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**
EnforcedemoX64(v11) 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
PGP Universal Server 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

Symantec Messaging Gateway Disk: 90GB RAM: 1.3GB	Symantec Messaging Gateway Virtual Edition, this image runs version 9.5 of the appliance software	**SMG UI:** Administrator/symc4now
Window 7x86(V11) 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:

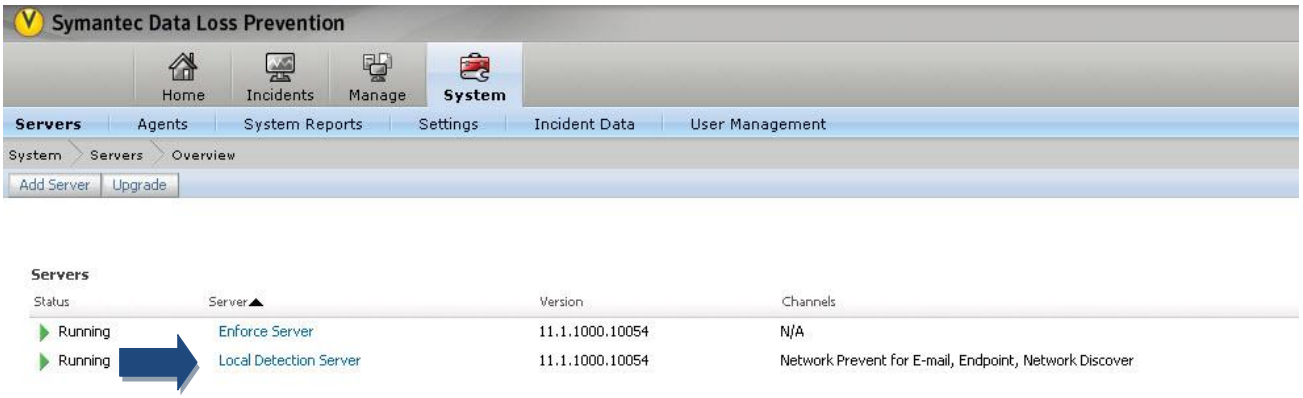
Task1: Configure Network Prevent for reflecting mode

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.

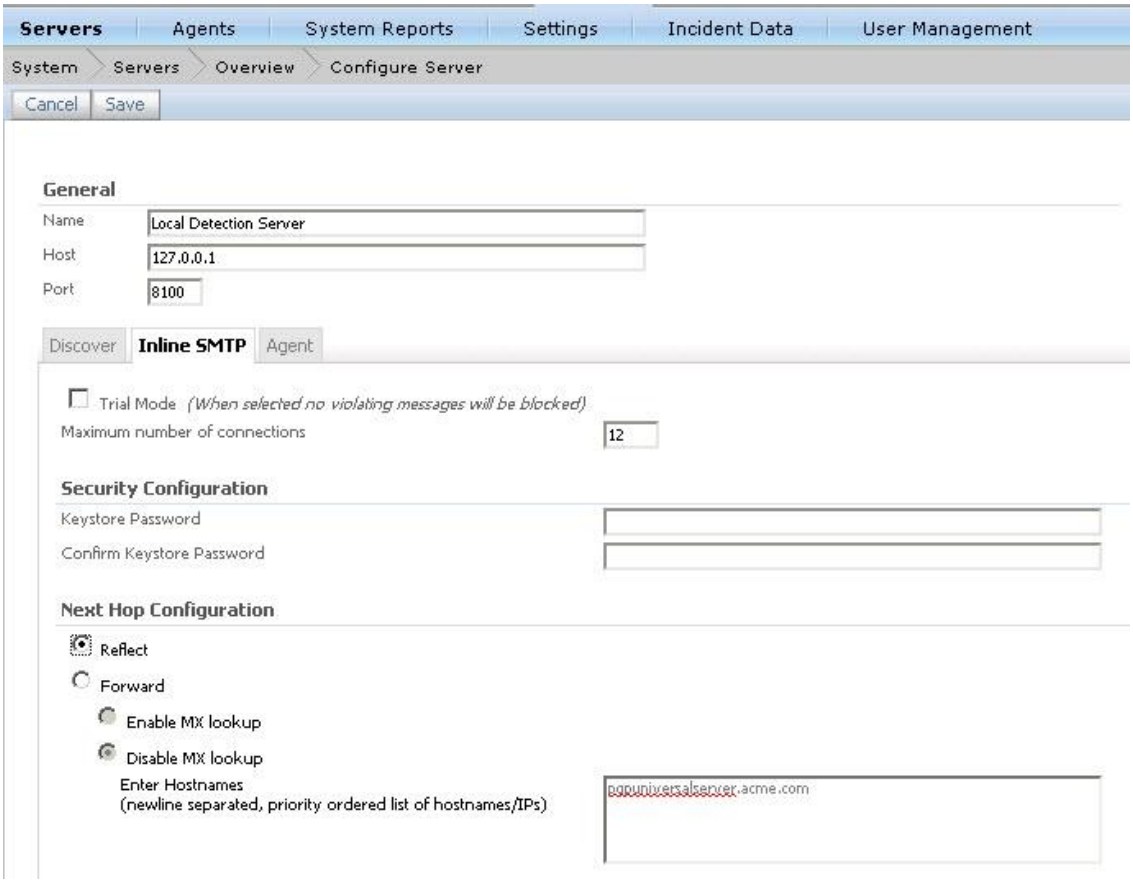
1. Log into the **EnforcedemoX64(V11)** console with the following:
    - Username: Acme\Administrator
    - Password: Protectdemo!

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

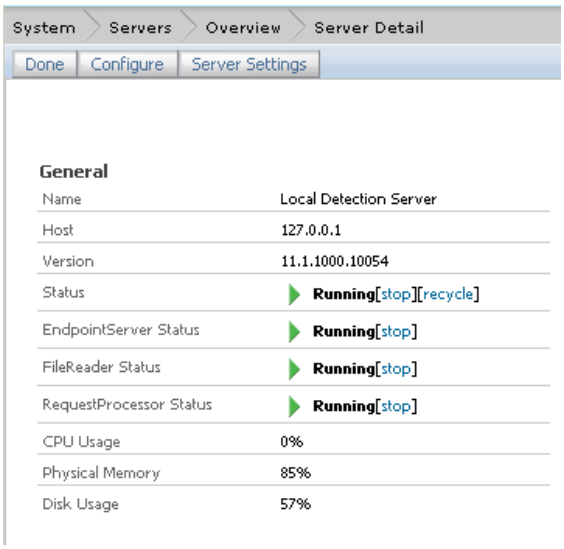
5. Select the System tab, under Servers, click on *Local Detection Server*.



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.



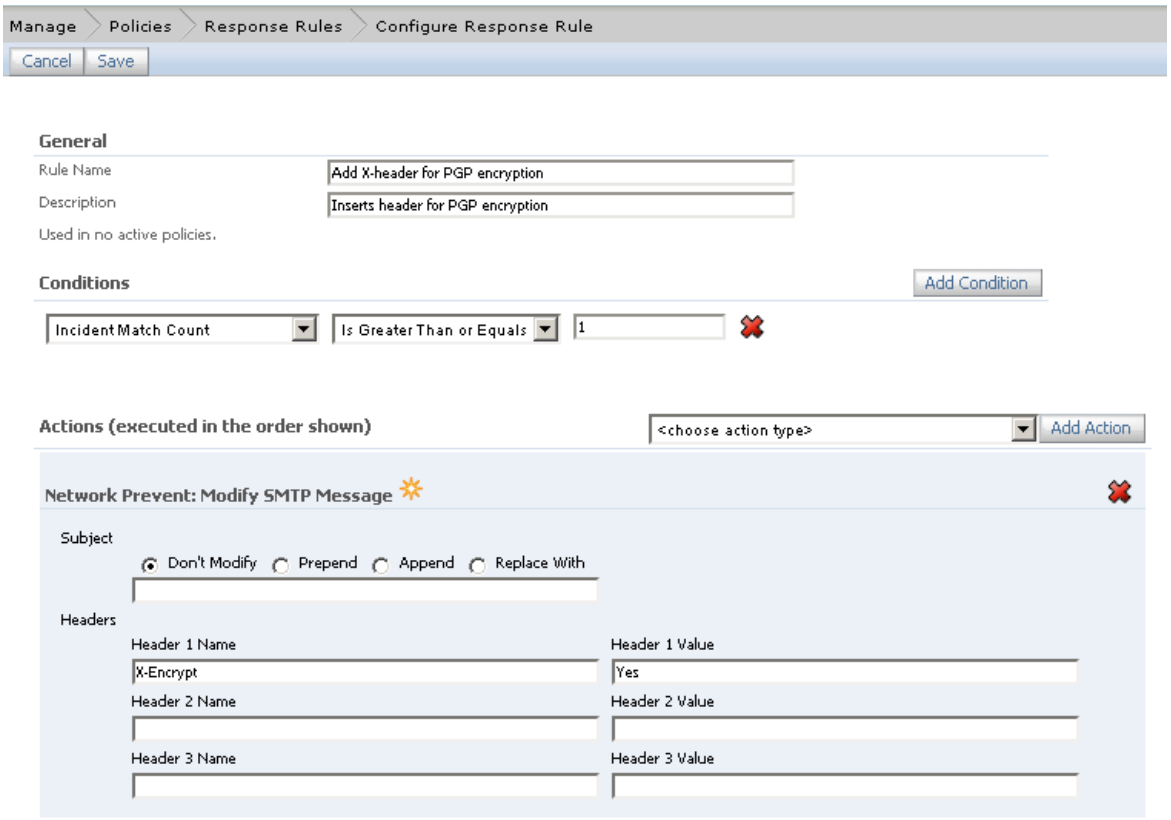
12. Select *Done* to continue.

