Cyberoam
Unified Threat Management

Cyberoam Anti Spam Implementation Guide

Version 10

Document version 10.00.0302 - 1.0-27/07/2010

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com , www.cyberoam.com

Contents

Preface

Welcome to Cyberoam's - User guide.

Cyberoam Unified Threat Management appliances offer identity-based comprehensive security to organizations against blended threats - worms, viruses, malware, data loss, identity theft; threats over applications viz. Instant Messengers; threats over secure protocols viz. HTTPS; and more. They also offer wireless security (WLAN) and 3G wireless broadband and analog modem support can be used as either Active or Backup WAN connection for business continuity.

Cyberoam integrates features like stateful inspection firewall, VPN, Gateway Anti-Virus and Anti-Spyware, Gateway Anti-Spam, Intrusion Prevention System, Content & Application Filtering, Data Leakage Prevention, IM Management and Control, Layer 7 visibility, Bandwidth Management, Multiple Link Management, Comprehensive Reporting over a single platform.

Cyberoam has enhanced security by adding an 8th layer (User Identity) to the protocol stack. Advanced inspection provides L8 user-identity and L7 application detail in classifying traffic, enabling Administrators to apply access and bandwidth policies far beyond the controls that traditional UTMs support. It thus offers security to organizations across layer 2 - layer 8, without compromising productivity and connectivity.

Cyberoam UTM appliances accelerate unified security by enabling single-point control of all its security features through a Web 2.0-based GUI. An extensible architecture and an 'IPv6 Ready' Gold logo provide Cyberoam the readiness to deliver on future security requirements.

Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

Default Web Admin Console username is 'cyberoam' and password is 'cyber'

Cyberoam recommends that you change the default password immediately after installation to avoid unauthorized access.

About this Guide

This Guide provides information on how to configure Cyberoam Anti Spam solution and helps you manage and customize Cyberoam to meet your organization's various requirements including restriction of spam mails, creation of groups and archiving emails to control web as well as application access.

Typographic Conventions

Material in this manual is presented in text, screen displays, or command-line notation.

Item	Convention	Example
Server		Machine where Cyberoam Software - Server component is installed
Client		Machine where Cyberoam Software - Client component is installed
User		The end user
Username		Username uniquely identifies the user of the system
Part titles	Bold and shaded font typefaces	Report
Topic titles	Shaded font typefaces	Introduction
Subtitles	Bold & Black typefaces	Notation conventions
Navigation link	Bold typeface	**System → Administration → Appliance Access** it means, to open the required page click on System then on Administration and finally click Appliance Access
Name of a particular parameter / field / command button text	Lowercase italic type	Enter policy name, replace policy name with the specific name of a policy Or Click Name to select where Name denotes command button text which is to be clicked
Cross references	Hyperlink in different color	refer to Customizing User database Clicking on the link will open the particular topic
Notes & points to remember	Bold typeface between the black borders	**Note**
Prerequisites	Bold typefaces between the black borders	Prerequisite Prerequisite details

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
eLitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-26400707
Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit www.cyberoam.com for the regional and latest contact information.

Overview

Welcome to Cyberoam's – Anti Spam User guide.

Cyberoam is an Identity-based UTM Appliance. Cyberoam's solution is purpose-built to meet the security needs of corporate, government organizations, and educational institutions.

Cyberoam's perfect blend of best-of-breed solutions includes User based Firewall, Content filtering, Anti Virus, Anti Spam, Intrusion Prevention System (IPS), and VPN(IPSec and SSL).

Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

Cyberoam Anti Spam as a part of unified solution along with Anti Virus and IPS (Intrusion Prevention System) provides real time virus and spam scanning.

Anti Spam module is an add-on module which needs to be subscribed before use.

Spam

Spam refers to electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail.

Spamming is to indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. In other words, it is an inappropriate attempt to use a mailing list, or other networked communications facility as a broadcast medium by sending the same message to a large number of people who did not ask for it.

In addition to being a nuisance, it also eats up a lot of network bandwidth. Because the Internet is a public network, little can be done to prevent spam, just as it is impossible to prevent junk mail. However, the use of software filters in e-mail programs can be used to remove most spam sent through e-mail to certain extent.

With the number of computer users growing and the exchange of information via the Internet and email increases in volume, spamming has become an almost everyday occurrence. Apart from network bandwidth, it also affects the employees productive as deletion of such mails is a huge task. Anti spam protection is therefore a priority for anyone who uses a computer.

