Cloud Email Firewall

1. Introduction

a. What is Spam?

Spam are messages which are unsolicited or sent from unknown senders. Usually they are sent in large quantities (even massive) and with commercial aims, which damages somehow to the receiver.

b. Economic and social impact of spam in business

The analysis of spam consequences in Organizations are made on the effects arise from them. In many cases, these effects are treated in purely qualitative but not necessarily economic, such as time loss, service mistrust, bandwidth consumption and storage capacity, time need for recovery and restoration of service, etc.

Referring to the economic impact, it is worth to highlight the absence of reliable information or detailed studies that allow citing reliable figures. The precise calculation of the losses caused by spam is not easy, as there are many variables involved in the spam phenomenon, which generates a complex analytical framework.

The costs of time and opportunity loss for companies and those of their individual employees are not the same. However how different of those are depending on wages, productivity, hierarchical dependence, etc. which lead to the need for new estimates of this figure.

Finally we must define the number of affected workers, those who not only use the computer at their jobs, but also make frequent use of email as a tool. This determines that, in the calculations of economic impact, we always talk about estimates based on statistical predictions.

Most studies conclude generically that the bulk of the economic impact of spam is related to:

- ✓ The loss of processing and human time.
- ✓ Investment in new technology infrastructure for a higher bandwidth and increased storage capacities and performance of backup to support this massive of mails.
- ✓ Investment in skilled technicians.
- ✓ Investment in antispam tools and updates.
- ✓ Loss of important information.

c. Spam Policy

The spam problem falls into conflicts of interests. The spammers, on one side, try to make businesses by creating an advertising mechanism very economical and effective, but very questionable from an ethical point of view. On the other side, the end users lose concentration and productivity by having to review a huge amount of mails to find out what is really important.

The problem will not exist only if the Spam business is no longer profitable, or it stops causing losses to companies and individuals. However, in the near future, none of those seem to happen. But, there do certainly exist techniques that reduce the impact:

- ✓ Preventing: Those methods focus on preventing spam from the source. This means solved the problem completely, which can be done in two ways, educating users and anti-spam laws.
- ✓ Reactive: Those methods seek to identify a spam mail once it has entered mail servers. This will only solve part of the problem, because of the consumption of resources, processes and memories.
- ✓ Pre-active: Those methods try to prevent spam even without processing. Try to identify the spammer instead of the Spam mail. In general these techniques are very effective, but must manage a constant monitoring and intervention of systems administrators in order to keep information from getting lost. The techniques mostly used include: Charts Reputation, Fingerprint, Grey listing, etc.

d. Threats and Solutions

At corporate and social level

One of the major concerns is the leaking of company information through Botnets. Is it really so easy for someone to enter other's bank account? Everyone knows some Phishing victims, and the trust in banks has not been changed in general. There are professionals specialized in the eradication of Phishing. And banks are spending large amount of money to solve this problem, but users education is still the best tool against it.
Another problem is the leaking of information. The increase of Zombies machines is huge, and they can be both personal and business computers, being able to copy our information, for example, industrial espionage.

At technical level

Contamination of space: It is able to disable the email service.
Use of resources: it requires more powerful computers and higher bandwidth to process the email.
Security commitments: Spam is used to transmit malware that is used to generate attacks of different features on systems, users and institutions.
Interoperability errors: react in a wrong way to spam with non-standard solutions may degrade your mail, not notice to users, similar to what spam makes.

2. Spamina Firewall for Email

a. Security Solution for Email

Every day 95% of emails received by companies are spam or malware. This situation leads to a drop of companies' productivity. Related with the same Control and Management, there are new requirements that affect the security.
The challenge for IT departments is essentially to ensure maximum availability, while providing full protection against any threats such as Spam, Virus and Phishing.

Our security solution is not only limited to analyze and block these threats listed above, but also retains in Spamina servers all types of harmful files that could threaten companies' security, such as worms, Trojans, Dialers, Jokes ...

