mailflow monitor

Service Overview
&
Installation Guide

Contents

1.0 Overview

Mail Flow Monitor works by replicating the path of emails into and out of your organisation. The service is internet based and works in real-time, so you can be alerted of issues affecting your organisations ability to send and receive emails.

There are three ways of setting up the Mail Flow Monitor service, all of which are detailed below, including instructions on how to configure the service.
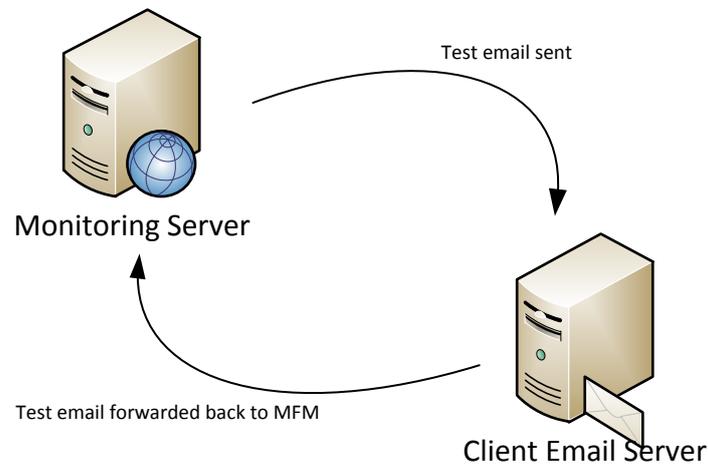
The Simple setup is designed to get you up and running in minutes, with minimal configuration, ideal for basic monitoring and alerting of issues.

The Advanced setup gives greater reporting facilities and also more information to assist in the troubleshooting of email related problems, both inbound and outbound.

The OWA test allows advanced testing of Microsoft Exchange Server 2007 and above in the same manner as the advanced configuration. However the OWA setup only needs to access the Outlook Web Access page over http or https to test both inbound and outbound mail flow.

2.0 Simple Setup

Using a full mail loop test Mail Flow Monitor can be configured quickly and easily to monitor your mail flow.

The monitoring server will send a test email to a mailbox created on your mail server, this mailbox will have a forward configured which will forward the email back to Mail Flow Monitor. After waiting two minutes the monitoring server will then check for the test email, if the email is found the monitoring server will indicate that the test is successful and will start again. If the message is not found the monitoring server will wait two minutes and will check again, the monitoring server will continue trying until the message is found or the failed threshold is reached. If the failed threshold is reached the monitoring server reports the failed Receive service.
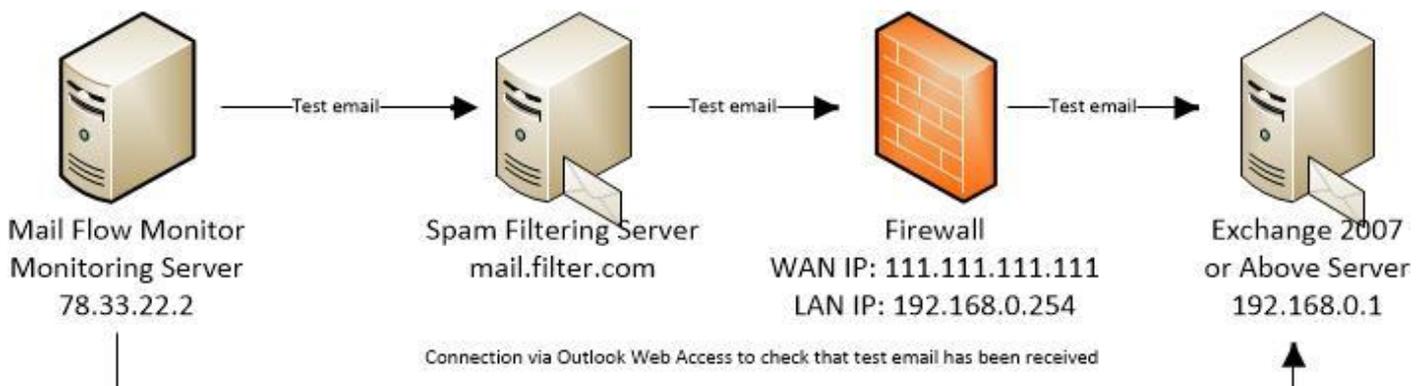
3.0 OWA Setup

Unlike the Simple setup, the OWA setup is split into two individual tests. There is a send test and a receive test. Details of these are below. The setup for the OWA test is minimal both in the portal and on the monitored system. The OWA test is only available to Microsoft Exchange Server systems from 2007 and greater.

