



Technical Information



www.jovian.ca

Europa is a fully integrated Anti-Spam & Email Appliance that offers 4 feature-rich Services:



> **Anti-Spam / Anti-Virus**

> **Email Redundancy**

> **Email Service**

> **Personalized Spam Management**

Anti-Spam/Anti-Virus - an intelligent and powerful multi-level, scoring-based anti-spam system.

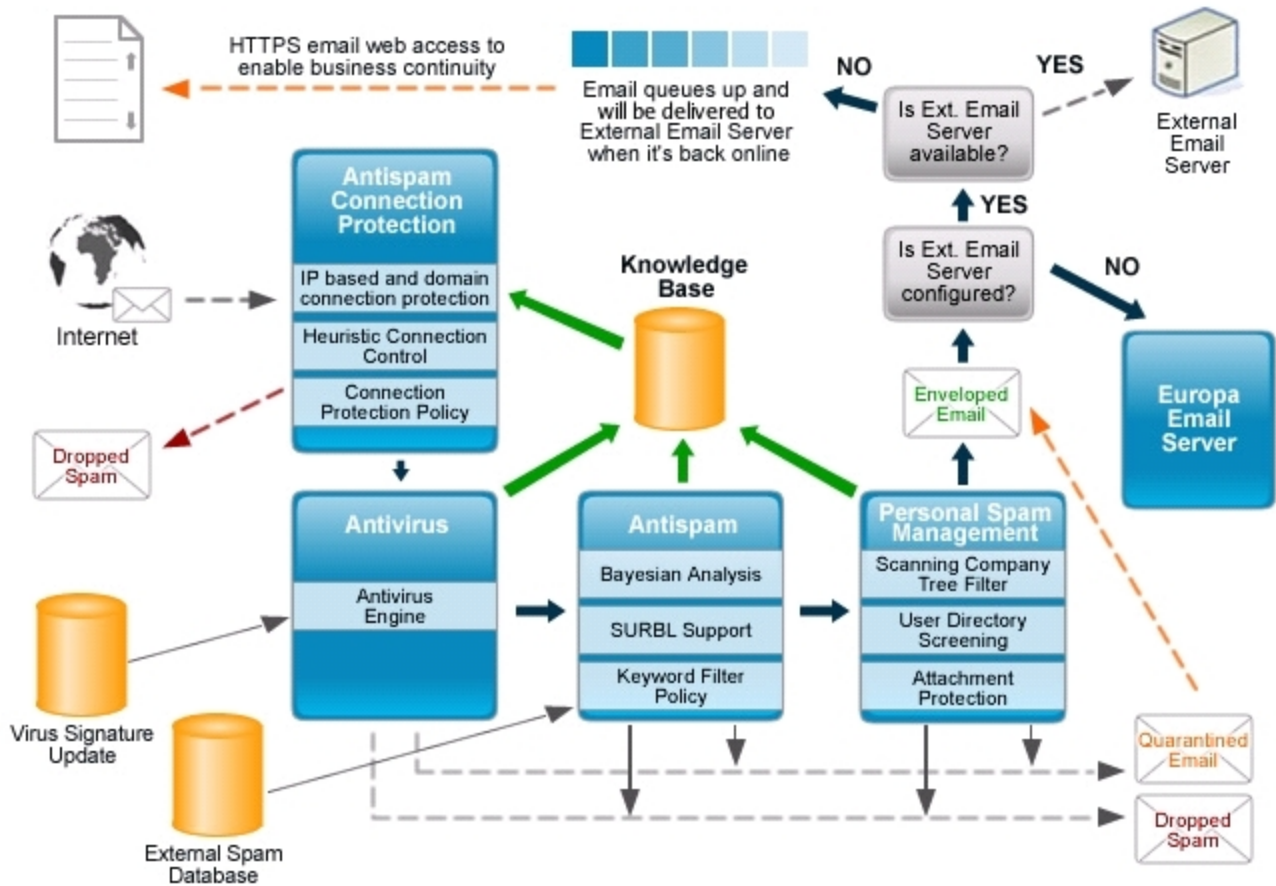
Email Redundancy - can be your hot standby redundant email server.

Email Service - can be your primary or hot standby redundant email server.

