



Setup Document Version 2.2+



www.joviantechology.com

Jovian Technology
2570 Matheson Blvd E., unit 114
Mississauga, ON L4W 4Z3
Tel: +1.888.584.2584 Fax: +1. 905.366.0102

Europa Setup Document Version 2.2+
February 2010
Revision 1

Copyright © 2006-2010 Jovian Technology Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the written permission of Jovian Technology Inc.

Disclaimer

Information in this document is subject to change without notice. The material contained here is supplied without representation or warranty of any kind. Jovian Technology Inc. therefore assumes no responsibility and shall have no liability of any kind arising from the supply or use of this document or the material contained herein.

Under no circumstances shall Jovian Technology Inc. be responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

The contents of this document are provided 'as is'. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. Jovian Technology Inc. reserves the right to revise or withdraw this document at any time without prior notice.

Contents

- 1 General Background
- 1.1 Introduction
 - 1.2 Simple Email Flow
 - 1.3 More complex cases
- 2 SPAM
 - 2.1 What is a SPAM
 - 2.2 Spammers
 - 2.2.1 How do spammers get my email address?
 - 2.2.2 What spamming techniques are being used?
 - 2.2.3 Beyond the spamming methods
- 3 Setup Europa Prerequisite
 - 3.1 Basic Requirement
 - 3.2 Using Dynamic IP address
 - 3.3 SMTP inbound service
 - 3.4 SMTP outbound services
 - 3.5 PTR record
- 4 Europa System Installation
 - 4.1 Network parameters
 - 4.2 Setup Europa
 - 4.3 Europa as different email solution
 - 4.3.1 Europa as a spam filter
 - 4.3.2 Europa as an email server and spam filter
 - 4.3.3 Europa as a hot standby redundant email server solution
 - 4.3.4 Europa as a Second Level Spam Filter
 - 4.4 Additional Network Configuration
 - 4.4.1 External access parameters
 - 4.4.2 Optional DNS configuration
- 5 Administrate User IDs
 - 5.1 Different User ID Types
 - 5.1.1 What happens if a virtual domain is now defined in the email server?
 - 5.2 More than one domain and more than one email server
 - 5.3 LDAP and Active Directory integration
- 6 Operation Parameters
 - 6.1 Why should I care about the operation parameters?
 - 6.2 System operation parameters
 - 6.3 Domain operation parameters
 - 6.4 User operation parameters
- 7 Features
 - 7.1 Email Path inside Europa
 - 7.1.1 Local email server or external email server
 - 7.1.2 Quarantine Manager
 - 7.1.3 Discovery Manager
 - 7.1.4 Backup and Restore
 - 7.1.5 Europa Junk Folder
 - 7.2 Multiple Level Black/White list

- 7.2.1 BWL scanning path in the multilevel BWL
 - 7.2.2 Automatically promote the BWL items
 - 7.2.3 Primary and secondary group
- 7.3 Other features
 - 7.3.1 Outbound auto white list
 - 7.3.2 White on grey
 - 7.3.3 Email summary: Daily and Hourly
 - 7.3.4 MPOP clients
- 8 Notes and References

General Background

Introduction

Europa is an *all-in-one complete email appliance* for your organization. This document explains how to properly setup and use the **Europa** appliance.

This document is written for **Europa 100** administrative user (login id: **admin**). It assumes that you have some basic *TCP/IP* ^[1] knowledge; however, you may need a quick refresh course on Internet *Email* ^[2] Communication.

During the **Europa** appliance installation, you will encounter a set of technical terminologies. To illustrate the relationships of these technical terms, this document first introduces a **Simple Email Flow** diagram; followed by the explanations of the technical terms and their usage. Some basic *Spamming*^[3] techniques are then introduced in the **Spam** section, so that you will have a general idea of how to tune the system operation parameters.

Europa can be configured as one, or a combination, of the following email appliance solutions: an *Anti-Virus*^[4] / Anti-Spam email filter, a hot standby redundancy email server and an email server. The different configurations are explained in next section **Europa System Installation**.

The **Administrate User IDs** section explains different **Europa** user ID types, and shows you how to create user IDs in Europa. In most cases, **Europa 100** is configured for only one *domain*^[5]; however, all **Europa** models are capable of supporting multiple domains.

Europa has a rich set of configurable features. In the **Operation Parameters** and **Features** sections, the major features and its parameters are explained for you to configure them properly.

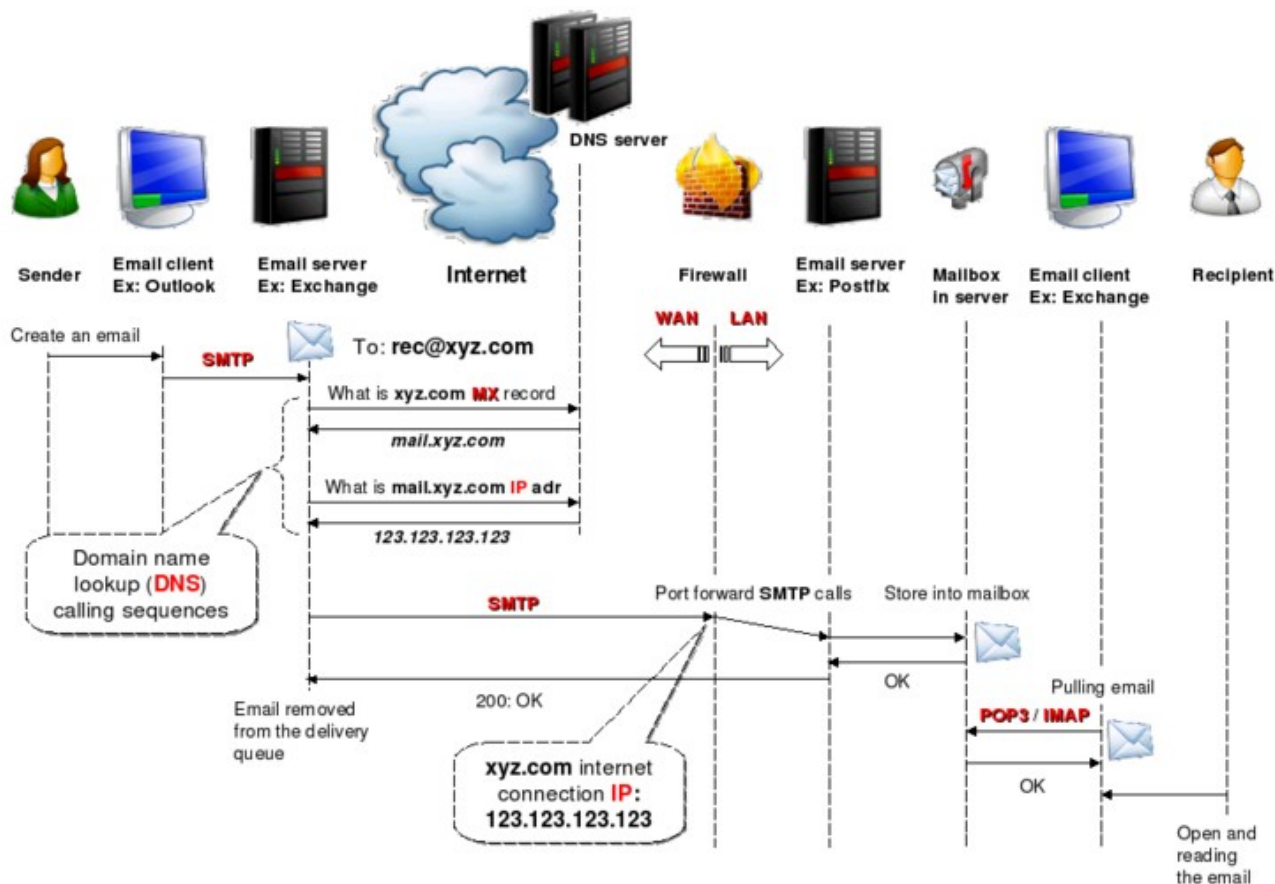
For your reference, when a term first appears in this document, a *Wikipedia*^[6] *URL*^[7] is added. All terminologies and technologies are introduced from simple to complex case. When you are confused with some terminologies, you are encouraged to reference back to the earlier cases. Feel free to skip any section if you are already familiar with the topic of the section. This setup document cannot explain all **Europa** functions, features, and parameters, you should refer to the **Europa Reference Manual** for more details.

Note: If **Europa** is not configured as an *active online SMTP machine* (spam filter/email server) and **only MPOP** service is needed, you will find this document provide too much information on the Internet domain email service setup. If this is the case, you should

1. Refer to the **Quick Setup Guide** for Europa network configuration.
2. Logon to Europa, add a domain and add the required user IDs.
3. Enable the MPOP service for the domain and the user(s).
4. Refer to the **User Guide ver 2.2** for setting up the user's MPOP client.

Simple Email Flow

The following is a very simple email flow diagram which illustrates how an email is transferred from the sender to the recipient.