3.1 Receive Test

The monitoring server sends a small test email to your mail server using the Receive Email alias e.g. MFMusername@yourdomain.com, the test is sent as a normal email which ensures that the same path as any other email is taken. The MX record is resolved and the message is delivered to the server, if there is a problem connecting and delivering the test email to the MX record server the receive test reports a failure.

After the test email has been delivered to the MX record mail server the monitoring server will wait two minutes, the server will then connect to your mail server using OWA to check that the message has been received. If the message is found the monitoring server will indicate that the test is successful, it will then wait another two minutes and start over. If the message is not found the monitoring server will wait two minutes and then it will check for the message again, if the message is still not found the monitoring server will repeat the check until the message is found or the failed threshold is reached. If the failed threshold is reached the monitoring server reports the failed receive service.
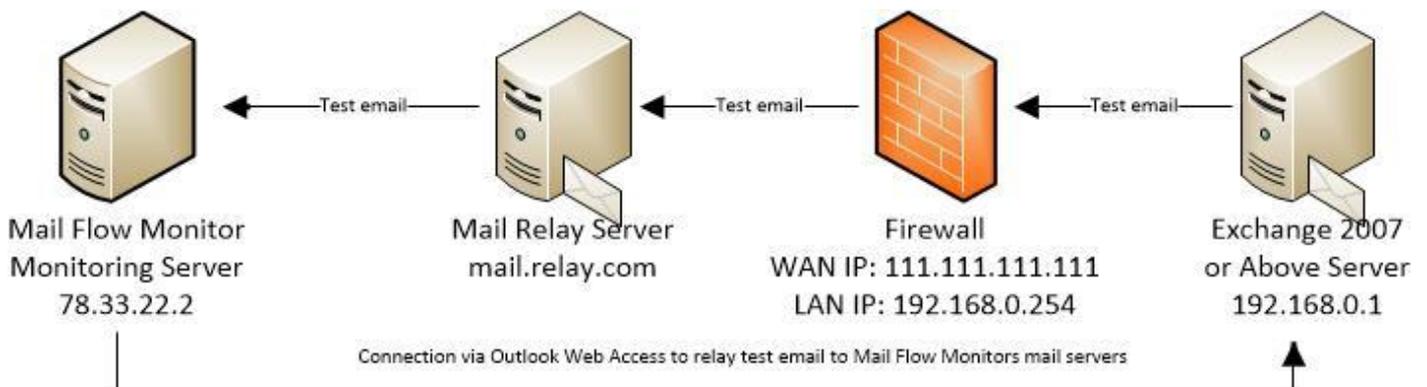
The failed threshold is configured in the portal for the amount of failures required before an alert is sent. This is configured in the sensitivity options for each test.

3.2 Send Test

The monitoring server will connect to your mail server via OWA and relay a small test email to one of Mail Flow Monitors service servers

This email will be delivered by your mail server like any other email sent from your company to Mail Flow Monitor's mail server. After delivering the test email to your mail server the monitoring server will wait two minutes before checking Mail Flow Monitor's mail servers for the test email. If the message is found the monitoring server will indicate that the test is successful, it will then wait another two minutes and start over. If the message is not found the monitoring server will wait two minute and then it will check for the message again, if the message is still not found the monitoring server will repeat the check until the message is found or the failed threshold is reached. If the failed threshold is reached the monitoring server reports the failed send service.