Task 2: Configure the Encryption Policy

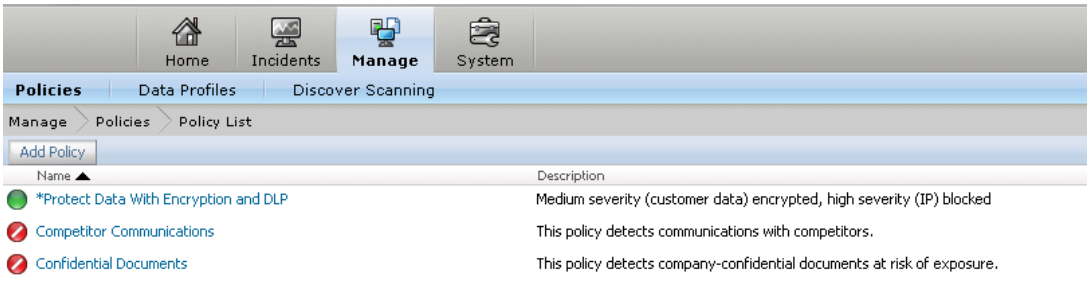
Network Prevent will be used to identify content that needs to be encrypted. The policies can be as complicated as identifying customer data or as simple as identifying a keyword in the subject line. Regardless of the content that is identified the key action is adding a header in the violating message 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

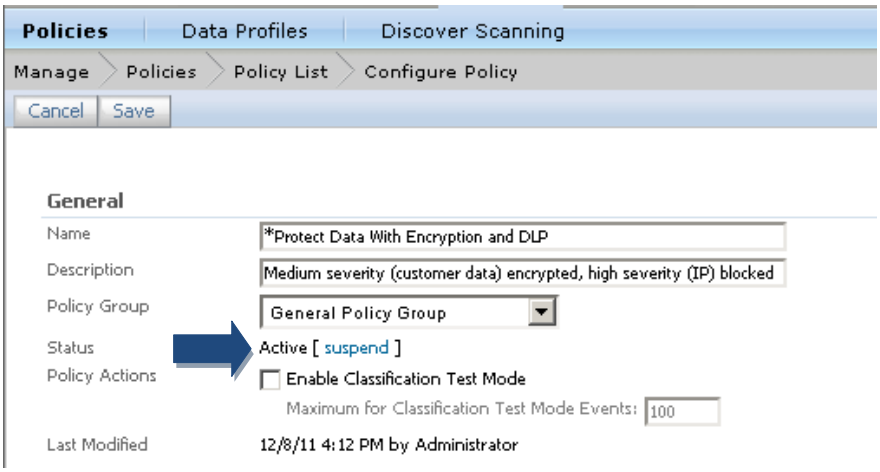
2. From the Manage Tab, select *Response Rules*.
3. From the Response Rules, select *Add Response Rule.*
4. Under Choose the type of response rule to add, select *Automated Response.*
5. Click *Next* to continue.
6. Configure the rule as follows:



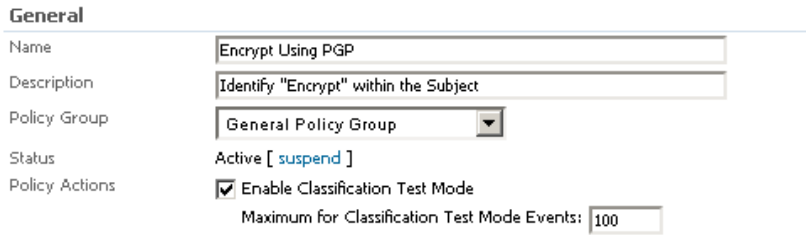
7. Click *Save* to continue.
8. From the Manage Tab, select *Policy List*.
9. From the list click on the policy *Protect Data With Encryption and DLP*.



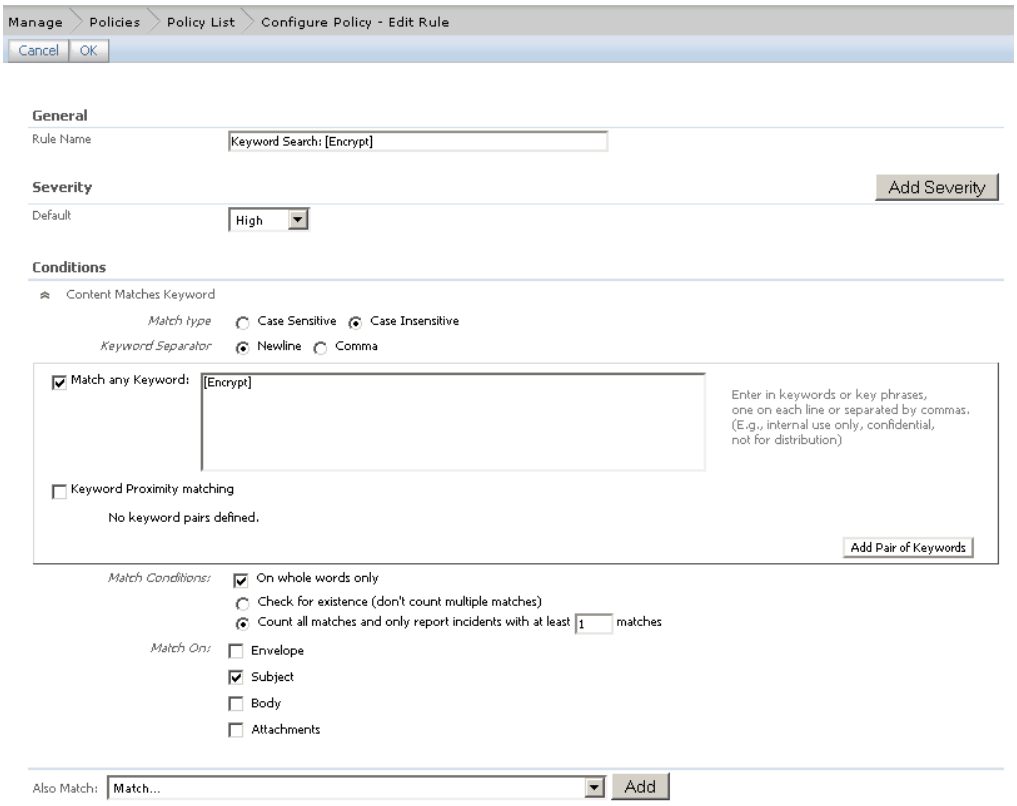
10. Under General, next to Status, click on *Suspend.*



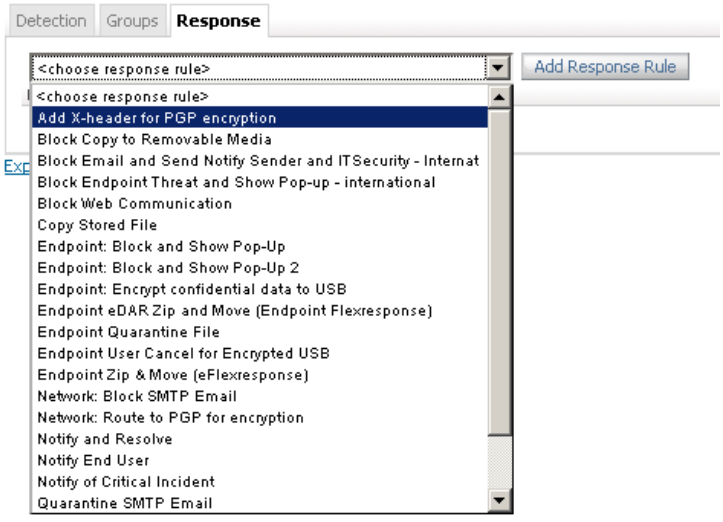
11. Click *Save* to continue.
12. From the Policy List, select *Add Policy.*
13. Under Choose a type of policy to add, select *Add a blank policy.*
14. Click *Next* to continue.
15. Configure the policy as follows:



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:



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*



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

Congratulations, you have completed Part 1!