1. The sender uses his/her email client program (for example: Outlook) to create an email to **rec@xyz.com**
2. The email client program uses *SMTP*^[8] protocol to transfer the email to an email server machine.
 - ◆ The email server can either reside in the *LAN*^[9] or the external service provider.
 - ◆ Some email servers may require this SMTP to be authenticated over *SSL*^[10] secure connection.
 - ◆ Most email servers require login such as Account name and Password.
3. The email server tries to deliver the email to the recipient's email server.
 - ◆ Delivery process is not instant, it depends on the email server loading.
 - ◆ Therefore, email communication is **never** designed as real time communication process.
 - ◆ The email server calls its *DNS*^[11] server for requesting the *MX*^[12] (*Mail Exchanger*) record of domain **xyz.com**.
 - ◇ DNS server replies back with a domain name **mail.xyz.com**.
 - ◆ The email server then calls the DNS server again for requesting the *IP*^[13] address of **mail.xyz.com**.
 - ◇ DNS server replies back with **123.123.123.123**.
4. The email server connects to IP: **123.123.123.123** and port **25** (SMTP port) with SMTP protocol.
5. In general, most sites are protected by the *firewalls*^[14].
 - ◆ In the firewall terminology, internet is *WAN*^[15] (wide area network) which connects to the world; and the internal network is LAN which connects to all local machines.
 - ◆ The firewall is placed between LAN and WAN to protect you from the *hackers*^[16] breaking into and gaining access to your local machines.
6. However, the firewall itself cannot accept email delivery. In general, a *SMTP port forward*^[17] configuration is created to forward all the incoming SMTP TCP/IP packets to the local email server

- which can accept email delivery.
7. According to the SMTP protocol, the sender email server provides the recipient email server with information on **MAIL FROM & RCPT TO** attributes, and the content of the email.
 - ◆ In most cases, if **RCPT TO** has an invalid email ID, the SMTP connection will be terminated.
 8. The content of the email is transferred:
 - ◆ The recipient email server stores the email in the user's *mailbox*^[18].
 - ◆ The recipient email server responds **OK**.
 - ◆ The email is removed from the sender email server delivery queue if and only if the **OK** response is received.
 9. If the **OK** response is not received, this email transfer transaction is incomplete.
 - ◆ The sender email server will re-try the above steps in the next delivery cycle.
 - ◆ The time of the next delivery cycle depends on the email server configuration and its loading.
 10. Now, the email is sitting in the user's mailbox (in the recipient email server).
 11. The recipient's email client program pulls the new email from mailbox periodically.
 - ◆ The periodical pulling timer is based on the recipient's email client program setup.
 12. In general, most email servers support two email pulling protocols: 'POP3'^[19] and 'IMAP'^[20]
 - ◆ In most cases, these email pulling services require the user's Account name and Password.
 - ◆ In some cases, these email pulling services require the SSL connection: POP3s and IMAPs.
 13. Once the email is transferred to the recipient computer, the email is displayed by the email client program.

This concludes a simple case of an email flow from sender machine to the recipient machine. With today's hardware performance and network bandwidth, the delivery delay time is shortened; however, be aware that email communication is never designed as a real time communication protocol.

More complex cases

- The following describes the possible reasons of why **the sender email server cannot connect to the recipient email server**:
 - ◆ The recipient internet connection, firewall or email server is down.
 - ◆ The recipient email server is busy.

SMTP delivery process is designed to be transaction-based. The sender email server will re-try in the next delivery cycle. After the maximum number of failed re-tries is reached, the sender email server responds back to the sender with **Non Delivery Message** email.

Again, the re-try timer and number of re-tries depend on the sender email server, not the recipient email server.

- **Why second MX record is needed?**

For some companies, one MX record (one IP) cannot handle all the incoming and outgoing email volume. They will add a next MX record (another IP address) to share the email traffic. Some companies even have more than two MX records. The second MX record can off-load the first MX record email traffic.

- **Which MX record is called first?**

Each MX record has a *preference* number. Most email servers start calling the MX record from lower to higher preference in ascending order. However, some email servers try to avoid the traffic jam, they are programmed to call from the highest to lowest preference MX record in descending order.

From the email communication's perspective, all the MX record preferences are equal. Since all MX records point to a working email server for the same domain, the MX record selection process totally depends on the sender email server and how the receiver sets its own MX record preference.

SPAM

What is a SPAM

In general, email spam can be categorized into:

- **Spamvertised email** - an email that advertises products or services.
 - ◆ The exact same copy of spam is massively distributed.
 - ◆ This kind of spam contains valid callback URLs to the advertised web sites.
- **Blank email** - an email that lacks advertisement, and often lacks the entire message body and subject line.
 - ◆ This kind of email fits the definition of spam because of its nature as bulk and unsolicited email.
 - ◆ This kind of spam is usually sent in a directory harvest attack (a form of dictionary attack) for gathering valid addresses from an email service provider. Since the goal in such an attack is to use the bounces to separate invalid addresses from the valid ones, the spammer may dispense with most elements of the header and the entire message body, and still accomplish his or her goals.
- **Phishing email** - an email that uses a phony sender address to gain the trust and direct users to enter personal information at a fake website.
 - ◆ The fake website's look and feel are almost identical to the legitimate one.
 - ◆ The spammer uses *HTML* ^[21] technique to hide the real web address.
 - ◇ For example, the URL *http://www.cibc_bank.com* can be displayed as *http://www.cibc.com*. When the user clicks the URL, the phony CIBC page is displayed.
- **Virus email** - an email that contains malicious code program.
 - ◆ The virus is delivered as an email attachment and *MIME*^[22] technique is used to change the extension of the attachment and to hide the executable program.
 - ◇ For example, when the user clicks the GIF/JPEG attachment, it may trigger the attached executable program.
 - ◆ Triggering the attached executable program can:
 - ◇ destroy the user's computer.
 - ◇ act as *spyware*^[23] to access the user's personal information.
 - ◇ spread virus by email and infect other machines.
 - ◇ turn the user's machine into a *zombie*^[24] machine to attack other machines.

Most of the viruses are downloaded through the **browser HTTP download session**. Virus email is less common, but email anti-virus function cannot be ignored.

Spammers

Spammers help their clients to massively spread spam in as many dimensions as possible. Statistics show that email spam can improve the phony product's selling record; therefore, there are still spammers in the market.

How do spammers get my email address?

They can get your email address by:

- Scanning user forums, discussion groups, facebook, blog, etc.
- Buying the email address listings from some marketing company.
- Getting your business card from different trade shows.
- Using malicious code or spyware to collect email addresses from the infected machines.
- Using *Directory Harvest Attack (DHA)*^[25] to find valid / existent e-mail addresses.
- Exchanging email address listings among spammers.

What spamming techniques are being used?

Spammers continually change their spamming techniques by:

- Studying different spam filter problems.
 - ◆ Constantly changing the spam formats accordingly to adapt the current spam detection weaknesses. (These formats include, but not limited to, simple plain text, image and *PDF* ^[26].)
 - ◆ Using different word patterns to avoid being detected.
 - ◆ Mixing random forum text with the HTML displayable spam text.
 - ◆ Using HTML to organize the word in vertical format.
 - ◆ and many, many more...
- Learning the world and social events.
 - ◆ For example: Sending earthquake contribution spam.
- Studying different *Internet service provider (ISP)*s^[27] implementations and policies
 - ◆ For example: Rogers blocks all the outbound SMTP traffic. China's ISPs allow their subscribers to send out email, etc.

Beyond the spamming methods

spammers can even go beyond the spamming techniques

- To execute DDoS ransom by launching SMTP distributed denial-of-service (DDoS^[28]) attack / (Zombie Attack) method on an email server and demanding ransom money to stop the attacks.
 1. Organizing a set of zombie machines to continuously send massive spam into one email server.
 2. Using some zombie machines to make SMTP idle connections to consume all the email server TCP/IP SMTP resources.
- To hijack DNS server (this is an extreme case) and redirect all/some incoming emails to the spammer's email server.

Setup Europa Prerequisite

Basic Requirement

1. **Internet connection.** This is a **must** have.
 - ◆ Bell, Rogers, and TekSavvy are the common Internet Service Providers (ISPs) in Canada.

2. TCP/IP IP address

- ◆ **Static** - Most ISPs provide a static IP for Business line subscriber for free or at a fee.
- ◆ **Dynamic** - For the rest of the subscribers, their WAN IP addresses are assigned by the ISPs *DHCP*^[29] server. These assigned IP addresses are changed from time to time.

3. Domain name and MX record

- ◆ An email address is comprised of a user name and a domain name.
- ◆ The sender email server uses the domain name to find the recipient domain's MX record. It, then, uses the MX record to find the recipient domain's email server IP address (*see the **Simple Email Flow** section for details*).
- ◆ In order to receive emails, you must register a unique domain name from a DNS hosting service provider.
 - ◇ easyDNS, NO-IP.com, and GoDaddy are the common DNS hosting service providers in Canada.
- ◆ Once you own a domain name, you can logon and change its MX record to point to your IP address.

For example, here is the NO-IP.com MX GUI:



The screenshot shows the 'Mail Options' section of the NO-IP.com control panel. It features a table with two columns: 'MX Record' and 'MX Priority'. Below the table, there is a text input field containing 'www.{domain_name}.com' and a dropdown menu set to '5'. A note below the form states: 'If you would like a more MX records, please upgrade to [No-IP Plus](#) or [Enhanced](#).'

- ◆ **Note:** MX record is not using an IP address, MX record is using a domain name.
 - ◇ Once the sender email server obtained the domain name from its MX record, the server then performs another *nslookup*^[30] to get an IP address from the domain name.

Using Dynamic IP address



If you already have a static IP address, please skip this section.