Cyberoam Gateway Anti Spam

Cyberoam Gateway Anti Virus provides a powerful tool for scanning and detecting infection. Cyberoam Anti Spam as a part of unified solution along with Anti Virus and IPS (Intrusion Prevention System), provides real time virus scanning that protects all network nodes – workstations, files servers, mail system from known and unknown attacks by worms and viruses, Trojans, spyware, adware, spam, hackers and all other cyber threats.

Cyberoam detects spam mails based on:

- RBL (Realtime Blackhole List)
- Mass distribution pattern using **RPD (Recurrent Pattern Detection) technology** for which Gateway Anti Spam module subscription is required. RPD technology responsible for proactively probing the Internet to gather information about massive spam outbreaks from the time they are launched. This technology is used to identify recurrent patterns that characterize massive spam outbreaks.

Cyberoam Gateway Anti Spam provides powerful tools for scanning and detecting spam in the incoming e-mail traffic. Cyberoam Gateway Anti Spam inspects all incoming emails - SMTP, POP3 and IMAP traffic - before the messages are delivered to the receiver's mail box. If spam is detected, depending on the policy and rules set, emails are processed and delivered to the recipient unaltered, reject and generate a notification on the message rejection, add or change subject or change the receiver.

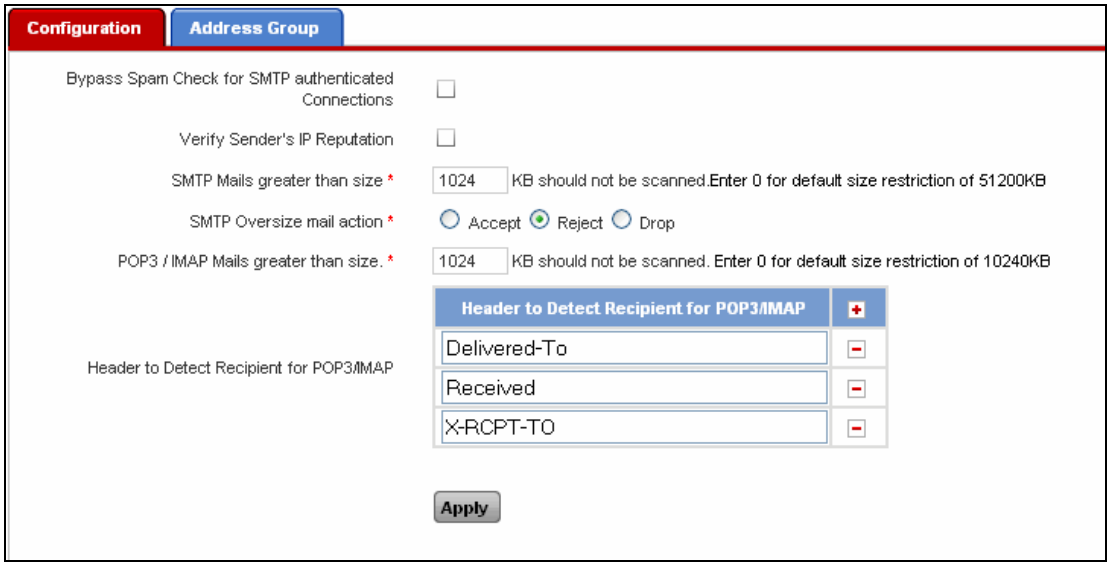
Cyberoam Gateway Anti Spam is fully compatible with all the mail systems and therefore can be easily integrated into the existing network.

Cyberoam Anti Spam allows to:

- Scan email messages for spamming by protocols namely SMTP, POP3, IMAP
- Monitor and proactively detect recurrent patterns in spam mails and combat multi-format – text, images, HTML etc. and multi-language threats
- Monitor mails received from Domain/IP address
- Detect spam mails using RBLs. If Anti Spam module is not subscribed, Cyberoam will detect spam mails based on RBL only and not on recurrent patterns in mails.
- Accept/Reject messages based on message size and message header
- Customize protection of incoming and outgoing e-mail messages by defining scan policies
- Set different actions for SMTP, POP and IMAP spam mails
- Configure action for individual email address
- Notify receivers about spam messages

Configuration

Configure restrictions on mails from **Anti Spam → Configuration → Configuration**.