Personalized Spam Management (PSM) - self-customization allows your employees to manage and fine-tune their spam filters.

Europa Email Processing

Europa processes incoming emails as follows:



Anti-spam Connection Protection

Spam email is detected at the early stage of email filtering through Anti-spam Connection Protection which occurs during TCP/IP connection. Detected spam emails are dropped.

IP and/or Domain-based Connection Protection

The sender's server is checked for IP and/or Domain validity. It is also checked against external databases of spam server lists. It is checked with the following filters:

- Heuristic Connection Protection

- Sender Verification
- Realtime Blackhole list Check
- Sender Policy Framework Check
- Reverse DNS lookup

Heuristic Connection Control

The heuristic connection protection filter enables Europa to automatically reject a connection from a sender's server when, within a given time interval, the occurrence of a number of harmful conditions is detected from that server. These conditions include the following:

- Unknown recipients
- Virus email
- Spam email

Information is collected during connection time and it is used to check with Europa's local Knowledge Base to avoid hazardous email reception. Administrators can configure the threshold and the duration of occurrences.

Connection Protection Administration Policy

Allows Administrators to specify a maximum connection time and a maximum email size to avoid DoS attacks and large, resource-hungry emails.

Anti-virus

The Anti-virus service consists of an Anti-virus Engine which obtains virus signatures from an external database. Update frequency can be configured from 1 to 8 hours. Recommended update frequency is 4 hours.

Emails are scanned with the Anti-virus Engine: questionable emails are quarantined; high scoring spam emails are dropped.

Anti-spam

This service scans an incoming email using various email filters and generates a spam rating/score for that email. The spam rating is then used to determine whether the email will pass through the filters, be quarantined, or be dropped.

Bayesian Analysis

This filter evaluates the header and content of an incoming email message to determine the probability that it constitutes spam.

SURBL Support

SURBL (Spam URI Realtime Blocklists) helps in identifying potential spam based on message body URIs.

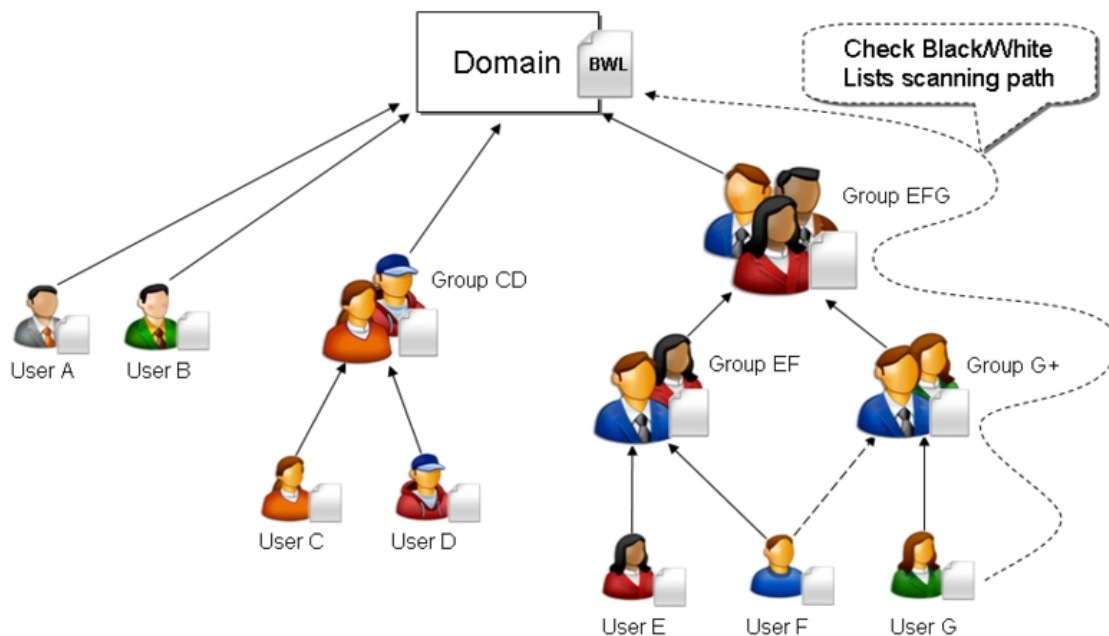
Keyword Filtering Policy

Enables Administrators to define a list of keywords as blacklist or whitelist. Incoming emails are evaluated against the blacklist to determine if they are spam or whitelist to determine if they are legitimate emails.