Part 2: Symantec PGP Configuration

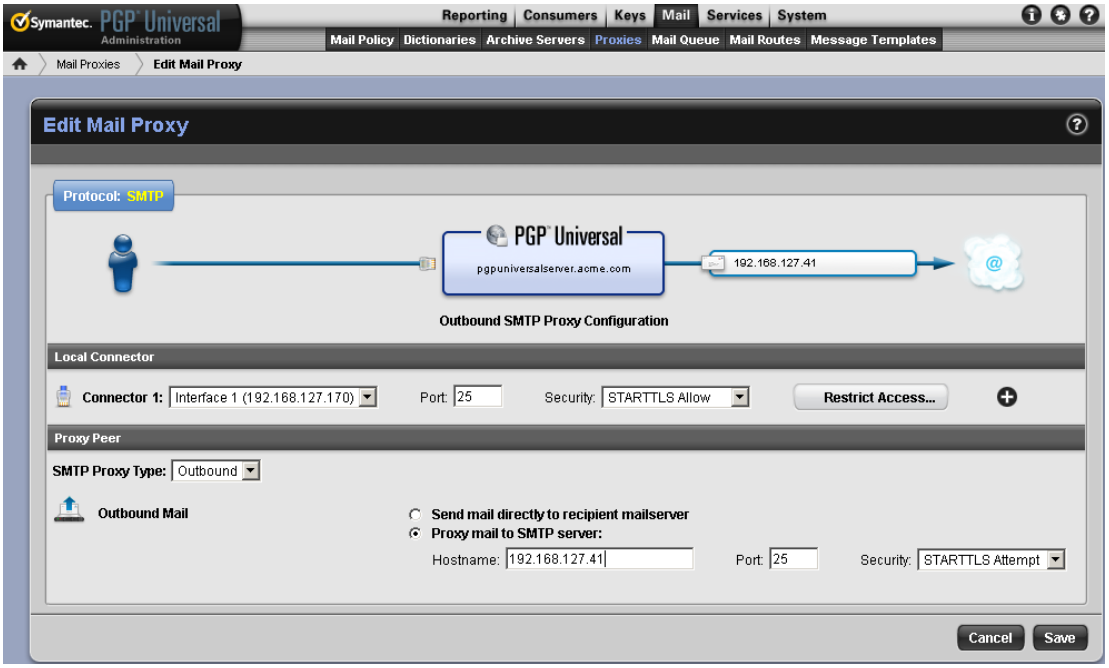
In general when integrating SMG, DLP, and PGP, both DLP and PGP should communicate through the Messaging Gateway. Therefore, any messages received by PGP should be encrypted. In addition the Messaging Gateway should act as the primary server to send messages outside of the organization, as a result similar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

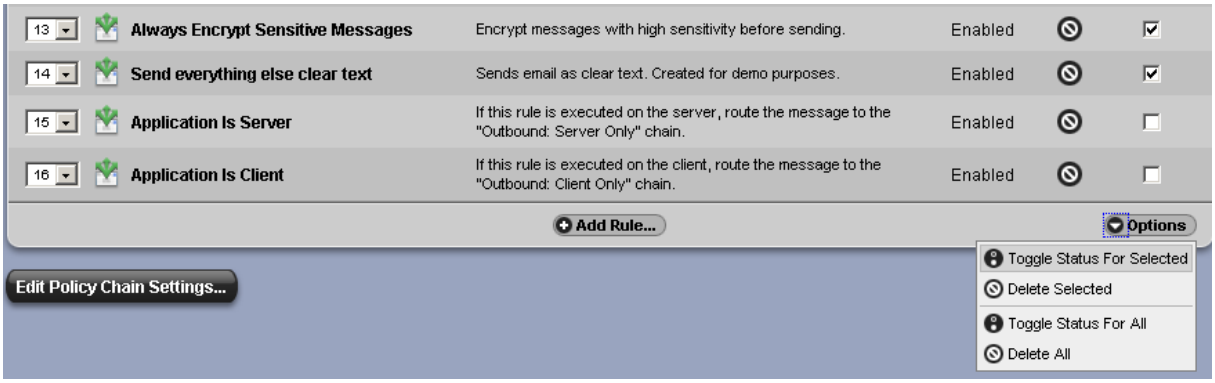
Task 2: Disable the Outbound Policies

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*

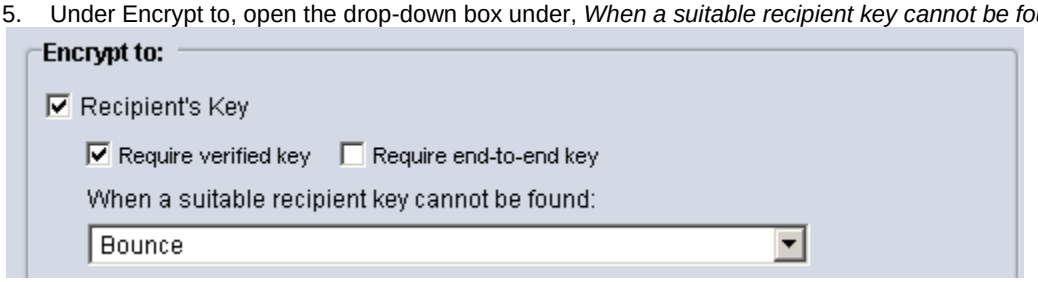


9. Click *Ok* to continue.

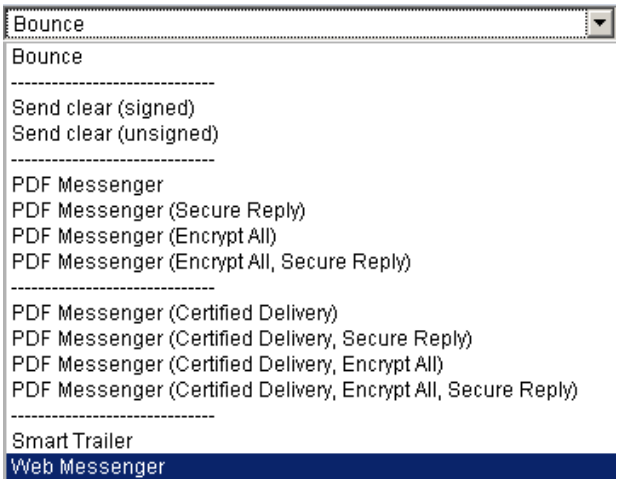
Task 3: Edit the Outbound Server policy

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 Messanger.*



7. Click *Save* to continue.

Congratulations, you have completed Part 2!

Part 3: Symantec Messaging Gateway Configuration

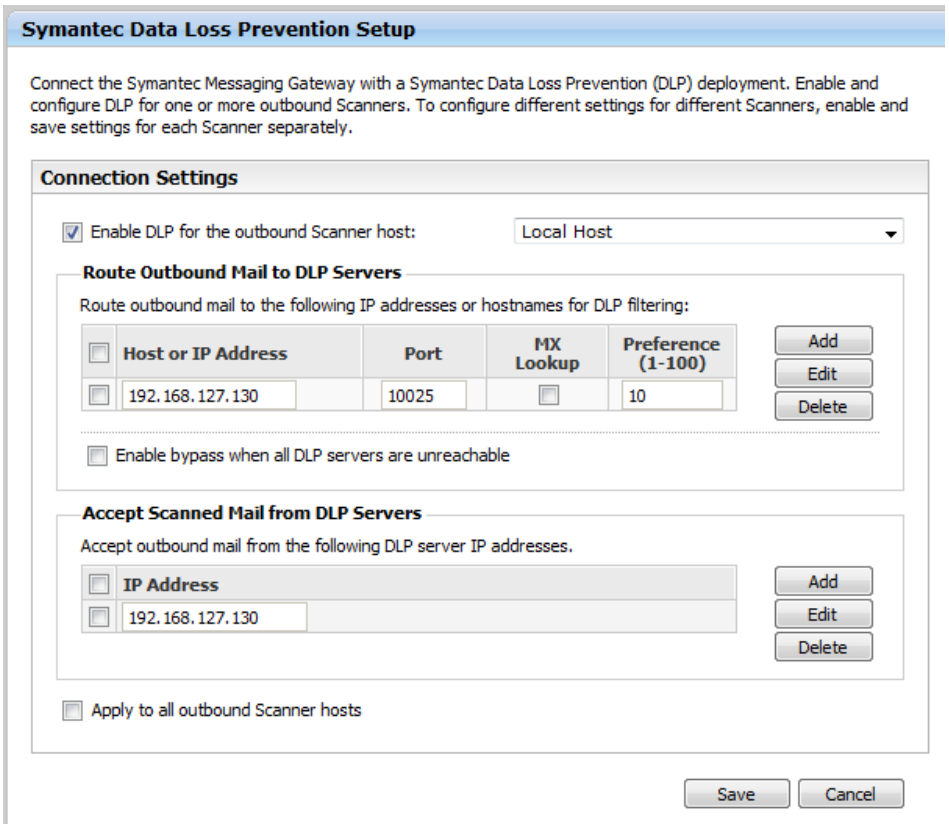
The Messaging Gateway is used to manage routing of all messages destined to either the DLP or PGP servers. In addition as a good best practice it should be the main email gateway that sends messages to the Internet. The Messaging Gateway is designed for direct integration with DLP and users can enable 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:

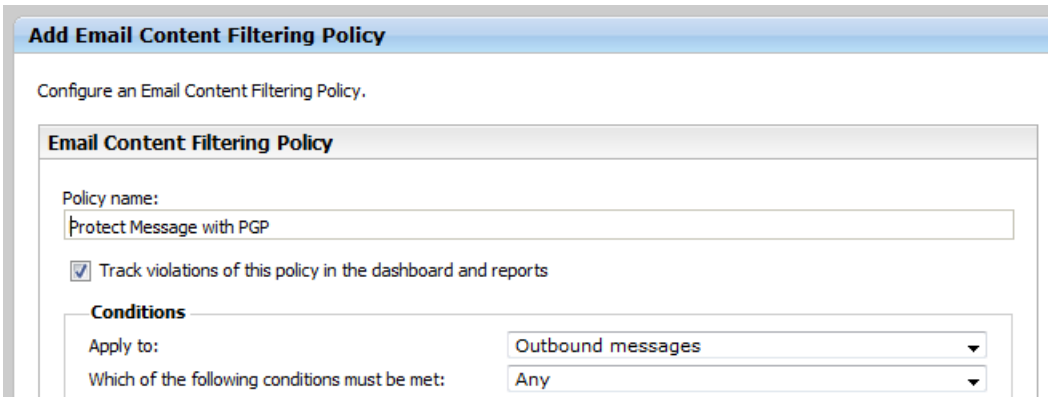


6. Click *Save* continue.

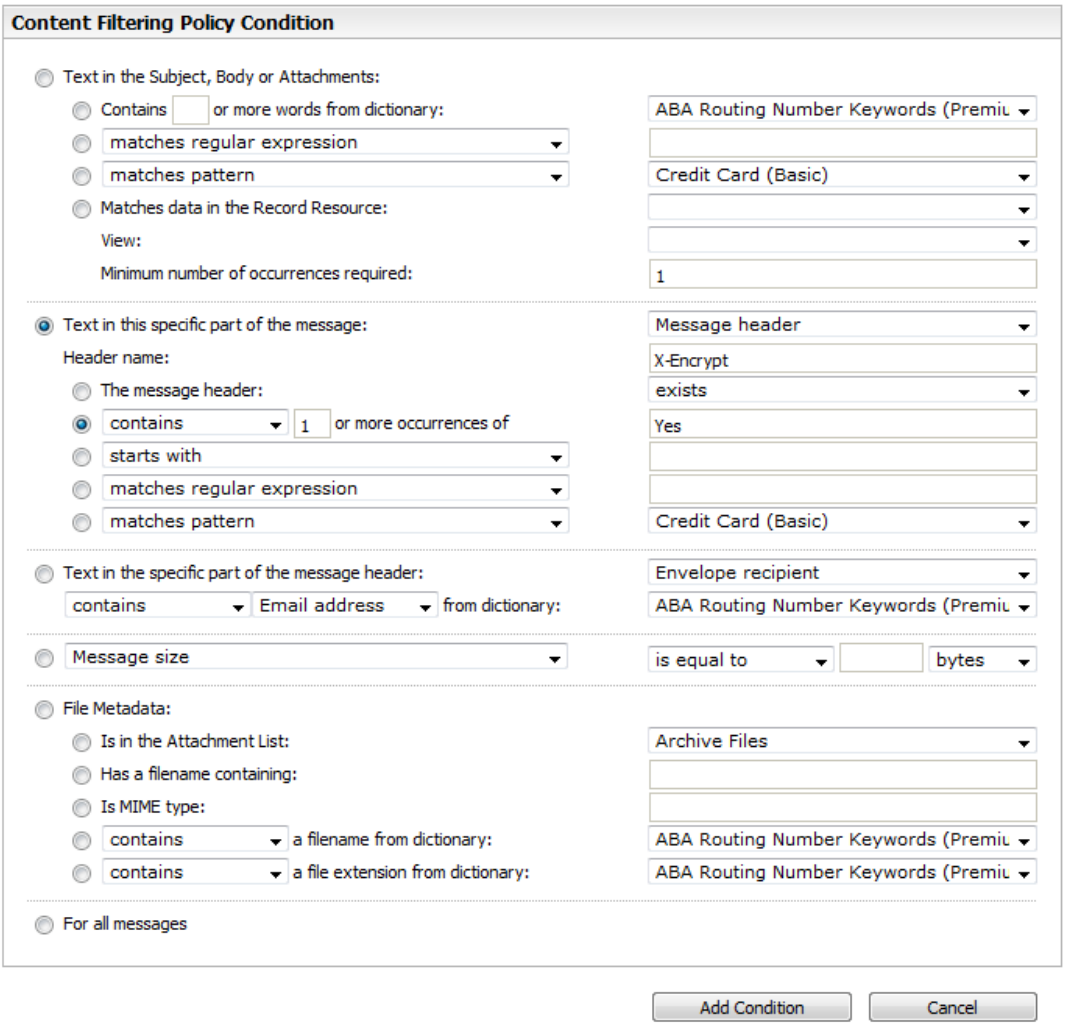
Task2: Create a Policy to Route Messages to PGP

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:

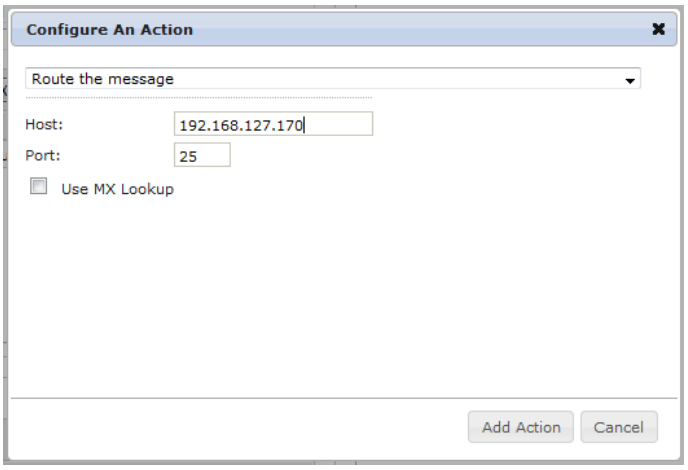
1. Go to the SMG UI, https://192.168.127.40/brightmail
2. Log into the SMG UI with the following:
    - Username: admin
    - Password: symc4now
3. From the Content Tab, under Policies, select *Email.*
4. Under Email Content Filtering Policies, select *Add.*
5. Under Content Filtering Police Templates,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



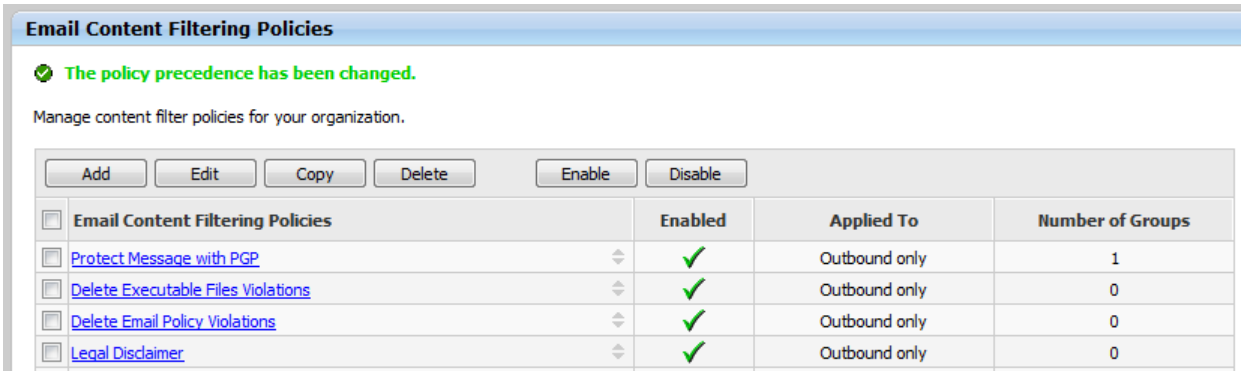
7. Under Conditions, click *Add* to customize the condition builder.
8. Based on Part 1, edit the Content Filtering Policy Condition as follows:



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.