Screen – Configure Parameters

Screen Elements	Description
Bypass Spam Check for SMTP Authenticated connections	Click "Bypass Spam check for SMTP authenticated Connections" to enforce RBL and RPD based spam checking. If enabled, SMTP authenticated connections are bypassed from RBL and RPD based spam checking. By default, it is enabled.
Verify Sender's IP Reputation	Enable IP reputation, if you want to verify the reputation of the sender IP address. Cyberoam dynamically checks the sender IP address and denies SMTP connection if IP address is found to be responsible for sending spam mails or malicious contents. If both "Bypass Spam check for SMTP authenticated Connections" and "Verify Sender's IP reputation" are enabled, for the authenticated connections, spam scanning based on RBL and RPD will be given the precedence.
SMTP Mails greater than size	Specify maximum size (in KB) of the file to be scanned. Files exceeding this size received through SMTP will not be scanned. Specify 0 for default size restriction of 51200 KB i.e. files exceeding 51200 KB will not be scanned if 0 is configured. **Note** For Cyberoam CR15i models: Specify 0 for default size restriction of 1024 KB i.e. files exceeding 1024 KB will not be scanned if 0 is configured.

SMTP Oversize mail action	Specify the action to be taken on oversize files i.e. Accept, Reject and Drop. If 'Accept' action is specified, all the oversize mails will be forwarded to the recipient without scanning.
POP3/IMAP Mails greater than size	Specify maximum size (in KB) of the file to be scanned. Files exceeding this size received through POP/IMAP will not be scanned and forwarded to the recipient without scanning. Specify 0 for default size restriction of 10240 KB i.e. files exceeding 10240 KB will not be scanned if 0 is configured. **Note** For Cyberoam CR15i models: Specify 0 for default size restriction of 1024 KB i.e. files exceeding 1024 KB will not be scanned if 0 is configured.
Header to detect Recipient for POP3/IMAP	Specify Header value to detect recipient for POP3/IMAP. Click Add icon to add headers and Remove icon to delete the header which is used for detecting the recipient's address.

Table – Configure Parameters screen elements

Address Group

Scanning rule can be defined for individual or group of

- Email address
- Network or IP address
- RBL (Real time black hole List) (applicable only for the spam mails)

Address group is the group of email addresses, IP addresses, or RBLs. Whenever the policy is applied to the address group, policy is applied to all the addresses included in the group.

RBL is a list of IP addresses whose owners refuse to stop the proliferation of spam i.e. are responsible for spam or are hijacked for spam relay. This IP addresses might also be used for spreading virus.

Cyberoam will check each RBL for the connecting IP address. If the IP address matches to the one on the list then the specified action in policy is taken.

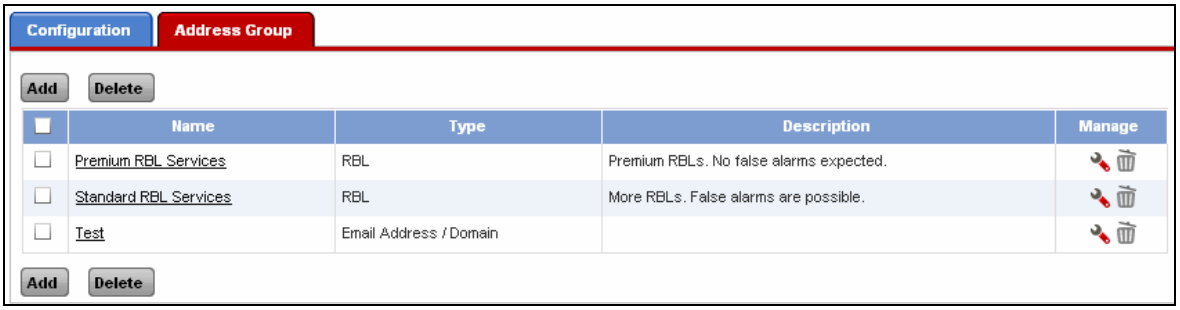
To manage address groups, go to **Anti Spam → Configuration → Address Group**.

- Add
- View
- Edit – Click the Edit icon in the Manage column against the Address Group to be modified. Edit Address Group pop-up window is displayed which has the same parameter as the Add Address Group window. Alternately, Click on the Address Group Name to open the Edit Address Group window.

- Delete – Click the Delete icon in the Manage column against an Address Group to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Address Group. To delete multiple Address Groups, select them and click the Delete button.

Manage Address Group

To manage address groups, go to **Anti Spam → Configuration → Address Group**.