The following diagram shows the common DHCP internet connection configuration:



For the dynamic IP address subscriber, you must use the [DDNS^{\[31\]}](#) service to continuously update your DNS entry and IP address. Today, most firewalls have this DDNS service (see the following two examples). Europa also provides this DDNS service (see the Europa Reference Manual for the details).

Dynamic DNS

Use a dynamic DNS service

None

DynDNS.org [Click here for information](#)

TZD.com [Click here for free trial!](#)

ngDDNS [Click here to register](#)

Dynamic DNS

Use a Dynamic DNS Service

Service Provider:

Host Name:

User Name:

Password:

Use Wildcards

SMTP inbound service

Europa can be installed behind a firewall. The firewall administrator must define an SMTP Port Forward rule to forward all the SMTP inbound traffic from WAN port 25 (*SMTP port*) to Europa (or your email server) IP address.

SMTP outbound services

PTR record

For detecting forged email address, most email servers perform [reverse DNS lookup^{\[32\]}](#) on the *PTR record* of the sender's email domain. This lookup checks the TCP/IP IP address with its *canonical name (CNAME)* [\[33\]](#). For

Europa_Setup_Docs

your Europa (or email server) to send out emails without being dropped, your PTR record should be setup properly.

- For Bell and Rogers subscribers, your outbound emails are relayed to and sent out from their email servers; no setup is needed.
- For TekSavvy subscribers, TekSavvy sets up the PTR record for its clients; no setup is needed.
- For other ISP subscribers, use the following commands to verify your PTR record. Contact your ISP to setup your PTR if it does not exist.

```
In the following example, "69.165.167.114" is your static IP address
# nslookup 69.165.167.114
114.167.165.69.in-addr.arpa      name = 69-165-167-114.dsl.teksavvy.com.
```

If the return address matches the above IP address, your PTR record is setup.

```
# nslookup 69-165-167-114.dsl.teksavvy.com.
Address: 69.165.167.114
```

If you do not understand the above terminologies and technologies, please consult your network administrator or the Europa resale vendor.

Europa System Installation

In the normal operation mode, Europa only needs two connections: power and *Ethernet*^[34] LAN connections.

In the system setup mode, Europa needs one or all of the following connection methods:

1. Use Ethernet crossover/straight cable (see the *Europa Quick Setup Guide* for details).
2. Use Europa console connection: VGA monitor and keyboard. In the following section, this method is explained.

Network parameters

Normally, you are using *Class C*^[35] LAN network. If your firewall (the *gateway*^[36]) is using **192.168.0.1** LAN address, then the IP addresses of all your network devices should be in the range of **192.168.0.2 - 192.168.0.254**, inclusive. If your LAN configuration is more complex, please consult Europa resale vendor for help.

Europa is a network device. It requires the following network parameters:

Parameter Type	Example Value
Static IP address	192.168.0.74
<i>Netmask</i> ^[37]	255.255.255.0 (for <i>Class C</i> network)
Gateway (firewall)	192.168.0.1
DNS server IP address	192.168.0.31 (If your firewall supports DNS service, then use your firewall address here. Otherwise, use the DNS address provided by your ISP.)

Setup Europa

1. Connection: Power plug, Ethernet cable to the firewall (or *Switch* ^[38]), VGA monitor, and Keyboard
2. Power On and see the following display

```

Europa Anti-SPAM & Anti-Virus (fail-over) Email Server System Console
Jovian Technology Inc. Copyright 2009 (http://www.jovian.ca)

System Information
Model:          Europa 1000
Firmware:      3.0.09196.0.2 (Jul 15, 2009 12:34:39)
Serial #:      013313-013313-013313
MAC Address:   CE:18:61:18:61:CE
Expiry Date:   2009-10-10
Reg UID:       0 out of 100
Disk Space:    0 out of 0
Hostname:      europa.localhost
Uptime:        System has been running for 1 min

Network Parameters
Ethernet Mode: Static [-----]
IP Address:     192.168.0.74 [-----]
Netmask:       255.255.255.0 [-----]
Gateway:       192.168.0.1 [-----]
DNS 1:         192.168.0.31 [-----]
DNS 2:         [-----]

Main Menu ID Password
New:           [ ] No space and single quote character
Again:         [ ]

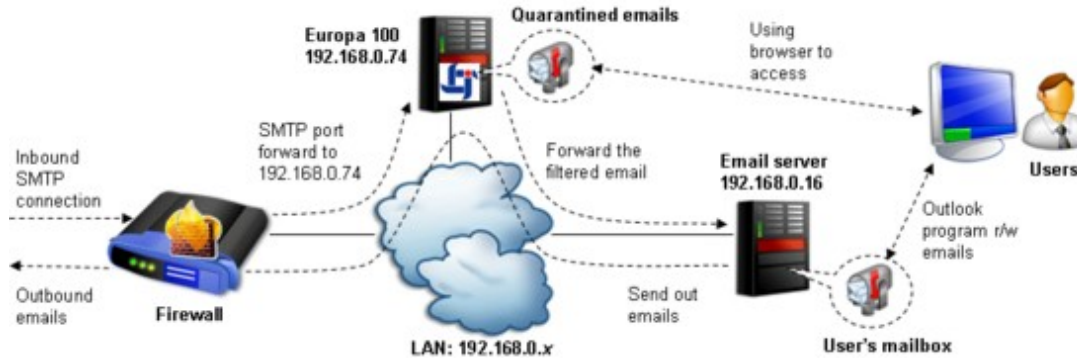
< Submit > < Cancel > < Reboot > < Poweroff > < Manufacture Reset >
Press: [TAB] - Navigate [ENTER/SPACE] - Select [CTRL-C] - Refresh screen
    
```

3. Enter all of the above network parameters and then **reboot**.
4. During the Europa reboot process, VGA monitor and keyboard can be disconnected from Europa machine. Wait for a few minutes for it to reboot.
5. After the reboot process is completed, use a browser to connect to your Europa Web GUI <https://192.168.0.74/europa>

Europa as different email solution

Europa as a spam filter

If your email server is working properly, there is no reason to replace it. In this case, Europa can be set up as a spam filter as follows,



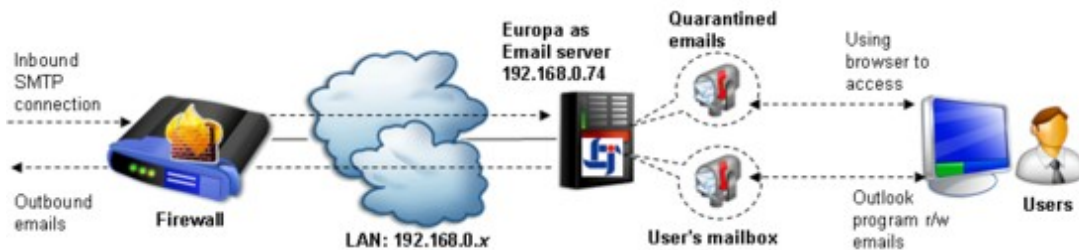
1. Change your firewall's SMTP port forward address to Europa. In this example: change port forward IP to **192.168.0.74**.
2. In Europa's Domain setup page, set the email server IP (See the *Domain setup* section). In this example: it is **192.168.0.16**
 - ◆ **Note:** Europa can support multiple domains and multiple email servers. Each domain has its own email server setup parameters.

Europa_Setup_Docs

3. Set up your outbound configuration in Europa (See the *Configure Europa as an Outbound Email Filter* section).
4. In your email server, set the outbound email *Smart Host* ^[39] parameter back to Europa. Now, Europa can perform as an outbound email filter.
5. Now, the user can do the following:
 - ◆ use an email client program (eg: Microsoft Outlook) to read/write the filtered emails.
 - ◆ use the web browser to access Europa's quarantined emails and manage his/her spam filter parameters.

Europa as an email server and spam filter

If you do not have an email server, Europa can be both a spam filter and an email server. Both users' mailbox and the quarantined emails are stored inside Europa as follows:



1. Change the firewall's SMTP port forward address to Europa's IP address. In this example: change port forward IP to **192.168.0.74**
2. In Europa's Domain setup page, set to local email server mode (see the *Domain setup* section).
 - ◆ **Note:** Europa can support multiple domains and multiple local email servers.
3. The User may access Europa's emails as follows:
 - ◆ Use an email client program (ex: Microsoft Outlook) to read/write the Europa filtered emails.
 - ◆ Use the web browser to access webmail to read/write the Europa filtered emails.
 - ◆ Use the web browser to access the quarantined emails and manage his/her spam filter parameters.

Europa as a hot standby redundant email server solution

Email server is an essential service for most organizations. For business continuity, a hot standby redundant email server solution should always be considered. However, the cost of email server clustering solution is too high; and requires sophisticated setup and administration skill. Europa can be configured as a **Hot Standby Redundant** email server.

When Europa acts as spam filter, Europa can support per domain email server hot standby redundancy mode as follows:

Europa_Setup_Docs



1. Setup Europa in spam filter mode (refer to *Europa as a spam filter* section).
2. To turn on the **Hot Standby Redundancy** mode:
 - ◆ Logon as **admin** user with the **Advanced Menu**
 - ◆ From the **Administration** drop down menu, select **Service** menu item.
 - ◆ In the **Domain Service Administration** panel, select the **Domain Name**.
 - ◆ Set the **Hot Standby Redundancy** radio button to **Enable**.
 - ◆ Select your **days** option for **Remove emails for Hot Standby after**. Click **Update**.