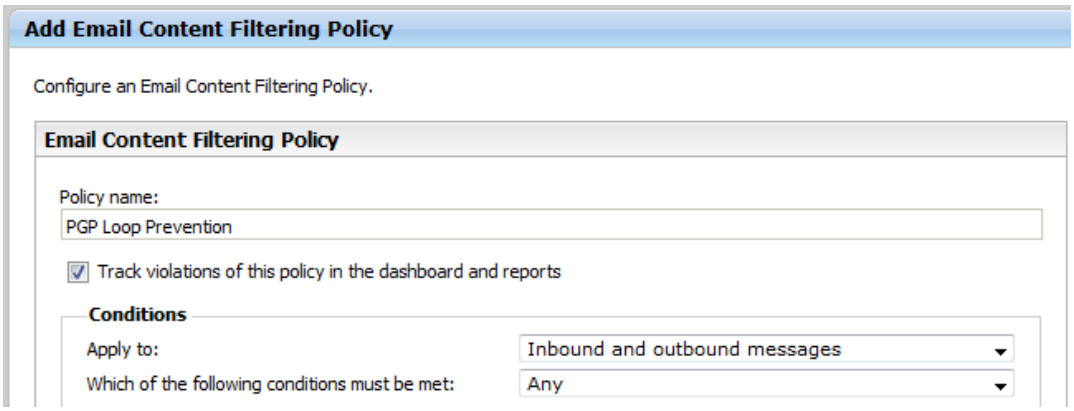


Task3: Create a Policy to Prevent a Mail Loop with PGP

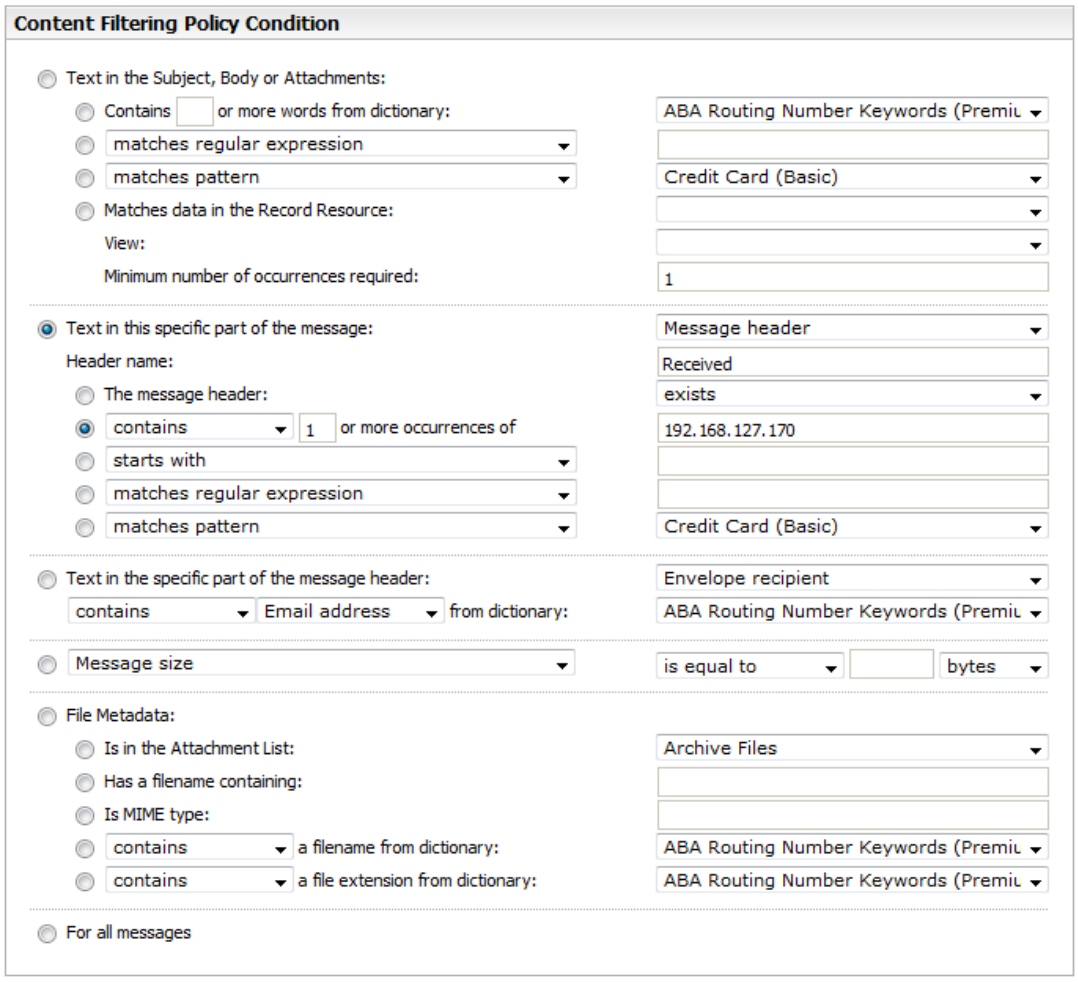
The second policy is required to prevent a mail loop with PGP. In a typical production scenario all messages should be routed to the Messaging Gateway for final delivery to the Internet. When a message is routed from SMG to PGP, PGP will either generate a notification that a message has been encrypted 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

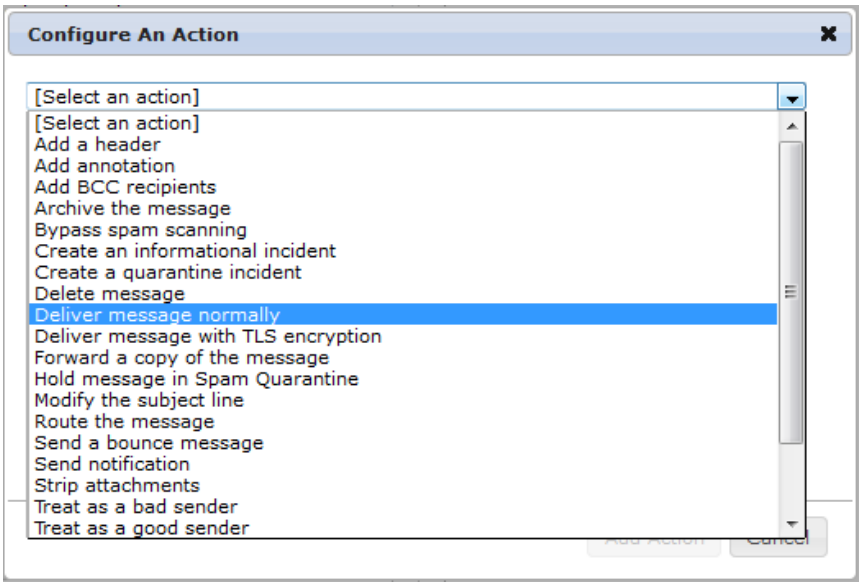
3. From the Content Tab, under Policies, select *Email.*
4. Under Email Content Filtering Policies, select *Add.*
5. Under Content Filtering Police Templates, select *Blank* and click *Select* to continue.
6. Edit the first part of the Email Content Filtering Policy as follows:



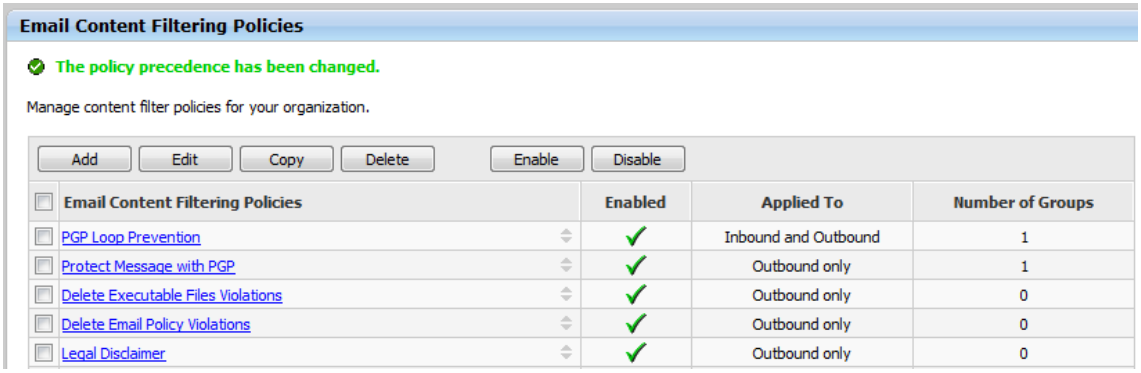
7. Under Conditions, click *Add* to customize the condition builder.
8. Edit the Content Filtering Policy Condition as follows:



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).



Congratulations, you have completed Part 3!

Part 4: Testing the Integration

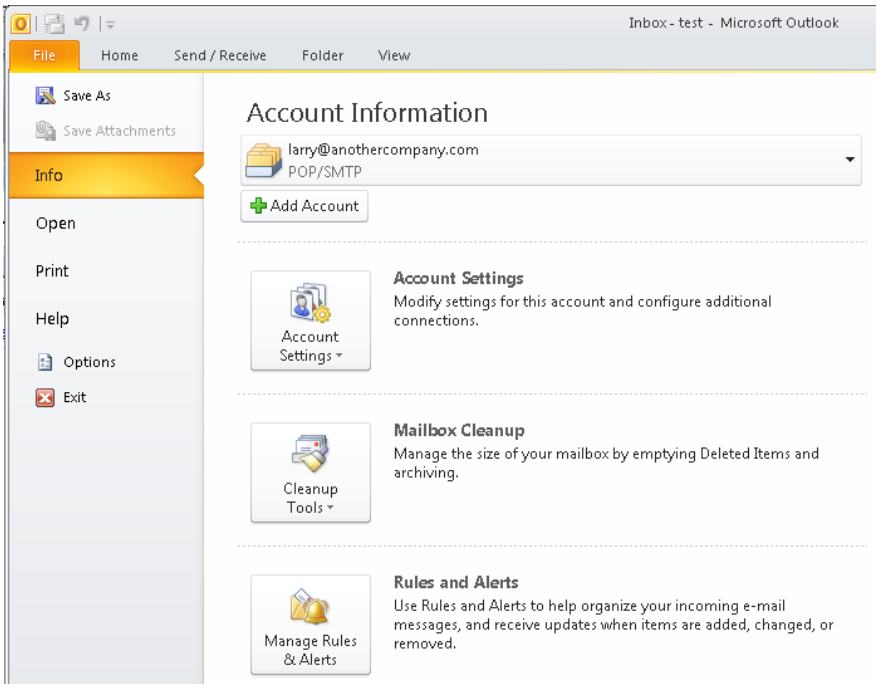
Now that you have configured the integration, test to confirm that each component is operating properly. You will be able to view the details in both the Message Audit Logs of the Messaging Gateway, the Incident reports of the Enforce platform, and the MTA logs of the PGP server. Finally as an end-user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

