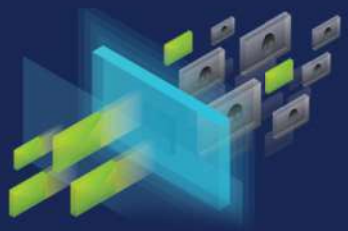
B.L.S. Consulting s.r.l.

JANUSMAIL - Mail Security

Every day Mailboxes and servers are subject to phishing, spam, ransomware, viruses and malware attacks.
JANUSMAIL is a new concept product, the result of 20 years of experience in the electronic mail management, created for:

- Protect emails and servers from attacks and spam
- Identify and resolve forwarding / receiving problems
- Manage massive amounts of emails without slowdowns
- Integrate seamlessly with zimbra servers
- In-depth analysis of incoming and outgoing emails
- Include specific features for service providers



CLUSTER SYSTEM

JANUSMAIL is fully scalable based on the workload required, can be provided as a service on BLS infrastructure, or installed at the customer, on a virtual or physical appliance.
For customers with redundancy needs or high mail loads, typically service providers, it is possible to distribute the load over several servers (clusters) always managed by a single console.You can also enable clustered configurations to increase capacity and guarantee fault tolerance.

ANTISPAM E ANTI PHISHING

Email security is guaranteed by a variety of extremely effective filters in particular against Malware and spam, designed to circumvent the systems of traditional protection.These systems work simultaneously, without slowing down email reception and making multiple and thorough checks.
The Mail Relay architecture also guarantees 100% analysis of incoming emails, regardless of quantity.

ANTIVIRUS & ANTIMALWARE

JANUSMAIL carries out further checks on incoming emails and attachments to identify viruses and malware using database of signatures continuously updated

Multiple Engine Antivirus- Block dangerous file types
Control of compressed archives- Heuristic systems

CLOUD / ON PREMISE OPTION

JANUSMAIL can be delivered as a cloud service, or on-premise for customers who prefer to have it in their own ced.

SAFETY FUNCTIONS

Automatic update of antispam rules
Blacklist and whitelist
Bayesian filter
SPF (sender policy framework),
DKIM (domainkeys identified mail)
DMARC (Domain-based Message Authentication)
Collaborative filters
Content filters
Filters on email format

Janus uses 3 different signature databases for the controls:
CLAMAV: main, daily, bytecode, pua

SANESECURITY: junk, jurlbl, phish, rogue, scam, spamimg, winnow_malware, winnow_malware_links, hackingteam,

SECURITEINFO PRO: securiteinfobat, securiteinfodos, securiteinfoelf, securiteinfo, securiteinfohtml, securiteinfooce, securiteinfopdf, securiteinfosh

Via A.Gramsci 25
27100, Pavia

PI 016606500187
0382/413825

commerciale@bls.it
www.bls.it

B.L.S. Consulting s.r.l.

ATTACHMENT ANALYSIS SYSTEM

Most Malware travels as email attachments.
JANUSMAIL is equipped with a tool that thoroughly checks the attachments:
- Analysis and extraction of email attachments
- Identification of the type of attachments from the extensions: MIME type declared and MIME type identified by analyzing the contents of the files
- Identification of executable files using 60 extensions and 10 MIME types
- Identification of high-risk files through 150 extensions, 30 MIME types and Microsoft Class ID extensions
- Identification of extensions also by literal analysis of the email with specific support of hundreds of anti-avoidance techniques
- Identification of anomalous files, executables or macros contained in the documents Microsoft Office and PDF
- Identification of compressed files that are encrypted and therefore cannot be analyzed
- Identification and analysis of emails included in other emails (nested emails) or replies from other servers (bounced emails)
- Decompression and decoding of attachments in numerous formats

POLICIES

JANUSMAIL includes the ability to create customized policies for filtering incoming and outgoing emails.
Some policies are automatic and concern the addition of known email addresses in Whitelist:
the system recognizes the addresses to which users send emails, and ensures that messages from these addresses are never blocked.
Furthermore, this policy automatically extends to the entire domain to which users send emails,
if the same activates the SPF signature.
These features help eliminate the problem of false positives.
Additional Policies can be entered manually, for example to limit the size attachments, to quarantine suspicious emails and more.