Mail Flow Monitor
Monitoring Server
78.33.22.2

Mail Relay Server
mail.relay.com

Firewall
WAN IP: 111.111.111.111
LAN IP: 192.168.0.254

Exchange 2007
or Above Server
192.168.0.1

Connection via Outlook Web Access to relay test email to Mail Flow Monitors mail servers

4.0 Advanced Setup

The Advanced setup works in a similar way to the OWA setup but the portal gives more flexibility and granularity on the type of configuration.
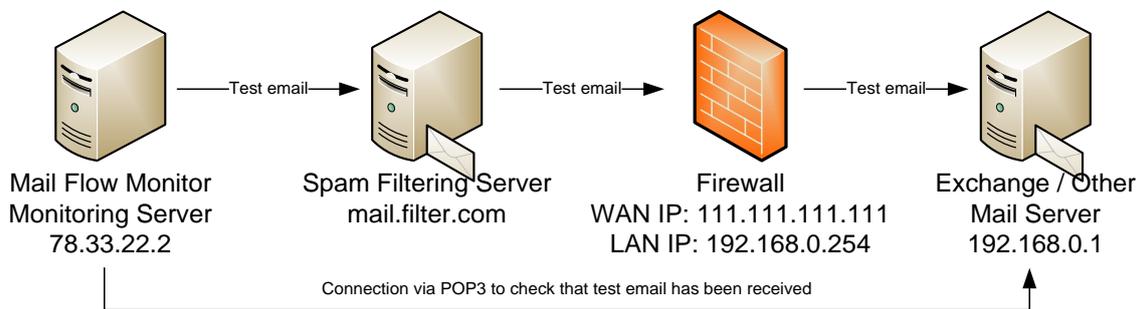
The receive test can be configured to utilise OWA or POP3 as the mechanism for testing.

The send test can be configured to utilise OWA or SMTP as the mechanism for testing.

If set up using OWA the tests work in the same manner as the OWA setup above, alternatively, the POP3 and SMTP configurations are explained below
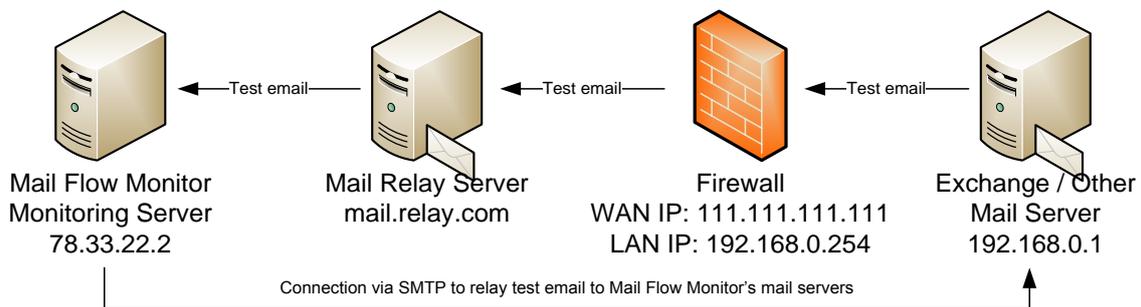
4.1 Receive Test – Using POP3

The receive test works in exactly the same manner as the OWA setup receive test, but when configured for POP3, the monitoring server will access the mail system using the POP3 protocol to check that the test email has been received

4.2 Send Test – Using SMTP

The send test works in exactly the same manner as the OWA setup send test, but when configured for SMTP, the monitoring server will access the mail system using the SMTP protocol to check that the test email has been received

5.0 Simple Setup Configuration

1) Create a mailbox enabled user on your email server and make a note of its email address
2) Log into the Mail Flow Monitor Portal at https://portal.mailflowmonitor.com

3) From "Mail Test Type" select Simple for the "Mail Loop Configuration"

4) Enter your domain name and enter the email address of the mailbox you configured in step 1 into the "Receive Email Alias"
5) Select the "Receive Sensitivity" you desire
6) Make a note of the "Forwarding Email Address" and modify the mailbox created in step 1 to forward its emails to this email address
7) Modify the Alert Settings as required (instructions can be found further down in this document) and enable "Service Running", then save the settings

Note: If you have Microsoft Exchange Server you will need to create a Contact to be able to forward the emails externally

6.0 OWA Setup Configuration

1) Create a mailbox enabled user on your email server and make a note of its email address
2) Log into the Mail Flow Monitor Portal at https://portal.mailflowmonitor.com

3) From "Mail Test Type" select OWA for the "Mail Loop Configuration"

4) Enter your domain name and enter the email address of the mailbox you configured in step 1 into the "Receive Email Alias"
5) Select the "Receive Sensitivity" you desire
6) Select the OWA sensitivity you require
7) Configure the connection type used to access OWA. This will be either http or https
8) Enter the external FQDN for your OWA portal (Note the application path is not required)
9) Enter the Active Directory username and password for the user set up in Step 1
10) If the certificate in use on your server is self-signed, check the box to Ignore Certificate Warning
11) Modify the Alert Settings as required (instructions can be found further down in this document) and enable "Service Running", then save the settings