Screen – Manage Address Group

Screen Elements	Description
Add Button	Add a new Address Group
Name	Name of the Address Group
Type	Type of Group: RBL, IP Address, Email Address/Domain
Description	Address Group Description
Edit Icon	Edit the Address Group
Delete Button	Delete the Address Group Alternately, click the Delete icon against the address group to be deleted.

Table – Manage Address Group screen elements

Address Group Parameters

To add or edit an address group, go to **Anti Spam → Configuration → Address Group**. Click the Add button to add an address group. To update the details, click on the Address Group or Edit icon in the Manage column against the address group to be modified.

Screen – Add Address Group

Screen Elements	Description
Name	Name to identify the Group
Group Type	Specify the Group Type. **Available options**: • **RBL** - RBL is a list of IP addresses whose owners refuse to stop the proliferation of spam i.e. are responsible for spam or are hijacked for spam relay. Cyberoam will check each RBL for the connecting IP address. If the IP address matches to the one on the list then the specified action in policy is taken. • **IP address** - Specify IP address or IP range to be added to the Address Group. • **Email address** - Specify Email Address or Domain Name to be added to the Address Group. Use + to add value to the list and − to delete value to the list
Description	Specify Address Group Description

Table – Add Address Group screen elements

Email Archiver

If you want Administrator or any other person in the organization to know about incoming mails into the organization, you can specify email address to which you want to forward the copy of such mails.

By using Email Archiver, the administrator can archive almost all the emails coming into the organization and thereby keep a close watch over data leakage. Emails of a specific recipient or a group of recipients can be archived using Email Archiver. Create multiple archivers to send a copy of emails to more than one administrator.

Cyberoam can archive all emails intended to recipients by creating new Email Archivers from **Anti**

Spam → Configuration → Email Archiver. You can:

- Add
- View
- Edit – Click the Edit icon in the Manage column against the Rule to be modified. Edit Email Archiver window is displayed that has the same parameters as the Add Email Archiver window.
- Search – Click the Search icon in the Recipient column to search for specific recipients. Address can be searched on the following criteria: is, is not, contains, does not contain. A pop-up window is displayed that has filter conditions for search. Click OK to get the search results and Clear button to clear the results.

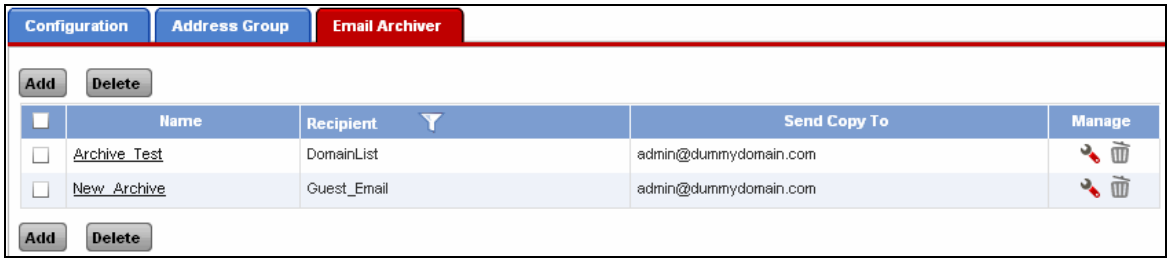
Screen – Search Recipient

Search Criteria	Search Results
is	All the Recipients that exactly match with the string specified in the criteria. For example, if the search string is Test, only recipients with the name exactly matching "Test" are displayed.
is not	All the Recipients that do not match with the string specified in the criteria. For example, if the search string is Test, all recipients except with the name exactly matching "Test" are displayed.
contains	All the Recipients that contain the string specified in the criteria. For example, if the search string is Test, all the recipients containing the string "Test" are displayed.
does not contain	All the Recipients that do not contain the string specified in the criteria. For example, if the search string is Test, all the recipients not containing the string "Test" are displayed.

Table – Search Recipient screen elements

- Delete – Click the Delete icon in the Manage column against Email Archiver to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Email Archiver. To delete multiple Email Archivers, select them and click the Delete button.

View Email Archives



Screen – Manage Email Archivers

Screen Elements	Description
Name	Email Archiver name.
Recipient	Email address of the recipient whose emails are archived.
Send Copy To	Email address to which the email copy is sent. This option can be applied to SMTP protocol only.
Edit Icon	Edit the email archiver
Delete Button	Delete the email archiver Alternately, click the Delete icon against the email archiver to be deleted.