Task 1: Configure Outlook

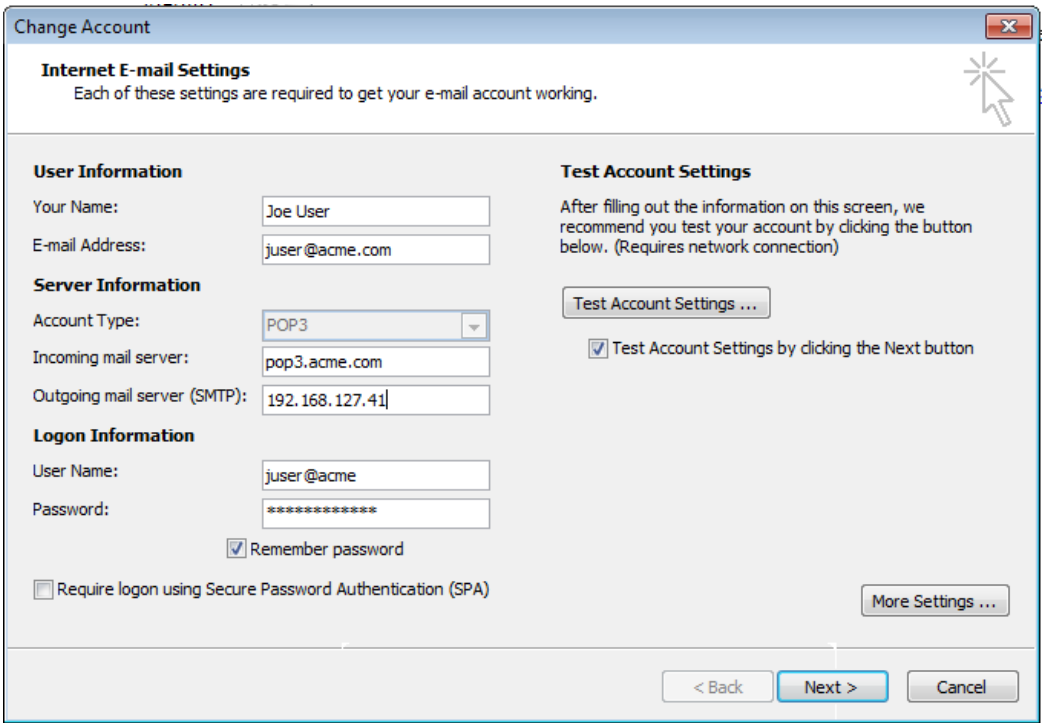
Before testing that the Network Prevent policy works, you will need to configure Outlook to relay outbound messages through the Messaging Gateway. Complete the following steps to re-route messages:

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

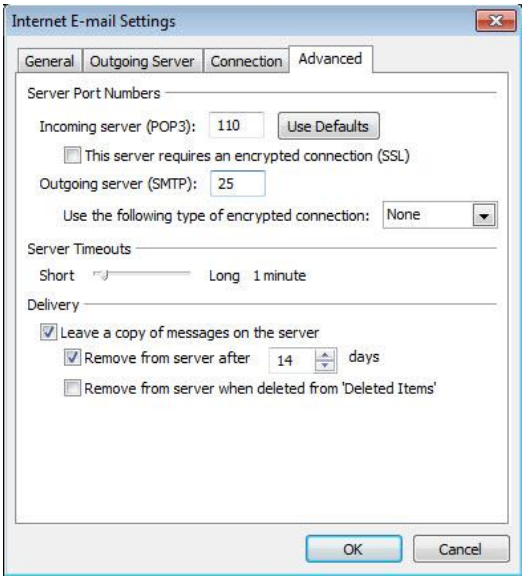
2. Open Microsoft Outlook.
3. Select the *File* tab.
4. Within the Info section, open the drop-down box for Account Settings and select *Account Settings*.



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.*

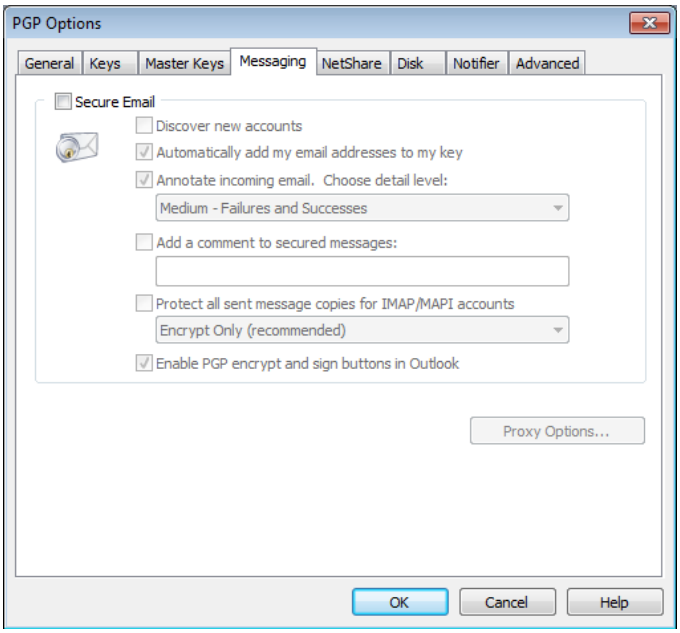


10. Click *Next* to continue.
11. Click *Finish* to continue, and close the Account Settings pop-up.

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. The disable the Secure Email on the desktop complete the following:

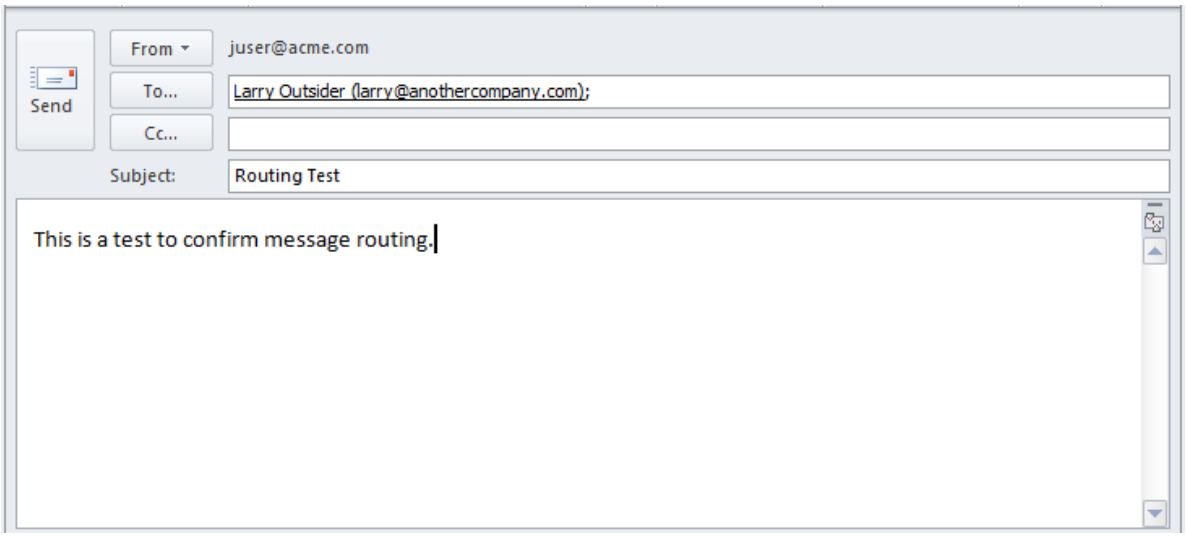
1. From the **Windows 7x86(v11)** Image, open the *Start Menu.*
2. Select *PGP Desktop*.
3. From the Menu Bar, select Tools, and go to *Options.*
4. Select the *Messaging* Tab.
5. Uncheck the box next to *Secure Email.*
6. Click *OK* and close PGP Desktop.