7.0 Advanced Setup Configuration

1) Create a mailbox enabled user on your email server and make a note of its email address (If required you can create a separate Active Directory user for the send test)
2) Log into the Mail Flow Monitor Portal at https://portal.mailflowmonitor.com

3) From "Mail Test Type" select Advanced for the "Mail Loop Configuration"
   Additional configurable options will now appear. These can be configured as follows:

7.1 Receive Test – Settings

There are 2 ways of configuring the receive test. The configuration denotes which method will be used to check that test emails have been received by your email system. Either OWA or POP3 can be configured.

If configuring via POP3, the mail system will need to be configured to utilise POP3, the mailbox that was created in step 1 will need to be enabled for POP3 collection and also the external firewall will need to be configured to allow POP3 access from Mail Flow Monitors monitoring service to the internal email server. If configuring via OWA, the mail system will need to be Exchange 2007 or greater and OWA will need to be configured for external access on the FQDN specified later in the setup process

 In the portal, you will need to configure the following:

Receive Test Active – Choose whether you want to monitor email flow into your mail system (The default is checked)
Receive Server Type – This will need to be configured as POP3 or OWA
Domain Name – Enter the external email domain name
Receive Email Alias - Enter the email address of the account set up in Step 1
Receive Sensitivity – Select the requried sensitivity for the receive test

Once this is configured you will then need to follow the configuration guide in 7.1.1 if you selected OWA or 7.1.2 if you selected POP3

If you have selected POP3 as the receive server type, you can skip this section. If you have selected OWA, then please configure as below:

OWA Server Sensitivity – Configure the required sensitivity of the OWA server
Connection Type – Configure whether your OWA portal utilises https or http to access from an external location
OWA Server Address - The external FQDN of your OWA portal (note the application path is not required)
OWA User Name/Password – Enter the Active Directory username and password for the user set up in Step 1
Ignore Certificate Warning – If the certificate in use on your OWA portal is self-signed, check the box

7.1.2 Receive Test – POP3 Settings

If you have selected OWA as the receive server type, you can skip this section. If you have selected POP3, then please configure as below:

POP3 Server Sensitivity – Configure the required sensitivity of the POP3 server
POP3 Server – Enter the external FQDN of your POP3 server/Mail server
POP3 Port – Specify the port which your POP3 server listens on externally
POP3 User Name/Password - Enter the username and password for the user set up in Step 1

OWA Settings

OWA Server Sensitivity:	Normal-High
Connection Type:	HTTP
OWA Server Address:	/ews
OWA User Name:	
OWA Password:	
Ignore Certificate Warning:	☐

POP3 Server Settings

POP3 Server Sensitivity:	Normal
POP3 Server:	mail.domain.co.uk
POP3 Port:	110
POP3 User Name:	MFMemailuser
POP3 Password:	pop3Password

7.2 Send Test - Settings

As with the receive test, there are 2 options which can be configured for the send test. The configuration denotes which method will be used to relay test emails through your email system and back to the Mail Flow Monitor servers. Either OWA or SMTP can be configured.

If configuring via SMTP, the mailbox that was created in step 1 will need to be enabled for relay through your send connector/SMTP connector and also the external firewall will need to be configured to allow SMTP access from Mail Flow Monitors monitoring service to the internal email server. The monitoring server address for the account you are setting up is available in the Mail Flow Monitor portal at https://portal.mailflowmonitor.co.uk
If configuring via OWA, the mail system will need to be Exchange 2007 or greater and OWA will need to be configured for external access on the FQDN specified later in the setup process

In the portal, you will need to configure the following:

Send Test Active – Check this box if you want Mail Flow Monitor to monitor the ability to send out emails from your mail system
Send Server Type – This will need to be configured as either SMTP or POP3
Send Sensitivity –Select the required sensitivity for the send test

Send Test Settings	
Send Test Active:	☑
Send Server Type:	OWA ⌄
Send Sensitivity:	10mins ⌄

Once this is configured you will then need to follow the configuration guide in 7.2.1 if you selected OWA or 7.2.2 if you selected SMTP