DELAYED MAIL FUNCTION

The questionable emails are kept in a quarantine queue for a predefined time, and then they are re-checked to then be accepted or permanently blocked.
Temporary quarantine allows antivirus and blacklists to update and prevent dangerous emails from being released.

SYSTEM ADMINISTRATIONS

System administrators will have available a graphical web console, simple and intuitive, for administration and mail relay management.

ADMINISTRATION CONSOLE FUNCTIONS

-- Multi-company and multi-domain system
- Authentication integrated with Active Directory or LDAP
- Management of user profiles

- Filter management by user, domain, customer
- Filters by attachment type,
- Filters for incoming / outgoing mail size,
- Creation of whitelists and blacklists

- Sending automatic reports of blocked emails
- Management of access profiles on 3 levels (domain, client, server)
- Statistics in real time on mail traffic

Via A.Gramsci 25
27100, Pavia

PI 016606500187
0382/413825

commerciale@bls.it
www.bls.it

B.L.S. Consulting s.r.l.

100% EMAIL MANAGED

The BLS system uses technologies based on bigdata techniques and parallel processing flows.
Highly performing, these technologies allow JANUSMAIL to accept, analyze and manage all incoming emails, without discarding any a priori and guaranteeing the recoverability of any email received by the user.

MAIL OUTPUT ON DIFFERENT IPS

JANUSMAIL can use multiple IP addresses to send mail, allowing each client / domain to be assigned a specific output IP address, or a pool of addresses.
If a client's address ends up in Blacklist, only the single IP address would be blocked, without compromising the other domains or customers (which would come out via different IP addresses), nor the entire mail server.

OUTPUT E-MAIL CONTROL

One of the most innovative features of JANUSMAIL is the outgoing filter, which counts the emails that are sent by the single box or by the domain per unit of time.
If it detects an abnormal number, the limit of which can be preset, it temporarily stops sending it from the first beyond the limit onwards.

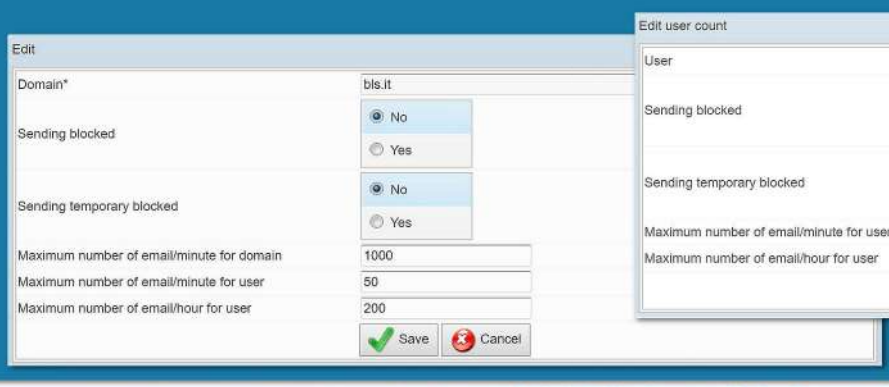
The blocked emails are not deleted but kept in the exit queue, and the system administrator can intervene by deciding whether to allow them to be sent or deleted.

This innovative system allows us to receive very well the risk that a user's inbox is exchanged for spam, for example due to infection by a virus that uses it to send large quantities of actual spam mails, or simply to incorrect behavior by the user.

AUTOMATIC DKIM CONFIGURATION

DKIM is probably the most widespread method for authenticating corporate emails, in order to avoid them being exchanged for spam.
On most systems the generation of public decryption keys is done manually, consuming time.
JANUSMAIL automatically marks the Emails with the DKIM signature, generating the keys to be included in the DNS.
Furthermore, the DKIM signature is generated no longer for Server, but for Domain, making it further secure.

The same prevention applies to the entire Domain.
The system is able to identify both the sending of maximum spam and the sending of slow spam.
In the example, the limit placed on a domain is 1000 emails per minute, and to domain users 50 emails per minute and 200 per hour.



