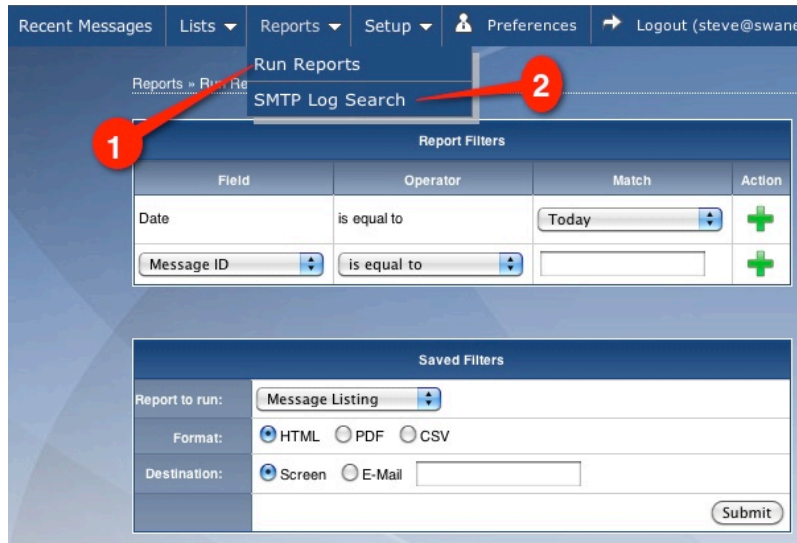**2011**

fort systems ltd

reporting for barricademx plus systems

documentation for system and domain administrators

Reporting for BarricadeMX Plus

Reporting functions are only available to users who are logged in as System Administrators or Domain Administrators. These monitoring functions are can be found by accessing the Top Level **Reports** pull-down menu:

Accessing the Reporting Functions

Selecting **1. Run Reports** will allow you to report on messages that have successfully passed through BarricadeMX filtering

Selecting **2. SMTP Log Search** will allow you to report on all smtpf connections that have been seen by the smtpf process.

Figure 1, Top Menu

Run Reports Data Log Search Data

All connections, messages that are rejected and returned to the sender and messages that are accepted for further filtering are stored in the **bmxlog** table in the Postgres database. Because of the large amount of data in this table, (every MTA connection from all email gateways) data in this table is only stored for three days.

Important: If a message is rejected by the BarricadeMX (the smtpf application) screening process, it will not be displayed in the **Recent Messages** screens and no data for the message will be available to the **Reports** -> **Run Reports** functions.

Run Reports Data

Details for messages that pass BarricadeMX screening are logged to the Postgres Database in the **maillog** table. This is the same data that is seen on the **Recent Messages** screens. Typically, this detailed message data is stored for 30 days.

Important: If a message is rejected by the BarricadeMX (smtpf process) screening process, it will not be displayed in the Recent Messages screens and no data for the message will be available to the **Reports** -> **Run Reports** functions.

Data on messages rejected by BarricadeMX screening will only be available by using the **Reports** -> **SMTPF Log Search** function and this data is only kept for three days.

Using the SMTPF Log Search function

Selecting **SMTP Log Search** from the top-level menu will bring up the Log Search data entry screen.

Reports » SMTP Log Search

This utility allows you to search the raw SMTP logs from the last 3 days.

You may search by any of the following:
IP address
CIDR Mask
Senders e-mail address
Senders e-mail domain
SMTP Session ID

Search: emm.careplusfinancia

1

2

IP address

Figure 2, Top, Recent Messages Screen

As the screen explains, any of the following items may be entered in the In the **Search** text box:

- IP Address
- CIDR Mask
- Senders e-mail address
- Senders e-mail domain
- SMTP Session ID

then select the **2.** Search "Arrow" to display the search results as shown below;

Figure 3, Bottom Recent Messages Screen

If any matching records are found, the:

- Date/Time
- Session ID
- IP address
- DNS PTR record of the sending server
- "HELO" record sent by the sending server
- Transaction Count
- Message Count
- Transaction ID
- Number of recipients
- Sender
- Recipient
- Status
- Last Session Error

Will be displayed for each record found in the Postgres **bmxlog** table. In the event that more data is required, you can use the Session ID or the Transaction ID to manually search the maillog text logs that can be found in /var/log/maillog. Please see How To Use grep Command In Linux / UNIX for instructions on how to search a text file for a specific text string.

Using the SMTPF Log Search function

Selecting **Run Reports** from the top-level menu will bring up the MailWatch Reports data entry screen

Figure 4, Top, Message Detail Screen

To add a filer select the **1**. **Field**, **2**. **Operator** and fill in the **3**. text field with the expression to **Match**, then select the **4**. Add symbol.