While your email server is down, Europa will queue emails for delivery. Meanwhile, users can access their recent emails from Europa's Webmail program. The users can use Europa to read and write emails as usual. When your email server is back online, all the queued emails will be delivered to your email server.

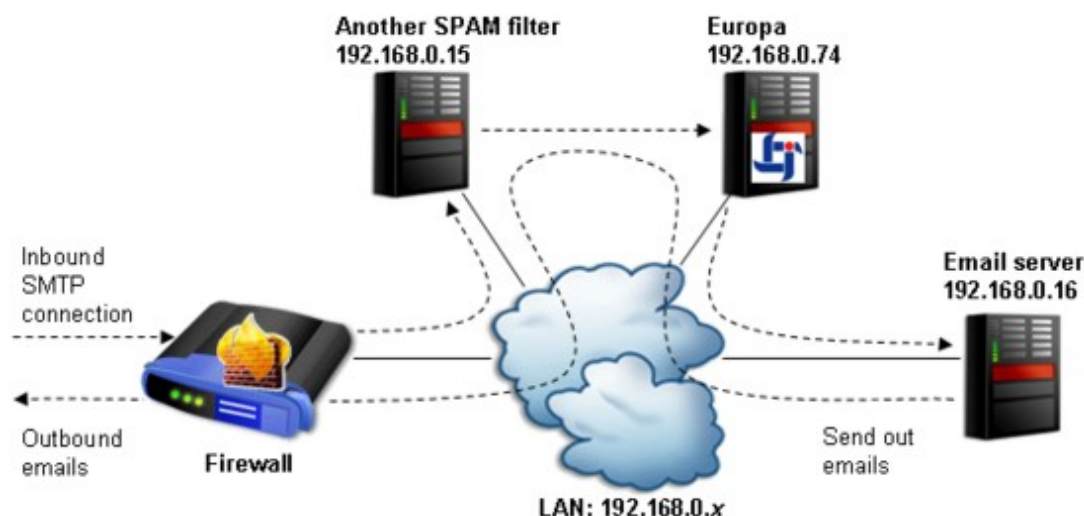
Europa as a Second Level Spam Filter

If you already have a spam filter in place and are not satisfied with the filtering results, you may relay the filtered emails to Europa as a second level spam filter. When Europa is installed as a second level spam filter, it is most useful to configure Europa as a **Personalized Spam Management system**. This Personalized Spam Management (**PSM**) is a unique (patent pending) feature of Europa. After an email passes through Europa's multilayered filter, Europa can add PSM icons (URL) into the email (see the *Europa Reference Manual* for more details). These icons embedded the callback URLs to Europa website. When the user reads the email, s/he can click these PSM icons to quickly black/white list the sender, or access his/her own spam summary page.

PSM is a very user-friendly feature as the user does not need to

- Remember Europa's IP address;
- Cut/Paste the sender email ID into Europa's Black/White list web page.

This PSM functionality is included in all of the above configurations. If you already have both spam filter and email server, and would also like to use Europa as a secondary email filter, you can configure Europa as follows:



1. Setup Europa in spam filter mode (refer to *Europa as a spam filter* section).
2. To configure Europa as an intermediary between the primary spam filter and the email server:
 - ◆ Logon as **admin** user with the **Advanced Menu**
 - ◆ From the **Setup** drop down menu, select **System** menu item.
 - ◆ In the **Mail Setup** panel:
 - ◇ Select **Behind Mail Gateway** to **Enable**.
 - ◇ Enter the IP address of the first level spam filter in the **Mail Gateway IP** field. In this example: **192.168.0.15**.
3. Logon to your primary spam filter, change the email delivery IP address from the IP of email server to the IP of Europa. In this example: from **192.168.0.16** to **192.168.0.74**.
4. Logon to the email server, change the Smart Host IP address from the IP of the primary spam filter to the IP of Europa. In this example: from **192.168.0.15** to **192.168.0.74**.

- Europa is designed to retain quarantined emails and to act as an email server.
- After setting your Europa as one of the above configurations, you must enter all the network and application parameters in order for Europa to work.
- The domains and the user IDs information are the most essential data on Europa (see the next section).
- By default, Europa does not accept any unknown domains or any unknown user ID emails.

Additional Network Configuration

There are three standard methods to access Europa emails: **Webmail page**, **POP3** and **IMAP** protocols. When users connect from the LAN environment, they can simply use the internal IP address (Ex: **192.168.0.74**). For accessing Europa from the Internet (WAN), the following network configurations are needed.

External access parameters

Add the following port forward rules to the firewall.

Inbound Port Name	Port Number	Forward to Europa's IP and Port
SMTP port	25	25 (For Europa to receive incoming emails.)
HTTP port	80	80
HTTPs (SSL) port	443	443 (If different HTTPs port is used, then change this accordingly.)
SMTPs (SSL) port	465	465
IMAPs (SSL) port	993	993
POP3s (SSL) port	995	995

From the above **domain name** and **MX record** setup section, the domain's DNS record should point to the firewall's WAN IP address. User's email client program should use the domain name rather than the IP address. When the user's machine tries to access Europa, the TCP/IP DNS lookup process will route these calls to the firewall WAN IP address; the firewall will then route (port forward) these calls to Europa's LAN IP address.

Optional DNS configuration

In the above TCP/IP DNS lookup process, the public DNS servers replies with the domain's firewall IP address. Even when such user is located inside the LAN environment, his/her calls are still using firewall WAN address to route back to internal Europa machine. This domain name and DNS setup still works; however, it increases the firewall workload and reduces the network throughput.

The following is optional: If your organization has an internal DNS server, add a local DNS entry to override the domain name and point to Europa's IP address. For example:

```
Local DNS entry:   xyz.com  ->  192.168.0.74
```

When the user is working inside the LAN environment, the DNS lookup process will reply with the local Europa's IP address rather than the firewall WAN IP address. All the subsequent Europa calls become local LAN traffic. (Please refer to the *Internal Route To Europa* section in the Quick Setup Guide for more details.)

Administrate User IDs

Different User ID Types

When Europa is configured as a spam filter, Europa recognizes the following user ID types.

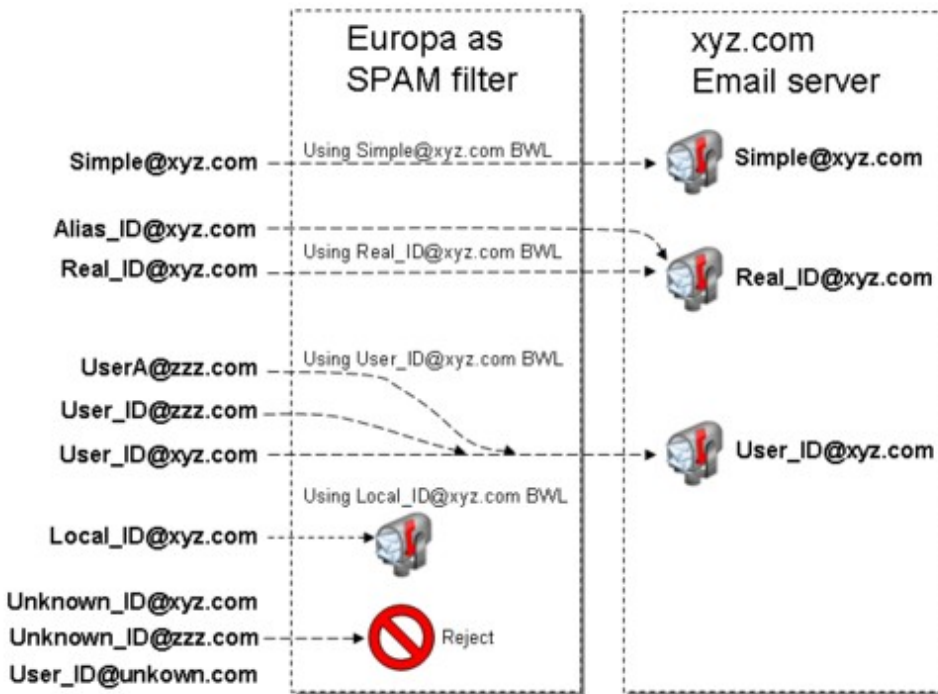
The *user id example* listed beside each user ID type is illustrated in the diagram below.

- **Real User ID** (ie. *Simple@xyz.com*): The user email ID has an actual mailbox in the email server.
- **Alias User ID** (ie. *Alias_ID@xyz.com*): A forwarding email address of a real user ID.

- **Virtual domain** (ie. *User_ID@zzz.com*; *zzz.com* is the virtual domain of alias user ID *User_ID@zzz.com*): An alias user ID that has its domain not belonging to the current domain of real User ID. The domain name only exists in Europa and is not defined in the email server.
 - ◆ Europa maps the virtual domain user ID to the real user ID.
- **Virtual Local user ID** (ie. *Local_ID@xyz.com*): The user's mailbox is located in Europa machine, rather than in the email server.
 - ◆ The email server does not even know this Europa local email user ID.
- **Unknown user ID and unknown domain name** (ie. *User_ID@unknown.com*): For all the email addresses that Europa does not recognize, Europa optionally rejects all those SMTP connections.

When Europa is configured as both spam filter and email server, Europa recognizes all the above user ID types except for the **Virtual Local user ID**; and all the emails are delivered to the **local user mailbox**.