If you have selected SMTP as the send server type, you can skip this section.
If you have configured OWA for the receive test, then you do not need to do any further configuration of the OWA settings.
Otherwise, please configure OWA settings as below:

If you have selected POP3 as the receive server type, you can skip this section. If you have selected OWA, then please configure as below:

OWA Server Sensitivity – Configure the required sensitivity of the OWA server
Connection Type – Configure whether your OWA portal utilises https or http to access from an external location
OWA Server Address - The external FQDN of your OWA portal (note the application path is not required)
OWA User Name/Password – Enter the Active Directory username and password for the user set up in Step 1
Ignore Certificate Warning – If the certificate in use on your OWA portal is self-signed, check the box

If you have selected OWA as the send server type, you can skip this section. If you have selected SMTP, then please configure as below:

SMTP Server Sensitivity – Configure the required sensitivity of the SMTP server
SMTP Server – Enter the external FQDN of your SMTP server/Mail server
SMTP Port – Specify the port which your SMTP server listens on externally
SMTP Authentication – Depending upon the authentication method you have decided on using, you will need to configure the following:

> **Allow relay via IP**: In this configuration, SMTP Authentication can remain unchecked. You will need to add the IP address of Mail Flow Monitor's monitoring server to the Allow list on your SMTP server. The monitoring server's IP address can be found in the portal under "Account Information"

> **SMTP Authentication**: In this configuration, SMTP Authentication is required to be checked. Confirm that the user created in Step 1 permission to relay through your email systems Send/SMTP connectors. Only plain text authentication is supported.

SMTP User Name/Password - Enter the username and password for the user set up in Step 1

7.3 Finalising the Advanced Server Setup

Once you have configured the Receive and Send tests as required, you can now complete the Alert settings section as specified in Section 8.0 of this guide.
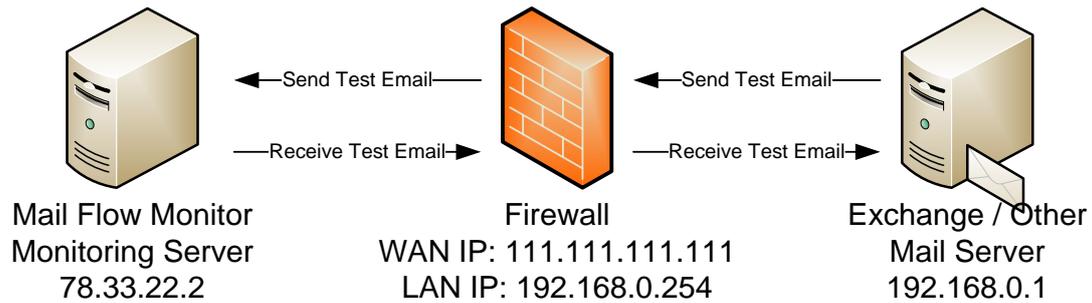
The final step is then to activate the service by ticking the 'Service Running' check box at the top section of the portal page.

7.4 Advanced Setup Examples

7.4.1 Scenario 1

Single mail server behind a firewall, the MX record point directly to the external IP address of the firewall.