Task 3: Message Route Test

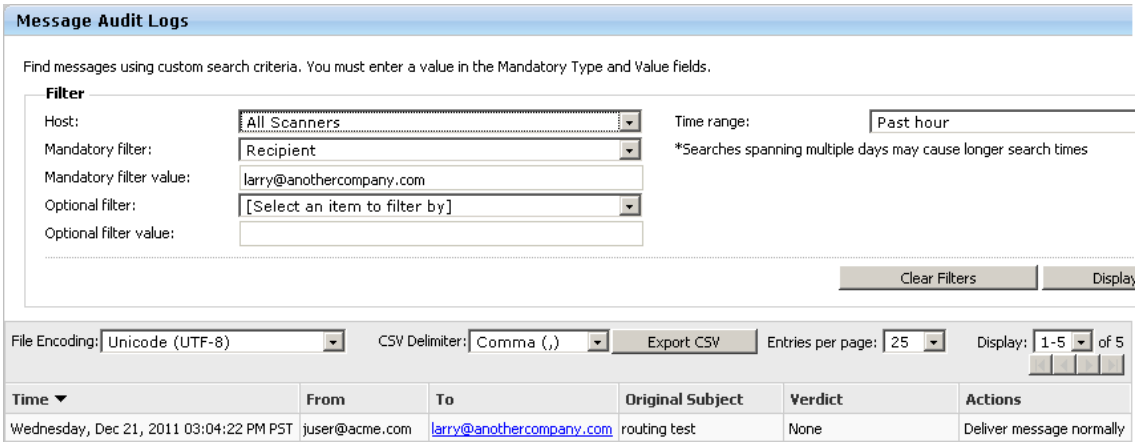
You should be able to send a message to test that mail is relayed through the Messaging Gateway. Using Microsoft Outlook and the user Joe Kerr, send a test message to larry@anothercompany.com. This test is intended to simulate outbound mail going where **jkerr@acme.com** is the internal user and **larry@anothercompany.com**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

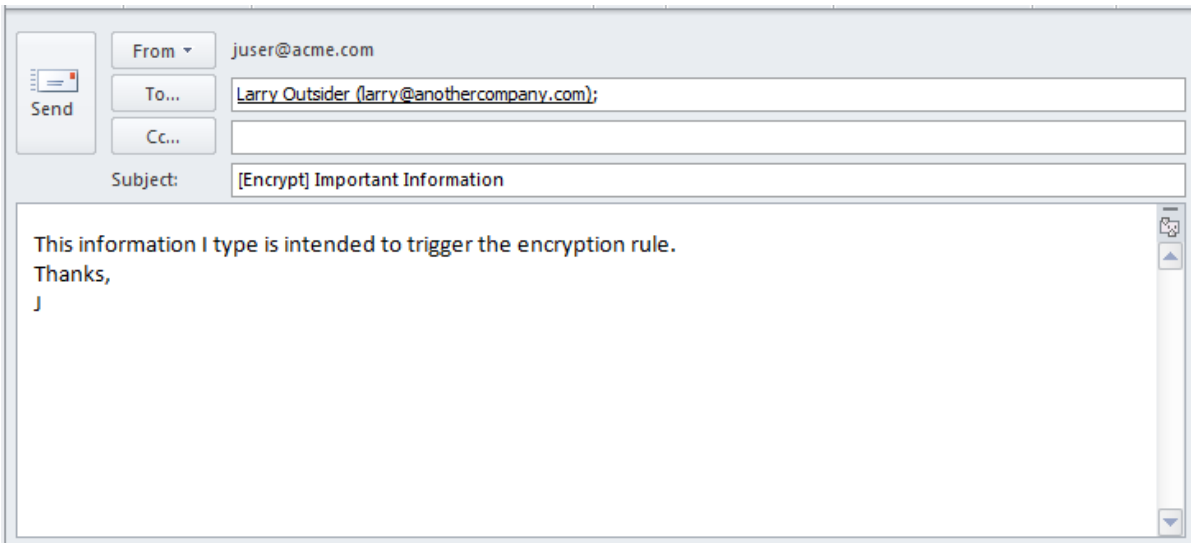
    b) From the Messaging Gateway Console
        i. From the Status tab, under SMTP, select *Message Audit Logs*
        ii. Under Search Criteria, Select Recipient and search for **larry@anothercompany.com**.
        iii. You should see a list of entries. Select the most recent entry and review the Delivery and Verdict details.
            Leveraging the Message Audit Logs is a good way to help troubleshoot issues related to message delivery.



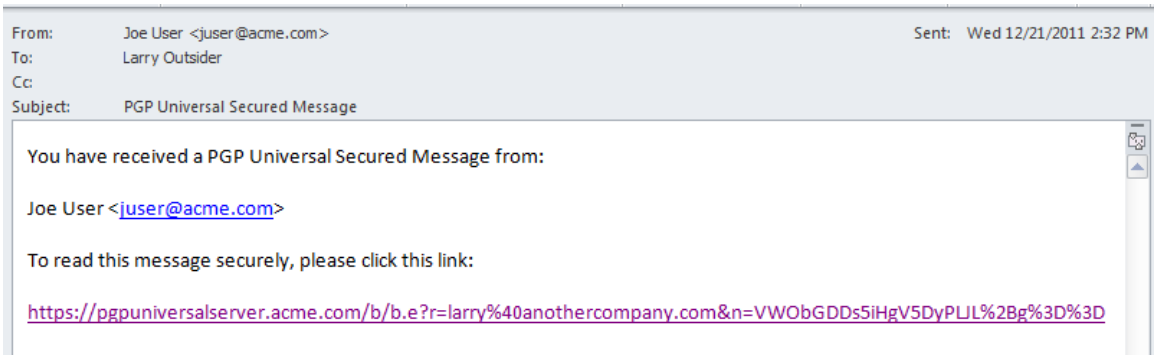
Task 4: Policy Violation Test

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:

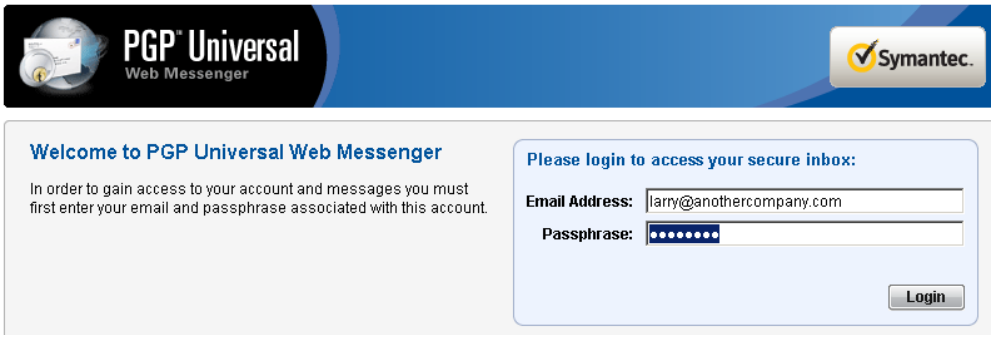
1. From the Microsoft Outlook, click *New E-mail*.
2. Edit the email as follows, remember the subject must contain the term “[Encrypt]:



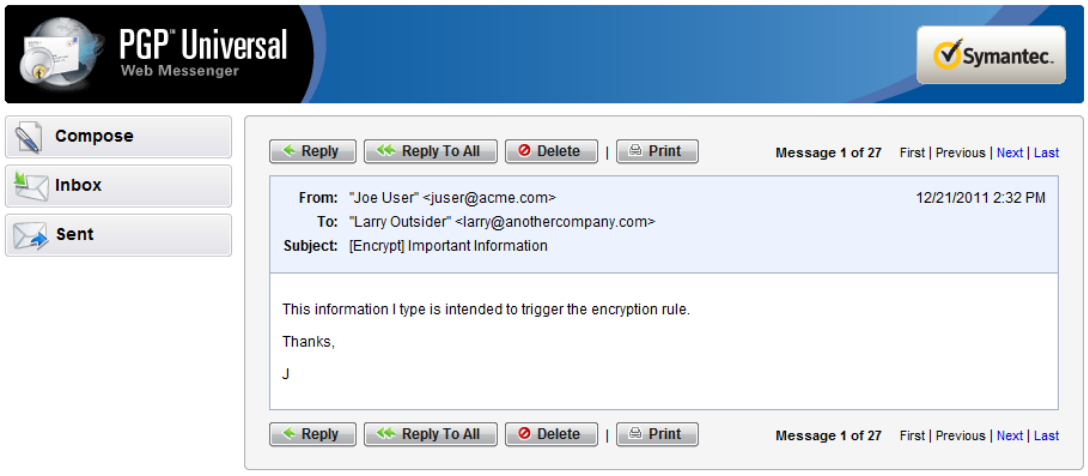
3. Click *Send* to send the message.
4. Go to **larry@anothercompany.com**’s inbox.
5. From the ribbon click on *Send/Receive All Folders*.
   The notification should have been delivered, indicating that a secured message is available for review.
6. Click on the URL within the message.



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.