The Service is presented in two ways according to different customer needs and criticality of their environments:

Spamina Email Service Firewall, option which applies the Cloud model and acts as external filter.
Spamina Email Firewall, Private cloud option that integrates most recognized hardware platforms with Spamina software, even allow server virtualization. Together they provide an extremely effective and efficient form to protect companies' e-mail accounts.

b. Dynamic multilayer system that combines different filters and protection mechanisms

These filters are continuously tested by Spamina Labs, an internal monitoring and control laboratory in continuous evolution that keeps your email free of threats. They are carefully monitored and modified to achieve an optimum performance in all times.

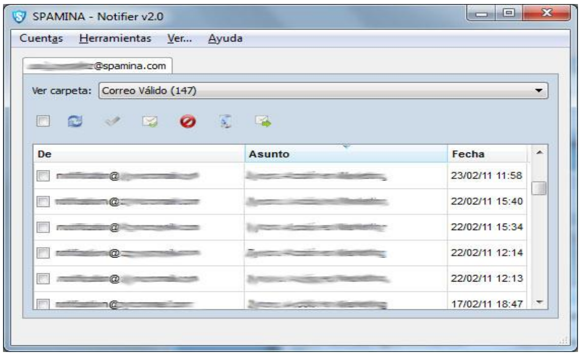
The objective of Spamina is to achieve the best filter that minimizes the time loss in spam for administrators and users by processing only valid emails to end users. Therefore both our own technologies (Spamina Predictive Analytics) and improved standard technologies (RBLs, Bayesian networks, white and black lists, grey listing ...) are applied instantly to our service. And automatically updating is also made to all our customers. To achieve our goal, we work with some of the best antispam technology providers in the world to ensure the maximum effectiveness at all times.

Thanks to the combination of the best technologies, Spamina makes it possible to decrease client e-mail server load, and eliminate any kind of threat so that the server can be dedicated solely to the final mail, which is usually less productive than 5% of total received mail.

c. Control, Management and Global administration

Offering maximum availability for corporate mailboxes and protecting them against threats in their environment is the goal of our security solutions.

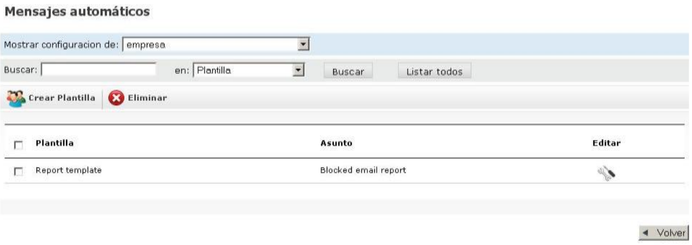
Accessing through administration panels with various available profiles, global administrator (and domain administrator -optional-), can control and view the solution as a whole or each domain separately. It is also possible that end users have access to some of these settings and their respective valid and spam mailboxes through Web or a small Notifier installed on their own computer. These panels are saftly accessible through SSL, sending and receiving mails use TLS automatically whenever servers of the sender and receiver support it.



[redacted]@spamina.com

Ver carpeta: Correo Válido (147)

De	Asunto	Fecha
[redacted]	[redacted]	23/02/11 11:58
[redacted]	[redacted]	22/02/11 15:40
[redacted]	[redacted]	22/02/11 15:34
[redacted]	[redacted]	22/02/11 12:14
[redacted]	[redacted]	22/02/11 12:13
[redacted]	[redacted]	17/02/11 18:47


Mensajes automáticos

Mostrar configuracion de: empresa

Buscar: en: Plantilla

Plantilla	Asunto	Editar
Report template	Blocked email report	

Usuario:
Contraseña:

d) Extensive reporting

The "Dashboard" provides a dynamic view of system status and filtering activity for different periods of time. The graphs show, intuitively, the total volume of emails processed and identified threats, sub-divided into categories of posts and classifications, respectively. In addition summary tables are presented with the same numerical data, both for incoming and outgoing mail. This will offer a summary of:

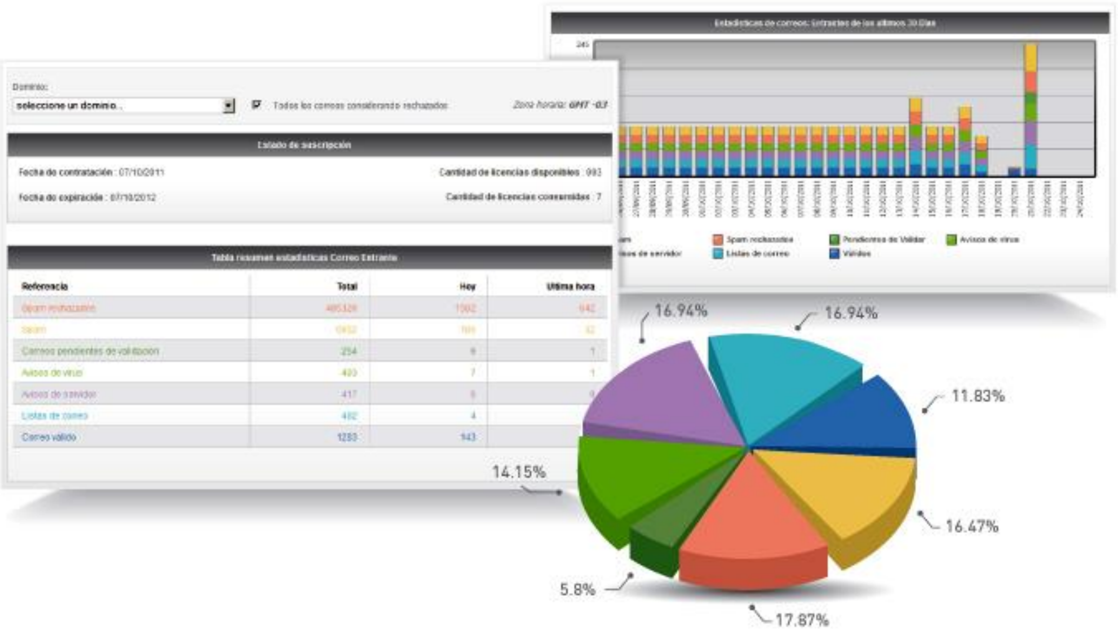
Incoming and outgoing mail.

Classification and quantity of messages received for different periods of time (last 30 days, today and last time).

Subscription status (start date, date of license expiration, number of licenses available and number of licenses consumed).

This version incorporates a reporting engine, available for enterprise and domain administrators, which provides information on filtering for both incoming and outgoing mail. It can be programmed to send different reports, and for each one of them, configure a diverse set of issues, among which may be included:

✓ List of domains on which you want the information
✓ Type of traffic (incoming or outgoing)
✓ Filter categories to be consulted
✓ Frequency (daily, weekly or monthly)
✓ Types of charts desired
✓ Recipients to whom the report will be sent
✓ Decide if the report is enabled or not to be sent during the defined period



Dominio: seleccione un dominio.. ☑ Todos los correos considerando rechazados Zona horaria: GMT -03

Estado de suscripción

Fecha de contratación : 07/10/2011
Cantidad de licencias disponibles : 993
Fecha de expiración : 07/10/2012
Cantidad de licencias consumidas : 7

Tabla resumen estadísticas Correo Entrante

Referencia	Total	Hoy	Ultima hora
Spam rechazado	405328	1002	642
Spam	[illegible]	[illegible]	32
Correos pendientes de validación	254	9	1
Avisos de virus	493	7	1
Avisos de servidor	417	5	0
Listas de correo	482	4	
Correo válido	1283	143	

Cloud Email Firewall comes with a great visual dashboard and with fully customizable reporting.

3. Spamina Technology

Spamina Labs
Internal monitoring and control laboratory that in continuous evolution keeps your mailbox free of threats by researching and making progress to suggest the best techniques in our filters.