MX Record   =   mail.abc.com
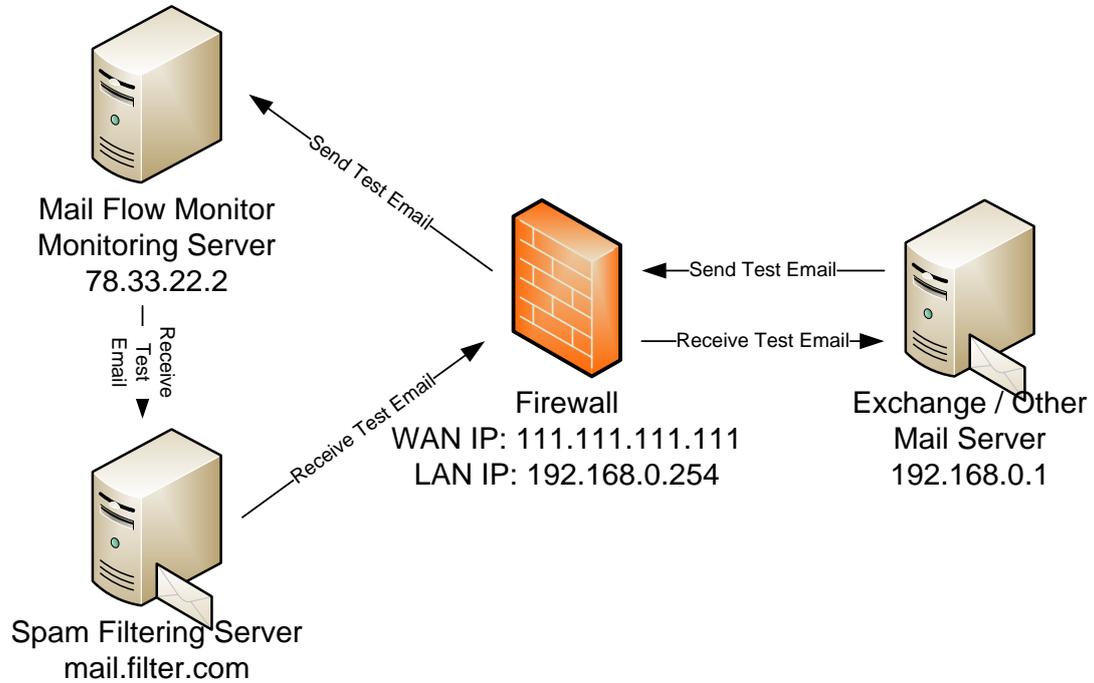mail.abc.com   =   111.111.111.111

Mail Flow Monitor Monitoring Server 78.33.22.2	Firewall WAN IP: 111.111.111.111 LAN IP: 192.168.0.254	Exchange / Other Mail Server 192.168.0.1	

From	Port	To	Destination IP
Any	25	111.111.111.111	192.168.0.1
78.33.22.2	110	111.111.111.111	192.168.0.1

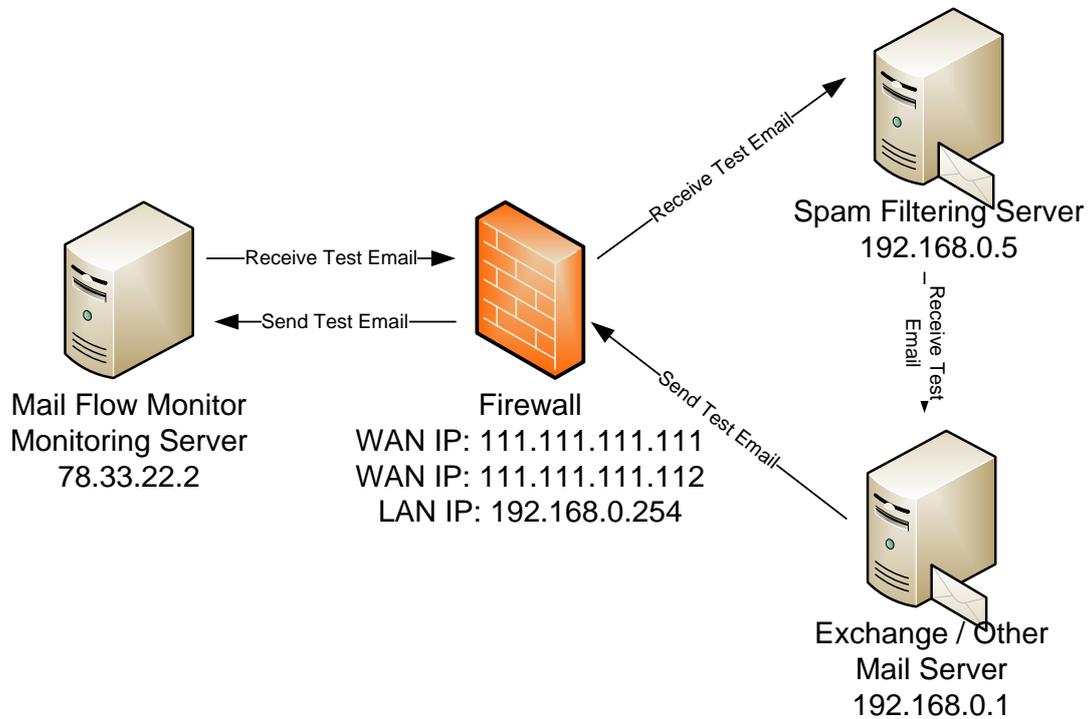Single mail server behind a firewall, the MX record points to a hosted spam filtering server.