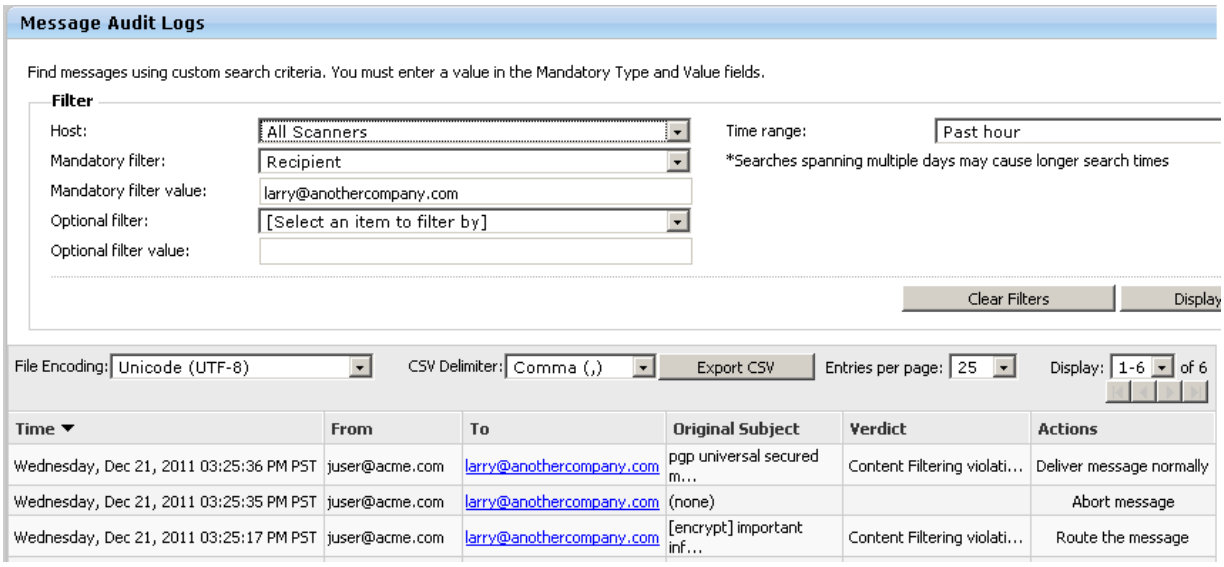
Task 5: Reviewing Logs

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:

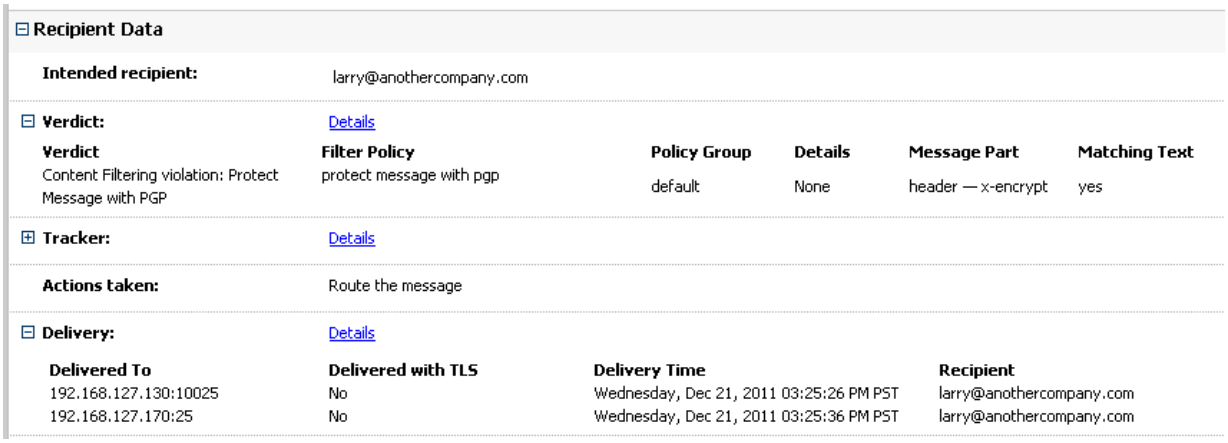
Reviewing SMG Entries

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

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



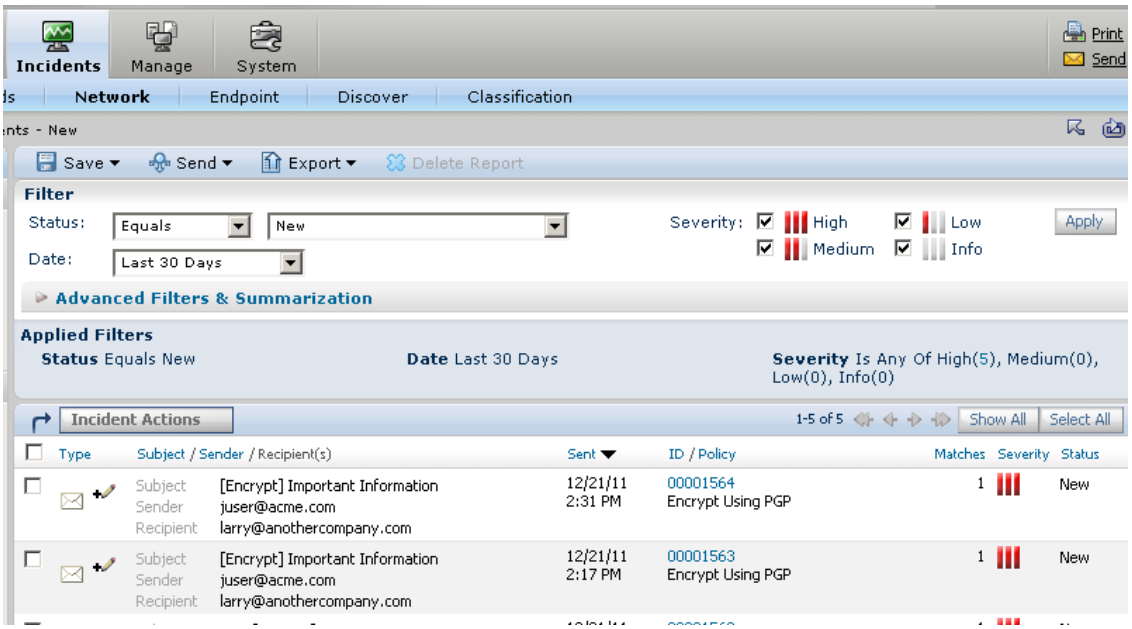
6. The entries should be read from bottom to top.
7. The first entry denotes that the message was first routed to DLP, the header was inserted by Network Prevent and the message was routed to PGP.



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

Reviewing DLP Entries

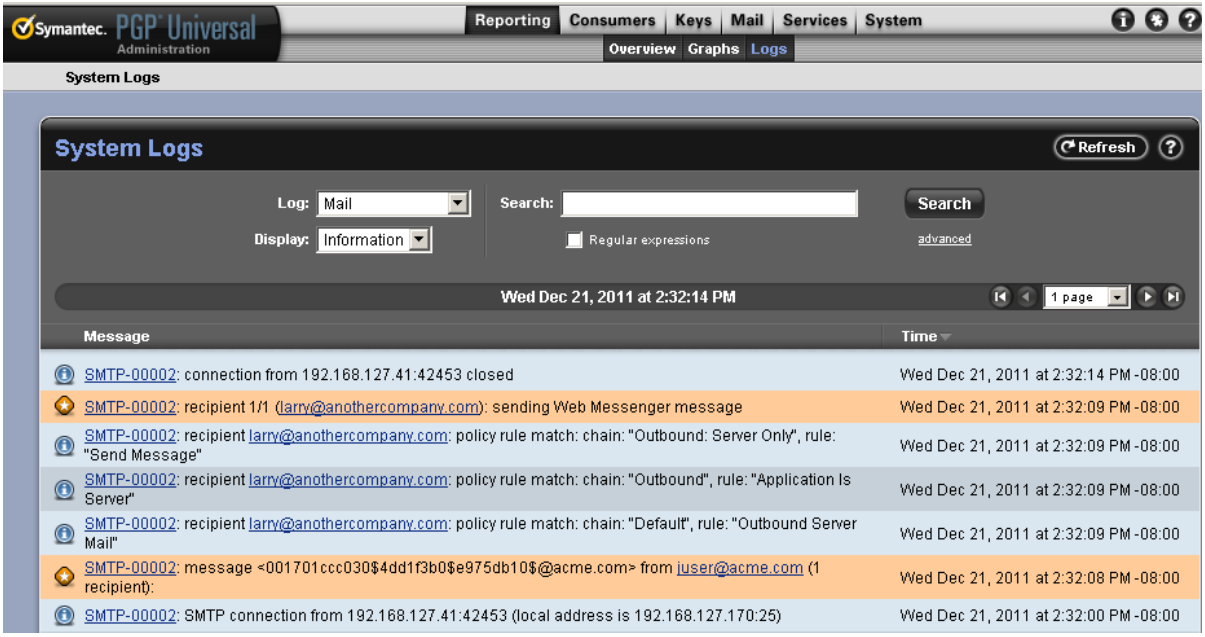
1. Log into the **DLP console**.
2. Select the Incidents Tab, and click on *Network*.
3. Under Network Reports, select *Incidents – New.*
4. The policy violation should be listed.



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.



Congratulations, you have completed Part 4!