Spamina Intelligence Database Updating
Pre-active System with dynamic updates and constant changings, updates Spam filters in real time.

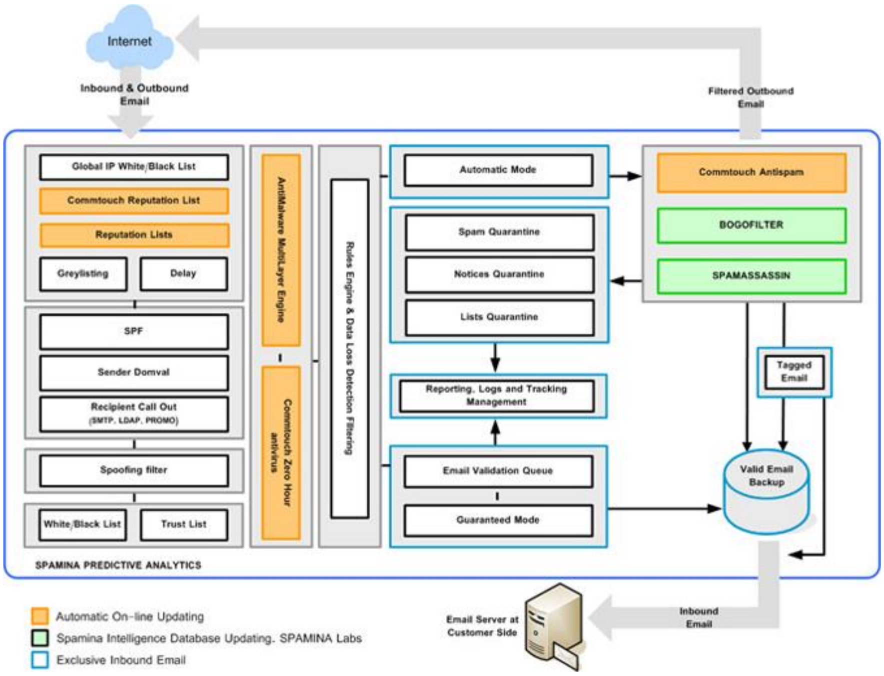
Spamina Predictive Analytics
The entire owned technologies of Spamina Email Firewall Service will make your mailbox a completely secure and manageable tool against any kind of external vulnerability.

The multilayer filter ensures maximum effectiveness, achieving up to 100% protection with the Guaranteed Filter mode. The various filters retain most of spam and process only valid mails.

4. Filtering and SDA Architecture

a) Outline and Filtering Technology

The following diagram shows the outline of the Spamina filtering technology :


Internet
Inbound & Outbound Email
Filtered Outbound Email
Global IP White/Black List
Commtouch Reputation List
Reputation Lists
Greylisting
Delay
SPF
Sender Domval
Recipient Call Out (SMTP, LDAP, PROMO)
Spoofing filter
White/Black List
Trust List
AntiMalware MultiLayer Engine
Commtouch Zero Hour antivirus
Rules Engine & Data Loss Detection Filtering
Automatic Mode
Spam Quarantine
Notices Quarantine
Lists Quarantine
Reporting, Logs and Tracking Management
Email Validation Queue
Guaranteed Mode
Commtouch Antispam
BOGOFILTER
SPAMASSASSIN
Tagged Email
Valid Email Backup
SPAMINA PREDICTIVE ANALYTICS
Automatic On-line Updating
Spamina Intelligence Database Updating. SPAMINA Labs
Exclusive Inbound Email
Email Server at Customer Side
Inbound Email

Spam filtering

White List / Black

Unlike other filtering systems, Spamina can apply IP lists before any other filter. This ensures that the client can receive mails from specific servers although these servers are labeled with bad reputation. There are different levels to implement these lists. The most restrictive one is applied at IP level by company´s administrator from his web panel. In this case, any IP from LB will be rejected or accepted (regardless of other connection filters).