The following diagram illustrates how the emails are delivered to the user's mailbox on the email server for each user type.



Recipient Email ID	User ID type	Domain type	Europa user's spam setting ¹	Deliver to or Remark
Simple@xyz.com	Real User ID	Real Domain	Simple@xyz.com user setting	Simple@xyz.com mailbox of Email server
Real_ID@xyz.com	Real User ID	Real Domain	Real_ID@xyz.com user setting	Real_ID@xyz.com mailbox of Email server
Alias_ID@xyz.com	Alias User ID	Real Domain	Real_ID@xyz.com user setting	Alias_ID@xyz.com mailbox of Email server ²
User_ID@xyz.com	Real User ID	Real Domain	User_ID@xyz.com user setting	User_ID@xyz.com mailbox of Email server

Europa_Setup_Docs

User_ID@zzz.com	Virtual domain (zzz.com) User ID		User_ID@xyz.com user setting	User_ID@xyz.com mailbox of Email server Europa changes the recipient ID to User_ID@xyz.com
UserA@zzz.com	Virtual domain (zzz.com) User ID		User_ID@xyz.com user setting	User_ID@xyz.com mailbox of Email server Europa changes the recipient ID to User_ID@xyz.com
Local_ID@xyz.com	Virtual local User ID	Real Domain	Local_ID@xyz.com user setting	Deliver to Europa local Local_ID@xyz.com mailbox
Unknown_ID@xyz.com	Connection rejected since no such User ID in real xyz.com domain			
Unknown_ID@zzz.com	Connection rejected since no such User ID in virtual zzz.com domain			
User_ID@unknown.com	Connection rejected since no such unknown.com domain			

- ¹ Each Europa user ID has a Black/White Listing (**BWL**) and a set of spam parameter settings.
- ² To preserve the incoming emails behavior, Europa does not change alias ID to the real user ID.
 - ◆ Some email servers merge both alias and real user emails into one mailbox.
 - ◆ Some email servers direct these emails to different email mailbox(s).

What happens if a virtual domain is now defined in the email server?

Europa knows nothing about this change in the email server. To turn the virtual domain into a real domain, You must manually add/change this domain information on Europa. For the existing virtual domain user IDs, Europa will not break the user IDs mapping behavior. You must manually redefine their email delivery destinations.

More than one domain and more than one email server

LDAP and Active Directory integration

Most organizations use *LDAP*^[40] or *Active Directory* ^[41] to manage their users' information. Europa can support one LDAP integration per domain. Periodical automatic LDAP sync function is supported. To setup the LDAP and Active Directory integration, please refer to *Europa Reference Manual* for more details.

Operation Parameters

Why should I care about the operation parameters?

Europa has a set of default operation parameters. These parameters are suitable for most organizations. However, each organization may have their own special needs and requirements such as

- Inbound/Outbound transfer of large size emails
- Special spam keywords that are only commonly identified within organization
- Protection under Zombie attacks
- Different security policies
- Customized Black/White List
- Different network configurations
- ..., many, many more

Here is an example: When your domain is under zombie attack by the spammers, Europa's Heuristic Connection Protection (HCP) service automatically adds firewall rules to block those zombies' IP addresses. You may want to change the detection parameters and the blocking duration of the HCP service.

In the following section, some of the essential operation parameters are described. This document does not intend to cover all parameters. For a complete set of functionalities description, please refer to the *Europa Reference Guide*.

Note: The following section is based on the *Europa System Administration Advanced Menu* structure.

System operation parameters

Europa is a network email appliance. The first layer of defense is the TCP/IP and SMTP connection level. The following are the network level defense parameters.

- **Mail Setup** : Setup > System. The following parameters prevent spammers from degrading your TCP/IP SMTP connections.
 - ◆ **Mail Connection Time Limit** (default: 120 seconds)
 - ◇ If your ISP subscription is a low speed connection, a longer connection time limit is needed. However, it is easier for the spammers to stall your connections.
 - ◆ **Mail Size Limit** (default: 5 MB)
 - ◇ Email communication was originally designed for text messages and not for files transfer. Most text email sizes are under 1MB. Today, emails are used for attaching multimedia files, as a result the size of emails have increased. When your users transmit large size emails, you need to increase the value of this parameter. Increasing the size makes it easier for the spammer to slow down your connection.
 - ◇ In general, it is a bad idea to transmit file in email because:
 - Emails are not secure so the files can be easily intercepted.
 - Transmitting emails with large files slows down your SMTP connection.
 - ◆ **Destination Concurrency Limit** (default: 4) and **Destination Recipient Limit** (default: 25)
 - ◇ These prevent the zombie machines from creating massive connections and sending emails to a massive recipient list.
- **Connection Level Services** : Filters > Connection Level Protection (CLP)
 - ◆ **IP Access List**: This is an email relay service. By default, Europa blocks all SMTP network connections from the internal network. If your web servers / application servers generate email to Europa, please add their IP addresses to this list.
 - ◆ **SMTP Level Unknown User Rejection** (default: Disable). This prevents spammers from performing Directory Harvest Attack.

- ◆ **Bounce Verification** (default: Disable). This prevents the misdirected "undeliverable email" bounce messages from forged sender spam.
 - ◇ When outbound emails are sent/relayed out via Europa, a Europa **Digital Watermark** is added into the header of each outbound email. When this message is bounced back, Europa can recognize its own outbound email.
 - ◆ **SMTP DOS Attack Protection** (default: Enable). When Europa detects a zombie machine trying to hold up all SMTP connections, Europa automatically adds this zombie machine into the firewall rule list.
-
- **Overridable Whitelist services** : Filters > Connection Level Protection (CLP)
 - ◆ **Whitelist IP** : This is to opt-out the known good IP addresses from the email anti-spam service. By default, Europa examines all the incoming SMTP calling IP addresses. When a calling IP address is accidentally added to the *Realtime Blackhole list (RBL)* ^[42] (see below), such IP address will be blocked from sending emails to your email server, this service allows you to define and whitelist such IP from undergoing the calling IP verification processes.
 - ◆ **Domain** : same functionality as above, except for using domain name as the exception list.
 - ◆ **Heuristic Connection Protection (HCP)** (default: Enable) : HCP service automatically adds rules to block the zombies from connecting. The attack detection parameters are number of occurrences within number of minutes (The default is 5 times in 2 minutes). During the zombie attack, these parameters should be changed to "less number of occurrences in shorter period of time".
 - ◆ **Greylist** (default: Disable) : *Greylisting* ^[43] is an anti-spam service. It is based on the email server *busy & retry later* behavior. Most spammers do not spend time to retry. A typical email server will normally try a couple times to deliver the email to the destination.
 - Greylisting itself can effectively block 70+% of the spammers. However, this method requires the sender email server to retry. Only the **first-time** sender's incoming email is delayed.
 - ◆ **Real-time Blackhole List RBL** (default: Enable) : For each incoming SMTP call, Europa checks the calling IP address with a set of (admin-selected) public RBLs. When a zombie (or spammer) machine is identified by other internet users, its IP address is added to some RBL(s). Europa rejects the SMTP call if the caller's IP is blacklisted by the chosen RBL(s).
 - Note: One of the most effective RBL is the **zen.spamhaus.org** server.
 - ◆ **Sender Policy Framework SPF** (default: Disable) : *SPF* ^[44] is based on a sender policy of the domain owner. Europa rejects the forged SPF return paths.
 - Caution (Enable at your own risk): SPF record is not commonly implemented, your contacts may be blocked; make sure you whitelist all the known important contacts as a precaution of dropping their emails.
 - ◆ **Reverse DNS (rDNS) Lookup** (default: Disable) : This is an SMTP connection level PTR record rDNS lookup service (see the PTR section above). rDNS is an effective way to detect forged calling IP address.
 - Caution: Not all organizations (especially the small organizations) have setup their PTR records, your contacts may be blocked; make sure you whitelist all the known important contacts as a precaution of blocking them.

Once the email is accepted by Europa, the second layer of defense is the Anti-Virus and Anti-Spam scanners. The following are the scanners operation parameters.

- **System AntiVirus** : Filters > Anti-Virus

- ◆ **Signatures synchronization** (default: Enable) : By default, Europa downloads virus signatures from the public anti-virus database.
- ◆ **Synchronize Virus Definitions every** (default: 4 hours) : When a new virus is found, such virus signature is added to the public anti-virus database. Synchronize every 4-6 hours is considered an acceptable length of time.
- ◆ **Max number of files in zip attachment** (default 50) : If an email has a zip attachment, Europa uses this parameter to prevent the **zip bomb** (recursive zip structure) virus.

Note: Most viruses are downloaded from HTTP Web download session. Europa anti-virus service is only used for email security. An anti-virus software is still essential for the user's machine.

- **System Anti-Spam Setup** : Filters > Anti-Spam
 - ◆ **Default Keywords Download** : Every night, Europa downloads a set of latest spam keyword rules from the Jovian web server.
 - ◆ **Spam Keywords List** : Allows **admin** to define a set of special keywords for their Europa anti-spam filter. If the score of the keyword is a positive value, it increases the spam score. If the score is a negative value, it decreases the spam score.
 - ◆ **Optical Character Recognition OCR** (default: Enable) : If the email has an image attachment, Europa uses OCR scanner to detect the keywords from the image file. The spam image files are generated by the graphic utility program. OCR program can trace the common font types and recognize the embedded words for keywords comparisons.