The Filter you have added will then show up in the **Active filters** list. In the example above we have added a filter. Filter **6**. In the example above adds a filter that will find any messages where the from domain matches "cnect.online.com"

You should then select the:

- **7**. Report to run **Format**. Message listing is the most commonly used format but many other are available.
- **8**. Report format. **HTML** is the default but **PDF** and **CSV** formats are available.
- **9.** Destination. **Screen** or **E-mail** formats are available. If you **select E-mail**, you must fill in a valid email address in the text box and ONLY CVS or PDF formats are available if **E-mail** is selected.

You may save your search criteria for re-loading later. Simply give the report a name in the text box next to **11**. **Save filter** and then select **12**. Save.
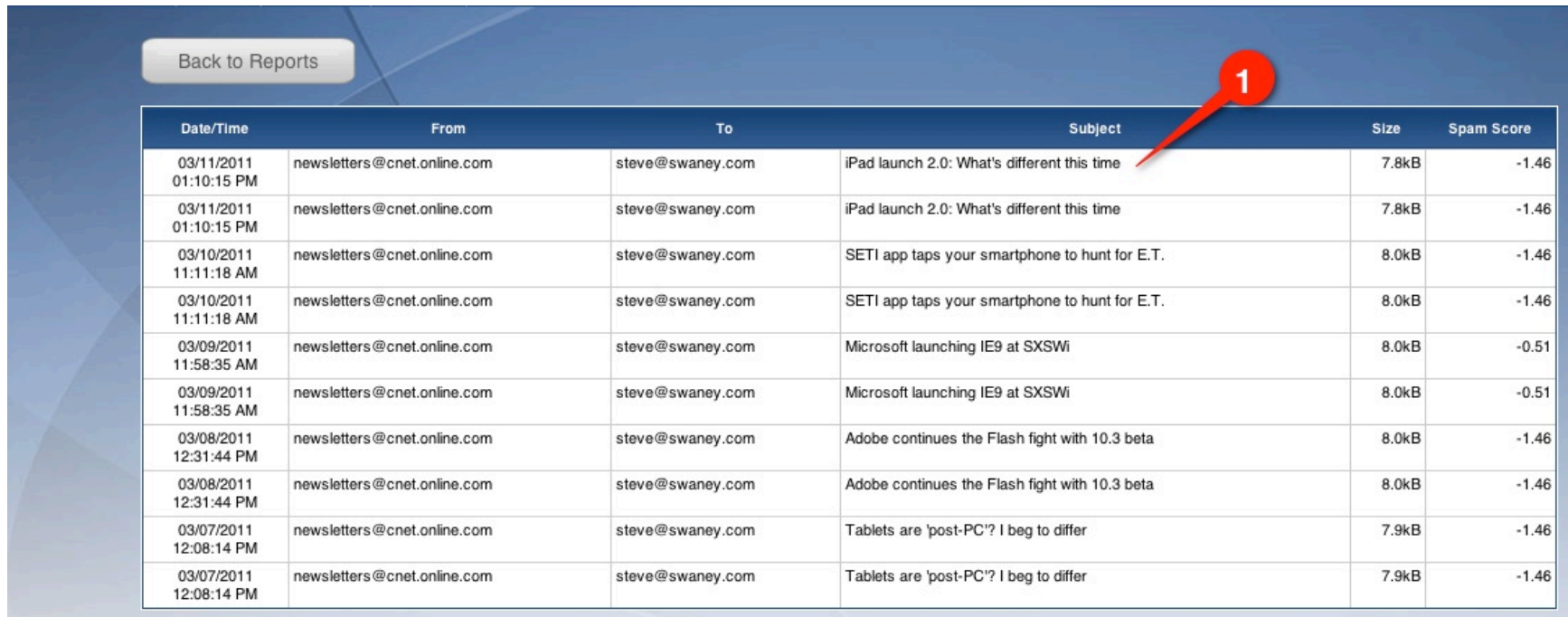
When you have completed filling in the form, select **13**. **Submit** to run and display or send the Report.

Using the Report

If you selected the default setting of:

- **Report to run:** Message Listing
- **Format:** HTML
- **Destination:** Screen

You should see a screen similar to the one below.

Double click on any message line to display the **Message Details** screen. Please see the **monitoring barricademx plus systems** Section of the BarricadeMX documentation for more information on the **Message Details** screen.

Logout

To finish using the Web interface and return to the login screen, simply select the Logout tab at the left of the Top Menu on the screen.

Additional Support

For additional support please contact the support desk at your Company, your Internet Service Provider or Email Services Provider.