IP's reputation

The second filter layer is for IP and RBLs. It checks the origin server's reputation from studying its historical and actual performance. This layer can categorize emails and eliminate between 80-95% of spam. This process does not only reduce a huge amount of spam but also cut the connection from spammers efficiently even before receiving their email. When spammers notice this rejection, they will take it into account and make following attacks to less protected domains.
Furthermore, in order to avoid false positives, SPAMINA won't delete any email in, at least, 2 of the checked 6 RBLs (sbl.spamhaus.org, xbl.spamhaus.org ,bl.spamcop.net, cbl.abuseat.org, dnsbl.sorbs.net, dnsbl.njabl.org). In case of coincide in less than two, the mail will be marked as spam.

White /Black lists of email address o domain

In order to avoid the false positive, either administrator or user can upload validate email addresses and domains.

Trust Lists

The trust lists are formed automatically with the validate email addresses received regularly by users. These lists are personalized and also generated automatically according to a proper algorithm that SPAMINA guarantees the reliability of the email accounts. Thanks to the trust lists, false positives can be avoided without any user's intervention. From admin panel you can view and eliminate email addresses which have been included for their domain and for each user.

Antivirus Filtering
The virus analysis is applied to all the incoming emails, regardless of whether they are validated or spam.
Currently Spamina applies ClamAV as antivirus by default, but it is possible to make a multilayer filter with other antivirus if this is requested during the service installation. The antivirus is constantly updated automatically. But it is possible to disable it from the administration interface web for all domains or only for some of them.

Greylisting
The emails are categorized according to the probability that they are valid. When the score they receive does not ensure that the source is valid, you can apply the technique of Greylisting which is a temporary error to the sending server. If the server is sending spam, typically will not retry, while if the mail is valid, the server must (if it is properly configured) to retry sending after some time. It is a test that is applied by default during the filtration under certain conditions of connection.

Sender's domain validation
It checks the existence of MX records to sender's domain to guarantee the mail delivery. If it does not exist, they will not be able to receive nor send mails. This test deletes spam sent from nonexistent domains.

Recipient validation
It verifies the existence of a recipient to eliminate spam sent to nonexistent accounts. This check will be applied depending on SMTP registration mode or against LDAP.

Delay
Emails are categorized according to the possibility of being validated or not. If an email receives low score shows that it does not ensure if the source is valid, the greylisting will be applied and it will give a temporarily error to the sender's server. If it is spam server, normally it won't try again; but if the email is validate, its server has the obligation (if it is correctly configured) to re-send it. It is a beginning test that is applied by default during the filtering under certain connection conditions.

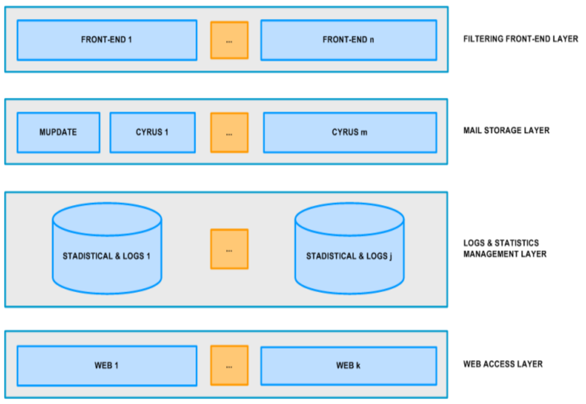
Filtering Rules

The content filtering for inbound mails runs according to the policies defined by the global or domain administrator. There is the possibility to create personalized filters, which run as rules composed of multiple conditions and corresponding performances.