Via A.Gramsci 25
27100, Pavia

PI 016606500187
0382/413825

commerciale@bls.it
www.bls.it

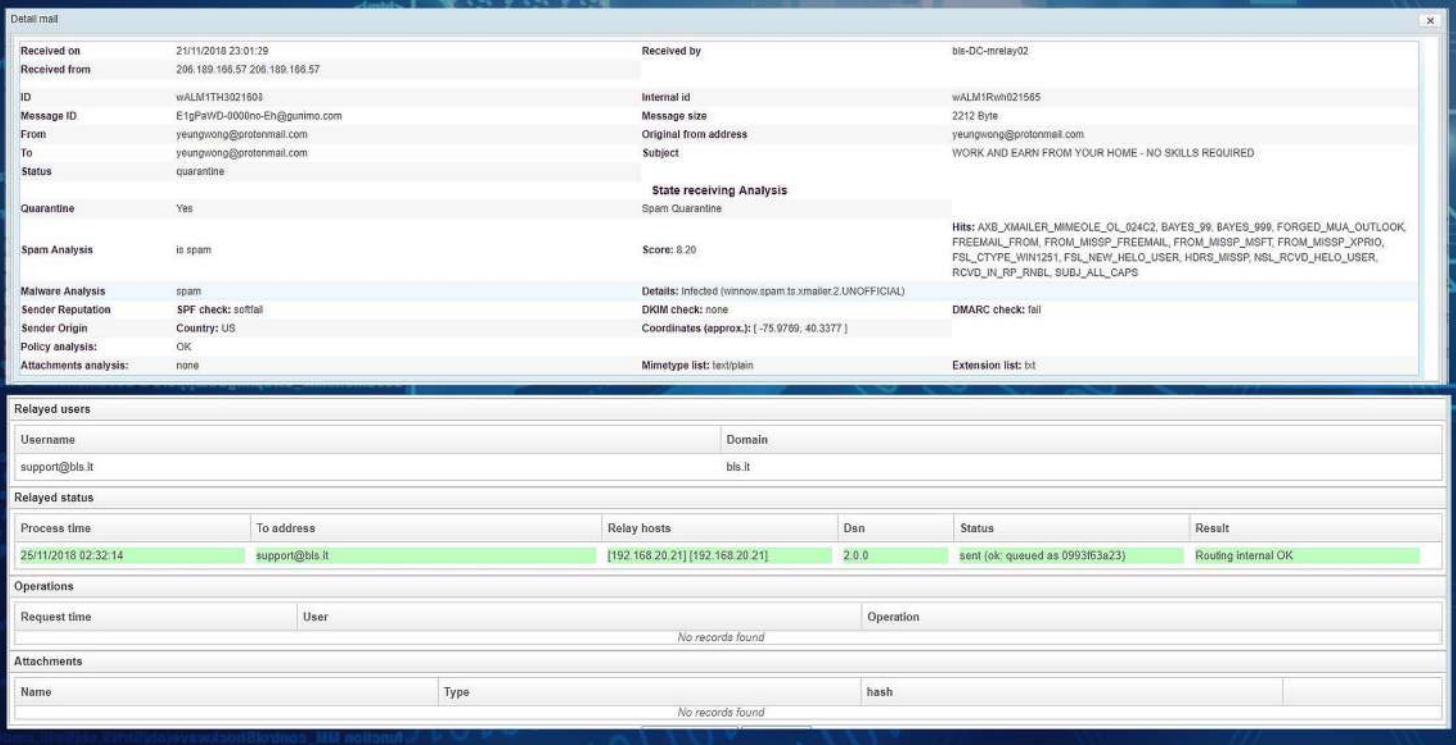
B.L.S. Consulting s.r.l.

USER MANAGEMENT CONSOLE

JANUSMAIL is equipped with a simple and intuitive management console.
The console allows users to see their emails received and sent, sorted in folders depending on the outcome of the various checks.

Users can unblock the mails blocked by the Antispam and report spam that may have passed the checks.

By clicking on each email, the user will have at his disposal a very detailed account of the route he has taken,
of the outcome of each filter and of the operations carried out by the administrators or requested by the users, for example the request release of an email blocked for spam.
The management console also allows the user to check the status of the emails he sent,
and therefore verify that it has been correctly delivered to the recipient's servers.



Via A.Gramsci 25
27100, Pavia

PI 016606500187
0382/413825

commerciale@bls.it
www.bls.it