTP-00002: recipient larry@anothercompany.com: policy rule match: chain: "Default", rule: "Outbound Server Mail"	Wed Dec 21, 2011 at 2:32:09 PM -08:00
SMTP-00002: message <001701ccc030\$4dd1f3b0\$e975db10\$@acme.com> from juser@acme.com (1 recipient):	Wed Dec 21, 2011 at 2:32:08 PM -08:00
SMTP-00002: SMTP connection from 192.168.127.41:42453 (local address is 192.168.127.170:25)	Wed Dec 21, 2011 at 2:32:00 PM -08:00

Congratulations, you have completed Part 4!