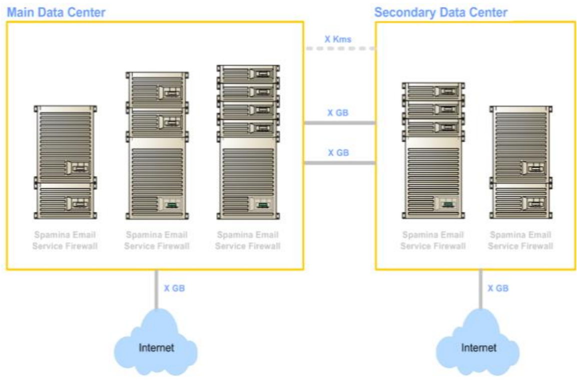
Possible options to create filters are conditions with To, From, To someone in the group LDAP, Subject, Body, Attachment, or emails with certain receiving date.
It is possible to remove attachments from an email, mark an email as SPAM or Valid, move an email to the trash, forward or send a copy to another recipient. In the case of selecting an email with MIME Attachment, filters will evaluate the Mime attachment. The use of "remove attachments" modifies email contents; this will affect those that have been signed using PGP or X.509, making them non-valid.

b. Scalable & Distributed Architecture
Thanks to the fully distributed and scalable architecture of Spamina, different components can be distributed in different layers which are installable on different physical or virtual machines or even distributed in CPD's different locations with high availability.

Scalable Architecture



Distributed Architecture


Main Data Center
Secondary Data Center
X Kms
X GB
X GB
Spamina Email Service Firewall
Spamina Email Service Firewall
Spamina Email Service Firewall
Spamina Email Service Firewall
Spamina Email Service Firewall
X GB
X GB
Internet
Internet

5. Filter Mode

Automatic Filter Mode

This technology is based on Open-Source systems where apply from Bayesian filter to DNS-based exam or external data bases search. In order to guarantee the efficiency, more than 600 rules are applied.

By using our own technology, Spamina Intelligence Database Updating, rules and tests of these two systems are constantly adjusted in order to obtain the best performance against all types of spam. Therefore, without users interfere, these two systems can satisfy the needs, optimize the system's efficiency and avoid false positive at the same time.

Some of the tests are:

"Headers" inspection
The "Headers" contain important information about the email.

Message Analysis
SpamAssassin reads the subject and body of an email by searching keywords or structures that make up a Spam.

Probabilistic / Bayesian analysis
Once initial rules for detection have been set, probabilistic analysis will be performed to determine similarities between new inbound emails and those emails which have already been identified as spam before.

"Hash" list / Email signature
Spam are usually sent to thousands of people at the same time. This can produce an unequivocal "Hash" as their structures are identical in every moment. SpamAssassin check "hashes"list about emails.

Guaranteed Filter Mode
It verifies sender's existence on receiver's White List. If the verification is positive, the mail will be delivered immediately. Otherwise, a message will be sent to the original sender explaining that an anti-spam service is being used by the receiver and the sender must click a link to verify his account.
Once the sender has been validated, his email will be delivered to the destination and all future emails from this address will be accepted.
In case the sender does not process validation, the receiver could validate it manually to avoid losing any emails. SPAMINA follows REC3834 recommendations to prevent the generation of collateral spam.

Quarantine
All those emails which have not been rejected and classified as spam will be delivered directly to a quarantine where the user can perform various actions (delete, move to white list, retrieve…) from administration panels.
It is also possible to keep server´s notices (NDR, NDN, DSN…) or emails received as distribution lists here. This is configurable for each user.
The content of the quarantine can be notified by email to each user daily or weekly according to administrator's configuration.

Outbound Filtering
SPAMINA applies content and antivirus filters to not only inbound emails but also outbound emails. There is also possibility to configure through the administration panel a maximum number of addressees, users, domains o companies, from which sending emails will be forbidden.
Furthermore as part of the outbound filtering, SPAMINA applies a signature to all emails sent through the system. This is SPAMINA Footprinting which allows future recognization to those emails sent by SPAMINA.

6. Cloud Email Firewall

Thanks to the fully distributed and scalable architecture of Spamina, different components can be distributed in different layers which are installable on different physical or virtual machines or even distributed in CPD's different locations with high availability.