Note: OCR does not work for those continued color hue phony style image file.
 - ◆ **Check External Spam Database** (Default: Enable) : The RAZOR database is checked against for spam detection.
 - ◆ **Soft rDNS** (default Disable) : The **Reverse DNS (rDNS) Lookup** performed in the SMTP connection level drops the TCP/IP connection directly. This soft rDNS is performed during the spam analysis, it only increases the spam score when rDNS lookup fails.

After the email is scanned by the Anti-Virus and Anti-Spam scanners, the email will be examined by the *domain level* anti-spam rules, followed by the *user level* anti-spam rules.

Domain operation parameters

System operation parameters deal with hardware and communication related configurations; while domain operation parameters deal with application, email server and other related services. In the following section, only the essential domain services are explained.

- **Email Service** : Setup > Domain Setup > Inbound > Edit a Domain
 - ◆ **Enable Email Service** (default: Disable). When this parameter is enabled, Europa acts as an email server for this domain. Otherwise, Europa relays out all the filtered emails to the email server of **External Mail Server IP** address.

- **Outbound Relay** : Setup > Domain Setup > Outbound
 - ◆ **Outbound** (default: Disable). If this function is enabled, all the outbound emails will be forwarded to the Relay host.

Domain Service groups a set of related services. These services affecting how the user receiving emails and how the mail flow to different destination.

Domain Service : Administration > Service > Domain Service Administration

- **PSM** (default: Enable). By default, all the filtered emails (except for the whitelisted sender) will include PSM icons which contain the call-back URL links. **PSM** feature can be enabled in a per user ID basis.
- **MPOP** (default: Enable). When this parameter is enabled, the domain users can POP emails from other email servers.
- **Forwarding Service** (default: Disable). When this parameter is enabled, the user can forward the filtered email to an external email address such as BlackBerry email address.
- **Outbound Mail Scan Service** (Default: Disable). When Europa is configured as a spam filter, the external email server's Smart Host parameter may be pointing to Europa's IP address and **Outbound Mail Port**. In such a case, all its outbound emails are relayed to Europa.
 - ◆ **Note**: By default, Europa's **Outbound Mail Port** is **2525** which is defined in Setup > System > Mail Setup panel.
 - ◆ The external email server IP address should be included in Europa Anti-relay service's **IP Access List** (see the System operation parameters).
- **Mail Server Health Check** (default: Enable). If an external email server is configured, Europa will check such email server TCP/IP status periodically. When such email server cannot be connected, Europa will send notification to the administrator.
- **Hot StandBy Redundancy** (default: Enable). When this parameter is enabled, Europa will keep a copy of all the filtered emails in Europa. These local copies will be removed after a *configurable number of days*.
- **Quarantine Synchronization** (default: Disable). This feature only applies to the external email server setup with a condition that such email server supports IMAP protocol.
 - ◆ When this parameter is enabled, Europa periodically synchronizes its local quarantined emails with the **Europa Junk** folder on the external email server for each domain user.
 - ◆ *Note*: This feature is always enabled when **Europa** is an email server. When Europa is an email server, it always synchronizes its quarantine emails with its **Europa Junk** folder.
- **Same Domain Senders Configuration** : Filters > Same Domain Sender
 - ◆ In general, the senders in the same domain are located inside the LAN environment. When an external server makes the SMTP calls with the same domain sender ID, the email highly likely comes from the spammer forging the sender ID.
 - ◆ There are some special cases which this feature allows some defined user email IDs to send back emails.
 - ◇ BlackBerry email server uses the original user email ID to call back.
 - ◇ Remote employees use external ISP email servers to relay emails back.

Domain user spam control parameters such as Black/White List and spam score level control.

- **Black/White List Administration** : PSM > Black/White List
 - ◆ You can access all, from domain to user level's, black/white lists.
 - ◆ Europa can automatically whitelist the outbound recipient email IDs.
 - ◆ Europa can block users from sending outbound emails to the blacklisted recipients.

- **Domain Anti-Spam Setup** : Filters > Anti-Spam
 - ◆ **Days of Quarantine** (default: 14 days). The quarantined emails will be removed after *number of days*.
 - ◆ **Email Score Control Level**: The anti-spam scanner will assign a score to each filtered email. The following control levels are used to determine what is a spam and how to handle it.
 - ◇ **Drop** (default: 10) - Email will be dropped when score > *Drop* score.
 - ◇ **Quarantine** (default: 6.4) - Email will be quarantined when score < *Drop* score and score > *Quarantine* score.
 - ◇ **Tag** (default: 4) - Email will be tagged when score < *Quarantine* score and score > *Tag* score.

Domain user browser session control.

- **Session Limit** : Setup > Domain Setup > Inbound > Edit a Domain
 - ◆ **User Session Time Limit** (default: 8 hours) is the browser's logon session expiration time. Changing this value reflects different security level for different domain.

User operation parameters

The users have their own set of spam operation parameters. However, by default, most of them are disabled and domain level setup values are used. You can exclusively give the change permission to individual user ID. The domain and user level operation parameters have the same meaning and operate the same. The following shows the operation parameters only in the user level. (The *Europa User Guide* covers all user interfaces and their usage.)

- **Sender Profile Analysis**

When the domain email service is enabled (ie. having "Europa as email server"), the user's mailbox resides in Europa. For each email, Europa can scan and collect sender's profile information for the user. The analysis result includes the Black/White list status of and the number of emails received from each sender.

- **MPOP account setup**

After you enable the MPOP service for all users, each user still needs to setup his/her MPOP account(s). In most cases, you may not know your user's external email account and password.

- **Auto Reply Setup**

User can setup his/her auto reply when s/he is on vacation.

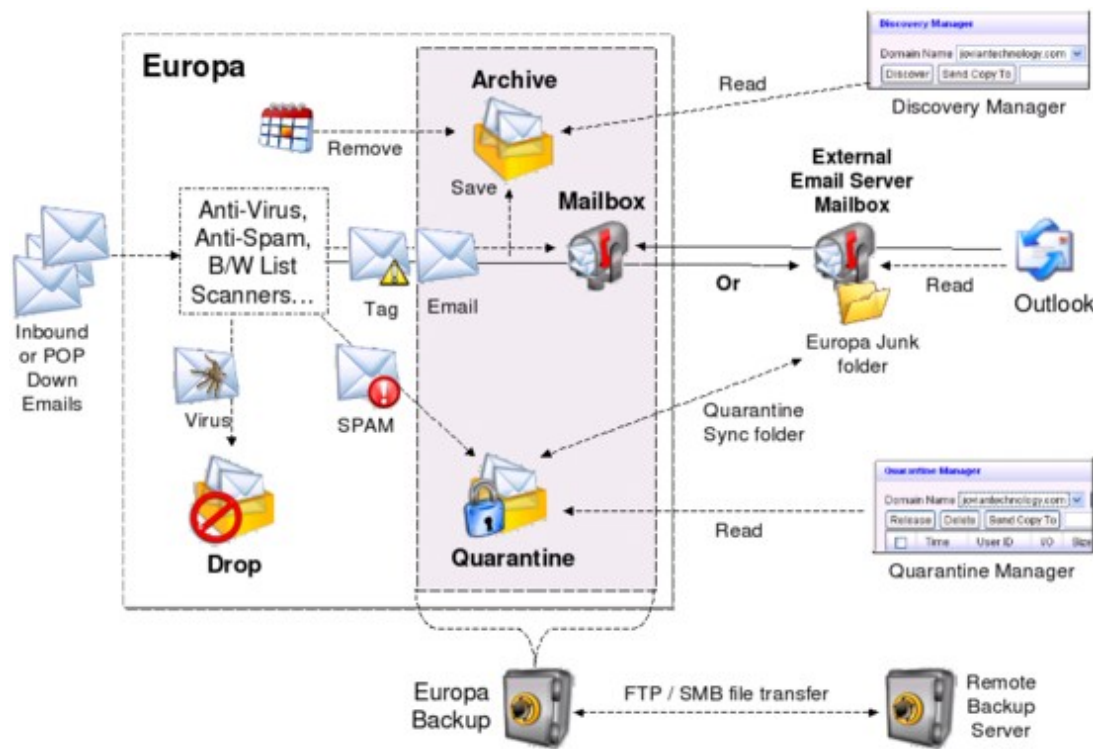
Features

The above sections cover the email communication, system/network setup and configurations, user types, and different levels of operation parameters. However, some Europa unique features are not yet explicitly explained. In the following section, these Europa unique features are presented.

This setup document does not intend to (and cannot) cover all the details of Europa. For the complete reference of functions, please refer to **Europa Reference Manual**.

Email Path inside Europa

To illustrate Europa special features, let's start with how the components and the tools are used in the email path diagram.



The email flow starts with either an inbound or a pop-down email.

- An email can be received by the inbound SMTP call or by the Europa MPOP client program.
- All the emails are then scanned by a set of filters: anti-virus, anti-spam, Black/White list, ..., etc.
 - Note:** Europa has more than 14 different scanning filters.
 - ◆ If the email contains virus, the email is either dropped or quarantined to the domain admin's quarantine mailbox.
 - ◆ If the email is identified as spam, the email is quarantined in the user's quarantine mailbox.
 - Note:** The quarantine mailbox resides in the Europa machine.
 - ◆ If the email is identified as possible spam, it is tagged and sent to the user's mailbox.
 - Note:** The identifying process is using the domain/user defined spam score values.
 - ◆ If the email is a clean email, it is sent to the user's mailbox.
- For all the filtered emails, they are also archived in the Europa machine.
 - ◆ **Note:** The archived emails will be removed after a *domain-specified number of days*.