Personalized Spam Management

The Personalized Spam Management service provides a user-defined filter mechanism for spam emails. It is a multi-level filter based on user-defined blacklists and whitelists. These blacklists and whitelists are organized in a tree structure with the domain level filter situated at the top of the tree. Departments, groups, sub-departments and sub-groups are in branches, and the end users are at the leaves.

Scanning Company Tree Filter



An email, whether ham (legitimate email) or spam, passes through the filter tree from the recipient (leaf nodes) to the top. If the sender email ID of an email matches with one of the multi-level defined filtering rules, i.e. the blacklist, the email is blocked and quarantined; thus the matching process is finished immediately. If there are no matches in the filtering rules, the matching process exits at the top

of the tree. This email is then delivered to the recipient's email account. Similarly, this logic is applied to the whitelist filtering rule. Whenever an email ID is matched on the whitelist, the matching process exits immediately, and the email is delivered to the recipient's email account without any further filtering.

Each delivered email is converted to HTML (multipart/alternative MIME type) if it is not already in HTML format. The email text content is "enveloped" by five(5) "customized" HTML callback URL buttons. In other words, the email content remains the same and the email is "encapsulated" with an extra HTML layer that provides the 5 HTML callback buttons. A user can then select the appropriate action to fine-tune his/her personal email filter. Since these are "customized" URLs, they are encoded with the callback hostname, the recipient email ID, and the sender email ID. After the user receives the enveloped email, he/she can:

- a) Logon to his/her quarantined summary page
- b) Add the sender's domain to the whitelist
- c) Add the sender's email address to the whitelist
- d) Add the sender's domain to the blacklist
- e) Add the sender's email address to the blacklist.

This greatly enhances usability and the interaction between the Email client program and the Email Spam control systems. When the user clicks the URL to blacklist a sender, the control automatically jumps from the Email client program to the web-based Email Spam control system. The sender's email ID is then added to the user's blacklist.

When all leaf users under the same parent node have the same filtering rule, the rule is automatically consolidated to the parent node level. In other words, if all users in a department blacklist the same sender, the rule is automatically consolidated to the next level, and becomes a departmental filtering rule. Similarly, this can be applied to all groups and sub-group levels.

After the system configuration, the structural filters are set up to model the structure of a corporation (integration with OpenLDAP and Active Directory are available). With appropriate capabilities granted, a representative in each level can manage and configure the filtering rules. For example, at the department level, a departmental administrator is chosen to set up the departmental email filter. At the user level, each user is provided with the right privileges to maintain his/her own filter, thus greatly reducing the System Administrator's workload.

As previously mentioned, a filtering rule can be automatically consolidated to the next level if all members within one level have the same rule in their black/whitelist. With the tree structure filter and the auto-consolidation, this method enables a logical extension on the user-level rules to the next level. By induction, this can be applied to a department, a branch, and so on, all the way to the corporate level. Therefore, in the above scheme, each user can accurately fine-tune the email filtering rules that

are applicable to their own group and then to the entire corporation.

User Directory Screening

This filter interfaces with the company LDAP (or Active Directory) to identify the validity of the recipients. For unknown recipients, the emails are dropped or quarantined. The scanned result is updated to the local Knowledge Base to assist with heuristic anti-spam protection.

Attachment Protection

Attachments that appear in any form of executable (e.g. .exe or .xls) are renamed to a non-executable form (e.g. With a file extension '_exe' rather than 'exe'). A user needs to rename this protected file extension to an executable form in order to carry out execution. This protection avoids accidental invocation of execution. This filter expands and extracts any zipped files attached to an incoming email. It then scans through each file in all directories for viruses.

Email Server

The Email Server service allows Europa to be your hot standby redundant email server or your primary email server. Europa interfaces with the LDAP server; mailboxes and passwords are synchronized with all users on the LDAP server.

This service supports both POP3s and IMAPs. It has a web-based email client that uses https for security purposes. It also supports Microsoft Outlook and other email clients.