Below are the installation formats for customers who have basic or medium needs according to the traffics or availabilities of their mail accounts. As detailed in the chart, Spamina is the same solution, adaptable to all types of companies or needs, regardless of the criticality of their environment.

6.1 Spamina Email Service Firewall

Spamina Email Service Firewall acts as an external filter between the recipient (PC, PDA, BlackBerry or mobile phone) and the e-mail sender. Messages are received and filtered before reaching the user and threat-free mail is delivered, regardless of where the user checks it (in the office, at home, etc.).

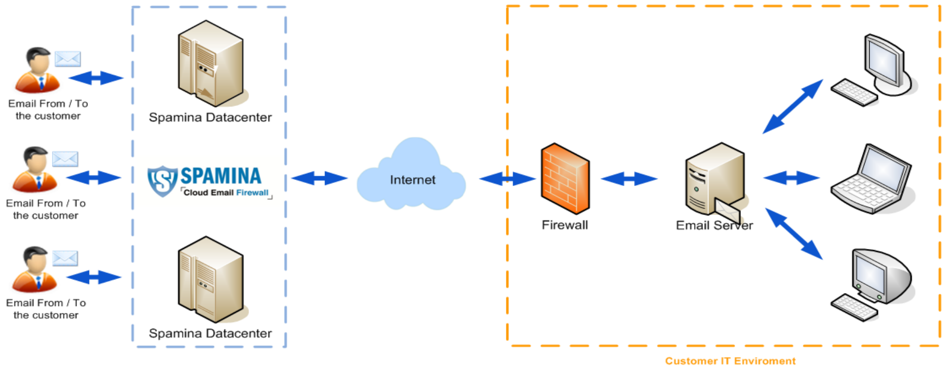
Valid e-mail is sent to a protected mail server and junk mail is kept in our data centre, available for online consultation, where blocked mail can be easily recovered as required.

The multilayer filter ensures maximum efficiency, achieving up to 100% protection with guaranteed filtering mode. Initially, a connection filtering removes most of the spam according to the source. Mails that have passed this first layer are scanned with our multi-layer anti-virus system. Finally, those who have not been rejected nor directly considered valid will have to pass content filtering where queries of DNS and Bayesian networks will be done under Spamina Labs supervision. Outbound mails can also be filtered, ensuring that any attack from the inside can also be controlled.

a. Cloud Mode :

SPAMINA Email Service Firewall efficiently protects companies e-mail accounts and enables an agile administration, even in critical environments. By applying the cloud-computing mode, companies will benefit from a range of benefits that will improve their daily work, both in terms of resources and costs.

- ✓ Own dedicated platform is not required. Outsourced management.
- ✓ Easily scalable. Additional hardware is not required.
- ✓ Mail Relay: Mail Support during 4 days in case of delivery problems in client servers.
- ✓ Mail Backup: Mails are stored during 10 days (15 days in case of Spam) after their delivery.
- ✓ Administration, Management and Control by Administrator and Users.
- ✓ Mail access from mobile through http://mobile.spamina.com.
- ✓ Total accessibility through Webmail: mails available and accessible at all times.
- ✓ Different protection levels: automatic and guaranteed filtering.
- ✓ Multi-domain protection.
- ✓ Filterings are performed in servers of Spamina, never in user's server, PC or mobile device. Total mobility.
- ✓ Bandwidth Optimization by reducing junk mail receiving.
- ✓ Monitored 24x7x365 service with a SLA guarantee of service continuity. 100% mail availability.


Email From / To the customer
Email From / To the customer
Email From / To the customer
Spamina Datacenter
SPAMINA Cloud Email Firewall
Spamina Datacenter
Internet
Firewall
Email Server
Customer IT Enviroment

b. Cloud for MSP's mode :

This cloud mode is designed for ISP's or customers who manage large volumes of data. This means that the product installation is made in physical or virtual layers, which allows load balance between filters (Front-End and Back-End). This architecture provides high scalability.