Local email server or external email server

Europa supports multiple domains. Some domains can use Europa as email servers; in such cases, their users' mailboxes are stored in Europa. For all other cases, Europa forwards the filtered emails to the domain specified email servers.

- Europa allows each domain to define its own email server.
- For the domain that is using Europa as the external email server, Europa allows its user mailbox to be redefined as local mailbox.
- For any user ID, delivery destination can be individually refined.
- Any email client program (Ex: Outlook) can access the local mailbox by POP3 or IMAP protocol.

See the above **Administrate User IDs** section for more details.

Quarantine Manager

Quarantine Manager (QM) allows the user to browse, search, release, and delete his/her quarantined emails. The user can display the email content in either HTML or text format by double clicking the email entry.

Discovery Manager

Europa stores all the filtered emails. Within a *configurable number of days*, the user can recover the filtered email by Discovery Manager. Europa's archiving and discovering processes are designed for short-term recovery only. For long-term discovery, a daily backup plan should be implemented.

Backup and Restore

Europa supports whole system backup or per domain backup. A daily scheduled backup task can only be setup by the **system admin**. Please be sure to have your remote storage (by FTP or SMB) setup for your backup files to be transferred properly.

- The whole system backup is huge, it covers all the configurations, and users' archives, mailboxes, and quarantined emails on Europa.
- The **system admin** can selectively backup the more important domains.

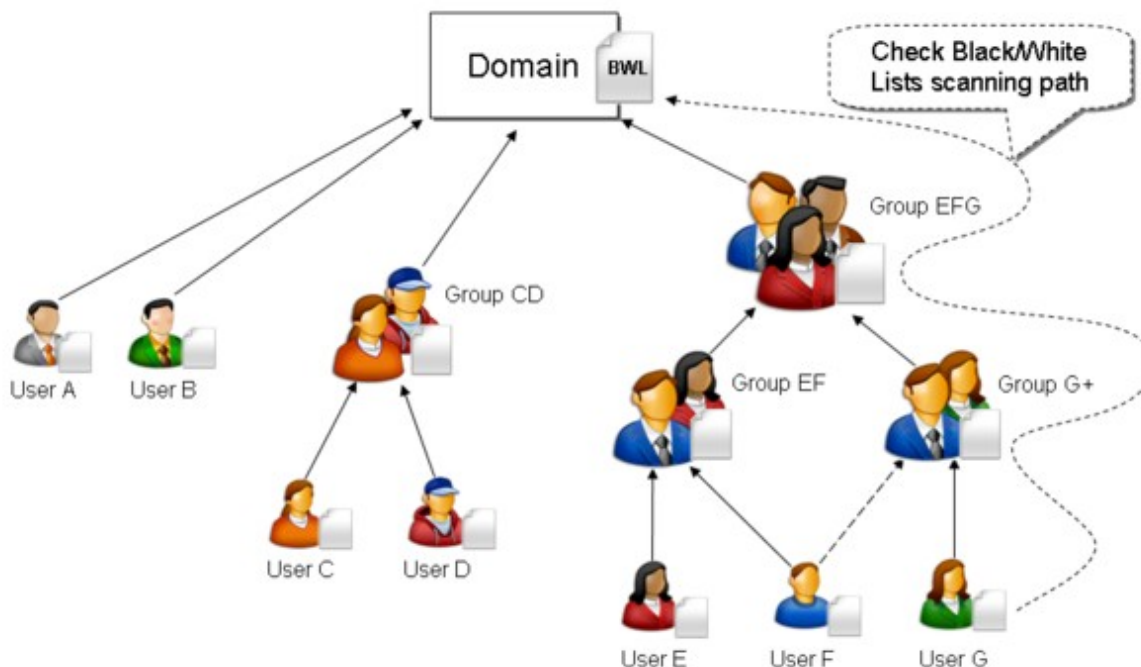
Europa Junk Folder

This feature allows the users to examine their quarantined emails by using their email client programa (Ex: Outlook) without login to Europa. For the local email server, the **Europa Junk** folder is automatically added. For the external email server, Europa uses IMAP protocol to synchronize the quarantined emails with the user's **Europa Junk** folder.

Multiple Level Black/White list

In Europa, Domain and User Black/White List (BWL) are interrelated. In fact, Europa uses groups and

sub-groups to simulate the department and team structure. A group is a logical unit that groups user IDs and sub-groups. The following diagram shows the multiple-level BWL(s) at different levels.



This domain has 7 user IDs and 4 groups. Both domain and user ID have their own BWLs, and each group also has its own BWL.

- **User A** and **User B** are individual users and do not belong to any group.
- **User C** and **User D** belong to **Group CD**.
- **User E** and **User F** belong to **Group EF**.
 - ◆ **Group EF** is the primary group for **User F**.
- **User F** and **User G** belong to **Group G+**.
 - ◆ **Group G+** is the secondary group for **User F**.
- **Group EF** and **Group G+** are the sub-group of **Group EFG**.

BWL scanning path in the multi-level BWL

In the above example, when the email's recipient is **User G**, Europa BWL filter scans the BWL(s) from the bottom (user level) up to the top (domain level). During the scanning process,

- If the sender ID (or sender domain) is matched, the process stops. The email is then either black or white listed.
- If no match is found, then the sender information is not defined in this multiple level BWL path.

Automatically promote the BWL items

When there is a common sender ID or sender domain added by all the users (and/or groups) in the same level, such sender ID or sender domain will be promoted to the next level up.

Primary and secondary group

When an user belongs to multiple groups, the BWL scanning path will start from the primary group first, followed by all the subsequent secondary group(s).

Other features

Outbound auto white list

When a domain outbound scanning service is enabled, Europa can automatically "white-list" and add the recipient email ID to the sender's BWL. After a period of time, when the user's BWL contains all his/her recipients' email IDs, false positives will be minimized.

White on grey

Greylisting is a highly effective spam avoidance technique, it delays the sender's email at its first appearance. However, from time to time, it also delays sender's email who has sent you emails from the past, this is because Greylisting technique is required to clean up its database periodically.

When the sender sends in an email, the sender's information is updated and will not be removed. However, if the sender does not send in any email for a period of time, his/her information will be removed from Greylisting database.

Europa **White on grey** service improves the Greylisting as follows,

- If the sender is white-listed, Greylist checking is skipped.
- Normal Greylisting technique is performed, otherwise.

Email summary: Daily and Hourly

Europa generates and delivers Daily email summary report to the user mailbox. Europa can also generate Hourly email summary report, as scheduled by the user. Europa can optionally generate the hourly report even when there is no email activities for that user.

MPOP clients

Europa's user can configure the MPOP client to pop down emails from other email servers for spam filtering: anti-virus, anti-spam, keywords, and BWL scanning, etc.

There is one drawback in using MPOP client: Europa is designed as the spam filter and email server to handle inbound SMTP calls. In the MPOP case, the sender's (or spammer's) Internet connection (IP address, PTR record, SPF, etc.) information is missing, thus the filtering process less effective.

Notes and References

1. ? http://en.wikipedia.org/wiki/TCP/IP_model
2. ? <http://en.wikipedia.org/wiki/E-mail>
3. ? [http://en.wikipedia.org/wiki/Spam_\(electronic\)](http://en.wikipedia.org/wiki/Spam_(electronic))
4. ? http://en.wikipedia.org/wiki/Computer_virus
5. ? http://en.wikipedia.org/wiki/Domain_name
6. ? <http://en.wikipedia.org>
7. ? http://en.wikipedia.org/wiki/Uniform_Resource Locator
8. ? <http://en.wikipedia.org/wiki/SMTP>
9. ? <http://en.wikipedia.org/wiki/LAN>
10. ? http://en.wikipedia.org/wiki/Transport_Layer_Security
11. ? http://en.wikipedia.org/wiki/Domain_Name_System
12. ? http://en.wikipedia.org/wiki/MX_record
13. ? http://en.wikipedia.org/wiki/Internet_Protocol
14. ? <http://en.wikipedia.org/wiki/Firewall>
15. ? http://en.wikipedia.org/wiki/Wide_Area_Network
16. ? [http://en.wikipedia.org/wiki/Hacker_\(computer_security\)](http://en.wikipedia.org/wiki/Hacker_(computer_security))
17. ? http://en.wikipedia.org/wiki/Port_forward
18. ? http://en.wikipedia.org/wiki/Email_mailbox
19. ? http://en.wikipedia.org/wiki/Post_Office_Protocol
20. ? <http://en.wikipedia.org/wiki/IMAP>
21. ? <http://en.wikipedia.org/wiki/Html>
22. ? <http://en.wikipedia.org/wiki/MIME>
23. ? <http://en.wikipedia.org/wiki/Spyware>
24. ? http://en.wikipedia.org/wiki/Computer_zombie
25. ? http://en.wikipedia.org/wiki/Directory_Harvest_Attack
26. ? <http://en.wikipedia.org/wiki/PDF>
27. ? <http://en.wikipedia.org/wiki/ISP>
28. ? http://en.wikipedia.org/wiki/DDoS#Distributed_attack
29. ? http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
30. ? <http://en.wikipedia.org/wiki/Nslookup>
31. ? <http://en.wikipedia.org/wiki/DDNS>
32. ? http://en.wikipedia.org/wiki/PTR_Record#PTR
33. ? http://en.wikipedia.org/wiki/Canonical_name
34. ? <http://en.wikipedia.org/wiki/Ethernet>
35. ? http://en.wikipedia.org/wiki/Class_C_network
36. ? http://en.wikipedia.org/wiki/Residential_gateway
37. ? <http://en.wikipedia.org/wiki/Netmask>
38. ? http://en.wikipedia.org/wiki/Network_switch
39. ? http://en.wikipedia.org/wiki/Smart_host
40. ? http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
41. ? http://en.wikipedia.org/wiki/Active_directory
42. ? <http://en.wikipedia.org/wiki/DNSBL#Terminology>
43. ? <http://en.wikipedia.org/wiki/Greylisting>
44. ? http://en.wikipedia.org/wiki/Sender_Policy_Framework