MX Record = server.filteringsolution.com

From	Port	To	Destination IP
mail.filter.com	25	111.111.111.111	192.168.0.1
78.33.22.2	25	111.111.111.111	192.168.0.1
78.33.22.2	110	111.111.111.111	192.168.0.1

Single mail server and a spam filtering server behind a firewall, the MX record point directly to the external IP address of the firewall.

From	Port	To	Destination IP
Any	25	111.111.111.111	192.168.0.5
78.33.22.2	25	111.111.111.**112**	192.168.0.1
78.33.22.2	110	111.111.111.111	192.168.0.1

8.0 Portal Alert Settings

The alert settings portion of the Mail Flow Monitor portal allows you to specify who receives notifications of failures and when. The available settings are:

Enable email alerts – When checked, email alerts will be active, corresponding to the remainder of the settings chosen

The next 4 options allow you to specify when you want alerts to be sent in case of a failure

Alert Email Address – The email addresses notifications are to be sent to. For multiple addresses, separate each with a semi-colon (;)

Continuous Alerts – Check this to receive continuous email alerts in the event of a failure. The alert emails provide a link to stop the continuous email alert at any time for that event

Daily Summary Email – Check this to receive an email with the daily status for this account

Summary Email Address – Enter in here the email address for daily summarys to be sent to

9.0 Mail Flow Monitor Desktop Client

There are two versions of the Mail Flow Monitor Desktop Client:
"Mail Flow Monitor Client" and "Mail Flow Monitor Multi-client"

Both can be downloaded from: http://www.mailflowmonitor.co.uk/how_it_works.html

9.1 Mail Flow Monitor Client

This client is used to monitor a single account, once the account settings have been entered the status of that account are displayed.

To modify the account settings click on the grey box at the far right of the client

To access the logs and reports, double click on the date and time

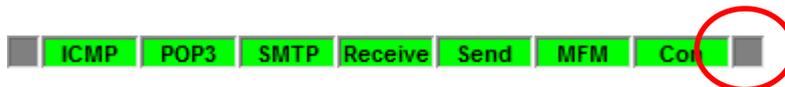## 9.2 Mail Flow Monitor Multi-client

This client is used to monitor multiple accounts, an overview of all accounts is displayed on the toolbar

To modify the accounts that are being monitored, click the grey box at the far left of the client

To view the status of each individual account, click on the grey box at the far right of the client

To access the logs and reports for an account simply click the "Log" hyperlink for the account you require

9.2.1 Single failure

When a failure is detected against a single client, the test that has failed will appear in red.

	ICMP	POP3	SMTP	Receive	Send	MFM	Con	

On expanding the status screen, the failed client will appear at the top of the page and the failed test will appear as FAIL!

Mail Flow Monitor Status - Seconds to connection: 4   Close

1 Failed Service!

Company Name	Last Update	ICMP	POP3	SMTP	Receive	Send	MFM	Logs
Company D	03/08/2011 15:22:54	OK	OK	OK	FAIL!	OK	OK	Log

11 OK Services!

Company Name	Last Update	ICMP	POP3	SMTP	Receive	Send	MFM	Logs
Company A	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company B	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company C	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company E	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company F	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company G	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company H	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company I	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company J	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log

When a failure is detected against multiple clients, each test that has a failure will appear in red.

	ICMP	POP3	SMTP	Receive	Send	MFM	Con	

On expanding the status screen, the clients with failed services will appear at the top, and the individual services for each client will be highlighted as FAIL!

Mail Flow Monitor Status - Seconds to connection: 15   Close

2 Failed Services!

Company Name	Last Update	ICMP	POP3	SMTP	Receive	Send	MFM	Logs
Company D	03/08/2011 15:22:54	OK	OK	OK	FAIL!	OK	OK	Log
Company J	03/08/2011 15:22:38	OK	FAIL!	OK	Unknown!	OK	OK	Log

10 OK Services!

Company Name	Last Update	ICMP	POP3	SMTP	Receive	Send	MFM	Logs
Company A	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company B	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company C	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company E	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company F	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company G	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company H	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log
Company I	03/08/2011 15:22:51	OK	OK	OK	OK	OK	OK	Log