6.2 Spamina Email Firewall

Spamina is a technological partner of the leading Appliance manufacturers: SUN, IBM and HP. Being an Official Partner guarantees our product's validity of being installed in hardware from any of these manufacturers, and its 100% operation. SPAMINA provides a wide range of options in implementing SPAMINA Email Firewall in the platform that best suits your technological requirements.

All Appliance models from our partners ensure an optimum performance on email protection and enable multi-layer installations that offer various levels of filtering, providing a fully scalable and distributed architecture.

a. Private Cloud mode (Appliance):

Spamina Email Firewall, a solution for private-cloud environment in Appliance format, is available in different models that guarantee an optimal performance in email protection by eliminating spam, viruses and other threats.

- ✓ Dedicated platform.
- ✓ High availability with active-active clustering.
- ✓ Redundancy options (disk, power supply, etc.).
- ✓ Greater capability for configuration. Permit the configuration of quarantine and mail back-up limits.
- ✓ E-mail firewall functions. Definition of rules and configurations.
- ✓ Multi-domain protection.
- ✓ Remote monitoring by the customers.
- ✓ SPAMINA Email Firewall solution with hosting data centre in SPAMINA.
- ✓ Technological support from our partners.
- ✓ Certified by SuperMicro, HP and IBM.

IBM Business Partner   Business Partner hp invent   SUPERMICRO

b. Cloud Mode :

As Spamina is a member of VMware Technology Alliance Partner Program and Citrix Technology Member, our service is also available in virtual mode by using VMware and Citrix technologies. It is a virtual software system that simulates a physical system with characteristics of a determined hardware. When running Spamina Email Firewall in this environment, it provides a similar execution environment as a physical server.

By using virtualization technologies, all the features and effectiveness of SPAMINA Email Firewall can be achieved in your own server, with all the benefits in terms of costs and resource control.

In traditional systems, it is necessary to carry out tasks separately, while in this new approach, the administrator can perform centralized management (maintenance, back-up or contingency plans) of resources, separating the operating system base dedicated to Spamina Email Firewall or other applications that run simultaneously. Moreover, a failure or halt in any virtual executions does not affect others so that its execution is completely safe.

- ✓ Benefits of the Private Cloud solution.
- ✓ Flexibility and speed in including new resources for virtualized servers.
- ✓ Cost reduction in space and consumption.
- ✓ Efficiency and flexibility Increases in resource usage, and therefore, IT cost reduction.
- ✓ Centralized global and simple administration.
- ✓ Manage resources as a group instead of in parts.
- ✓ Improved system cloning and copy processes.
- ✓ Better TCO and ROI.
- ✓ Reduces downtimes.
- ✓ Migrate virtual machines from one physical server to another in hot (without loss of service).
- ✓ Dynamic virtual machine balancing between physical servers in the resource pool, ensuring that each virtual machine is run on the most suitable physical server.
- ✓ Certified by VMware and Citrix Technology Member.

Free Evaluation

Spamina services can be easily and freely evaluated before committing to any subscription period. Just provide us with some simple details via an online sign-up form and we can have a free 15-day trial of any of the services up and running for you within 24 hours. Full reporting services are provided to help you learn what is going on with your email and Web usage and understand all that Spamina has to offer. There is no obligation to subscribe and it is quick and easy to disconnect the service if you don't wish to continue.

Request your evaluation at www.spamina.com

About Spamina

Spamina is the first company to provide a proprietary, integrated Security as a Service solution for cloud-based Web and email security featuring a common Web management and reporting console. Our mission is to provide clients with accessible, easy to understand security services that secure their Internet world and enable them to complete their business in safety and privacy – whether their enterprise is large or small.
Our security services utilize sophisticated, patented, real-time content analysis technologies developed and refined over the last 10 years to ensure maximum threat protection. Our approach to how we deliver this technology and enable clients to access, manage and report on their email and Web usage is to provide simple, easy to use services. This is key to ensuring that our clients understand and receive the maximum returns and benefits of Spamina SaaS.

Contact Spamina

For further information contact us at:
www.spamina.com