Appendix

CentOS 5.3 kernel 2.6.18-128.el5

Copyright (C) 2009 CentOS

http://www.centos.org/docs/5/html/5.2/Deployment_Guide/ln-id2973331.html

amavisd-new 2.4.0

Copyright (c) 2002,2003,2004,2005,2006,2007 Mark Martinec, All Rights Reserved

<http://www.ijs.si/software/amavisd/LICENSE.txt>

apache 2.2.3

Copyright (c) 1995-2007 The Apache Software Foundation

<http://www.apache.org/licenses/LICENSE-2.0>

clamAV 0.95.3

Copyright (C) 2002-2009 Tomasz Kojm

<http://clamav.net/doc/latest/clamdoc.tex>

courier-authlib 0.62.2

Copyright (c) 2000-2007 Double Precision, Inc.

<http://www.courier-mta.org/authlib/>

courier-imap 4.5.0

Copyright (c) 1998-2007 Double Precision, Inc.

www.courier-mta.org/imap/main.html

CentOS 5.3 kernel 2.6.18-128.el5

Copyright (C) 2009 CentOS

http://www.centos.org/docs/5/html/5.2/Deployment_Guide/ln-id2973331.html

GNU General Public License

Copyright (c) 1989,1991 Free Software Foundation, Inc.

<http://www.gnu.org/licenses/gpl.txt>

KompoZer 0.7.10

Copyright (c) 1998-2007 Contributors. All rights Reserved.

<http://kompozer.net/about/>

ImageMagick 6.2.5

Copyright (C) 1999-2005 ImageMagick Studio LLC

logrotate 3.7.4

Copyright (c) 1995-2001 Red Hat, Inc.

<http://www.imagemagick.org/script/license.php>

<http://download.fedora.redhat.com/pub/fedora/linux/core/5/i386/os/repodata/repoview/logrotate-0-3.7.3-2.2.1.html>

mediaWiki 1.13.3

Copyright (C) 2001-2008 Magnus Manske, Brion Vibber, Lee Daniel Crocker, Tim Starling, Erik Möller, Gabriel Wicke, Ævar Arnfjörð Bjarmason, Niklas Laxström, Domas Mituzas, Rob Church, Yuri Astrakhan, Aryeh Gregor, Aaron Schulz and others.

<http://www.mediawiki.org/wiki/Project:Copyrights>

mpop 1.0.17

Copyright (c) 2005,2006,2007 Martin Lambers and others.

<http://mpop.sourceforge.net/documentation.html>

msmtp 1.4.17

Copyright (c) 2005,2006,2007 Martin Lambers and others.

<http://msmtp.sourceforge.net/>

openSSH 4.3p2

Copyright (c) 1999-2007 OpenBSD

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland. All rights reserved

<http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD>

openssl 0.9.8a

Copyright (c) 1999-2007 The OpenSSL Project, All rights reserved.

<http://www.openssl.org/about>

perl 5.8.8

Copyright (c) 1987-2007, Larry Wall

<http://dev.perl.org/licenses/>

perl module Archive::Tar 1.29

<http://search.cpan.org/~kane/Archive-Tar-1.30/lib/Archive/Tar.pm>

perl module Archive::Zip 1.16

<http://search.cpan.org/~adamk/Archive-Zip-1.18/lib/Archive/Zip.pm>

perl module Authen::SASL 2.10

<http://search.cpan.org/~gbarr/Authen-SASL-2.10/lib/Authen/SASL.pod>

perl module BerkeleyDB 0.27

perl module Bit::Vector 6.4

<http://search.cpan.org/~stbey/Bit-Vector-6.4/Vector.pod>

<http://search.cpan.org/~pmqs/BerkeleyDB-0.31/BerkeleyDB.pod>

perl module Carp::Clan 5.3

<http://search.cpan.org/~stbey/Carp-Clan-5.3/Clan.pod>

perl module Compress::Zlib 1.41

<http://search.cpan.org/~pmqs/Compress-Zlib-1.42/Zlib.pm>

perl module Convert::TNEF 0.17

<http://search.cpan.org/~dougw/Convert-TNEF-0.17/TNEF.pm>

perl module Convert::UULib 1.06

<http://search.cpan.org/~mlehmman/Convert-UULib-1.06/UULib.pm>

perl module Date::Calc 5.4

<http://search.cpan.org/~stbey/Date-Calc-5.4/Calc.pod>

perl module Digest::MD5 2.36

<http://search.cpan.org/~gaas/Digest-MD5-2.36/MD5.pm>

perl module IO::Stringy 2.11

<http://search.cpan.org/~dskoll/IO-stringy-2.110/lib/IO/Stringy.pm>

perl module libnet 1.19

<http://search.cpan.org/~gbarr/libnet-1.19/Net/libnetFAQ.pod>

perl module MIME-tools 5.42

<http://search.cpan.org/~dskoll/MIME-tools-5.420/lib/MIME/Tools.pm>

perl module MIME::Base64 3.07

<http://search.cpan.org/~gaas/MIME-Base64-3.07/Base64.pm>

perl module Mail::SpamAssassin 3.1.0

http://spamassassin.apache.org/full/3.0.x/dist/doc/Mail_SpamAssassin.html

perl module Mail::SPF::Query 1.999.1

<http://search.cpan.org/~jmehnle/Mail-SPF-Query-1.999.1/lib/Mail/SPF/Query.pm>

perl module Net::CIDR::Lite 0.18

<http://search.cpan.org/~dougw/Net-CIDR-Lite-0.18/Lite.pm>

perl module Net::LDAP 0.33

<http://search.cpan.org/~gbarr/perl-ldap-0.33/lib/Net/LDAP/FAQ.pod>

perl module Net::Server 0.93

<http://search.cpan.org/~rhandom/Net-Server-0.94/lib/Net/Server.pm>

perl module String::Random 0.21

<http://search.cpan.org/~steve/String-Random-0.21/lib/String/Random.pm>

perl module Tie::File::AsHash 0.08

<http://search.cpan.org/~cangell/Tie-File-AsHash-0.08/lib/Tie/File/AsHash.pm>

perl module Time::HiRes 1.86

<http://search.cpan.org/~jhi/Time-HiRes-1.94/HiRes.pm>

perl module Unix::Syslog 0.100

<http://search.cpan.org/~mharnisch/Unix-Syslog-0.100/Syslog.pm>

php 5.1.6

Copyright (c) 1997-2007 The PHP Group

http://www.php.net/license/3_01.txt

postfix 2.3.3

Copyright (c) 1999 International Business Machines Corporation and others and it was created by Wietse Venema

<http://www.postfix.org/documentation.html>

PostgreSQL Data Base Management System 8.1.11

Portions Copyright (c) 1996-2009, PostgreSQL Global Development Group Portions Copyright (c) 1994-1996 Regents of the University of California

<http://www.postgresql.org/docs/faqs.FAQ.html#item1.3>

Postgrey 1.32.1

Copyright (c) 2004-2007 ETH Zurich, Copyright (c) 2007 Open Systems AG, Switzerland

<http://postgrey.schweikert.ch/>

razor2

Copyright (c) 1999-2007, Vipul Ved Prakash.

<http://razor.sourceforge.net/artistic.php>

samba 3.0.21b

Copyright (C) 1997-2003 Samba-Team

<http://us3.samba.org/samba/docs/GPL.html>

Slidebar

Copyright (c) 2006 webfx

<http://webfx.eae.net/license.html>

Spamassassin 3.2.5

Copyright 2000-2002, Justin Mason. All rights reserved.

SpamAssassin is distributed under the Apache License, Version 2.0

<http://spamassassin.apache.org/full/2.6x/dist/License>

squirrelmail 1.4.6

Copyright (c) 1999-2007 The SquirrelMail Project Team

license <http://opensource.org/licenses/gpl-license.php> GNU Public License

<http://www.squirrelmail.org>

symfony 1.0.12

Copyright (c) 2004-2008 Fabien Potencier

<http://www.symfony-project.org/license>

syslog-ng 2.1.4

Copyright (c) 1999-2004 BalaBit IT Ltd, portions were contributed by Jose Pedro Oliveira

http://www.balabit.com/products/syslog_ng/reference-1.6/syslog-ng.html/index.html

wz_tooltip.js v4.12

Copyright (c) 2002-2007 Walter Zorn.

<http://www.walterzorn.com>

YUI 2.6.0

Copyright (c) 2009, Yahoo! Inc. All rights reserved.

<http://developer.yahoo.com/yui/license.html>