Table – Manage Email Archivers screen elements

Add Email Archiver

To add or edit Email Archiver, go to **Anti Spam → Configuration → Email Archiver**. Click the Add button to add an Email Archiver. To update the details, click on the Email Archiver or Edit icon in the Manage column against the Archivers you want to modify.

Screen – Add Email Archiver

Screen Elements	Description
Name	Specify the name for the Email Archiver.
Recipient	Select Email address of the recipient whose emails are to be archived.

	 You can also add a new email address or domain from the Email Archiver page itself.
Send Copy of email to	Specify email address to which the email copy is to be sent. This option can be applied to SMTP protocol only.

Table – Add Email Archiver screen elements

Spam Rules

As soon as you subscribe Cyberoam Gateway Anti Spam, Spam Rules can be configured for particular sender and recipients.

Spam Rule defines what action is to be taken if the mail is identified as a spam and to which email address the copy of mail is to be sent. These rules can be applied directly to Email addresses now and thus, traffic can be directly scanned for Spam mails.

To reduce the risk of losing the legitimate messages, Spam quarantine repository - a storage location, provides administrators a way to automatically quarantine and remediate messages that are identified as spam.

This will help in managing spam and probable spam quarantined mails and you can take appropriate actions on such mails.

Detection of spam attributes

Cyberoam uses content filtering and three RBLs - Realtime Blackhole Lists – to check for the spam attributes in SMTP as well as POP3/IMAP mails:

- Premium
- Standard

RBL is a list of IP addresses whose owners refuse to stop the proliferation of spam i.e. are responsible for spam or are hijacked for spam relay.

Cyberoam will check each RBL for the connecting IP address. If the IP address matches to the one on the list then the specified action in policy is taken.

To manage spam rules, go to **Anti Spam → Spam Rules → Spam Rules**. You can:

- Add
- View
- Edit – Click the Edit icon in the Manage column against the Spam Rule to be modified. Edit Spam Rule window is displayed that has the same parameters as the Add Spam Rule window.
- Search – Click the Search icon in the Sender and Recipient columns to search for specific senders and recipients. Address can be searched on the following criteria: is, is not, contains, does not contain. A pop-up window is displayed that has filter conditions for search. Click OK to get the search results and Clear button to clear the results.

Screen – Search Sender/Receiver

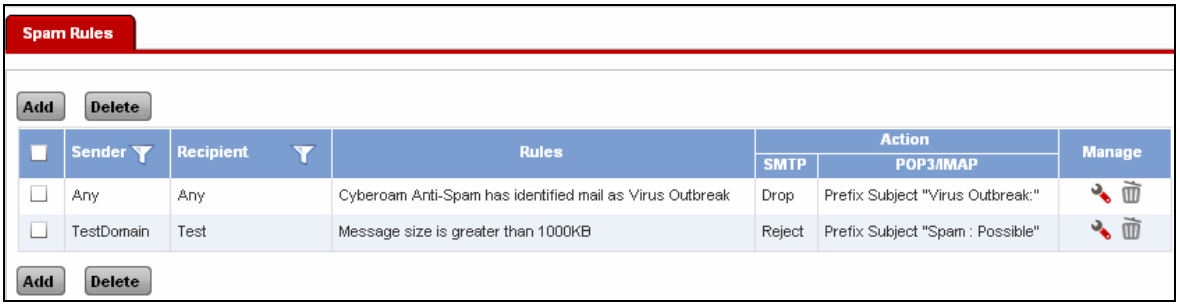
Search Criteria	Search Results
is	All the Sender or Recipient that exactly match with the string specified in the criteria. For example, if the search string is Test, only senders/recipients with the name exactly matching "Test" are displayed.
is not	All the Sender or Recipient that do not match with the string specified in the criteria. For example, if the search string is Test, all senders/recipients except with the name exactly matching "Test" are displayed.
contains	All the Sender or Recipient that contain the string specified in the criteria. For example, if the search string is Test, all the senders/recipients containing the string "Test" are displayed.
does not contain	All the Sender or Recipient that do not contain the string specified in the criteria. For example, if the search string is Test, all the senders/recipients not containing the string "Test" are displayed.

Table – Search Sender/Receiver screen elements

- Delete – Click the Delete icon in the Manage column against a Spam Rule to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Spam Rule. To delete multiple Spam Rules, select them and click the Delete button.

Manage Spam Rules

To manage spam rules, go to **Anti Spam → Spam Rules → Spam Rules**.



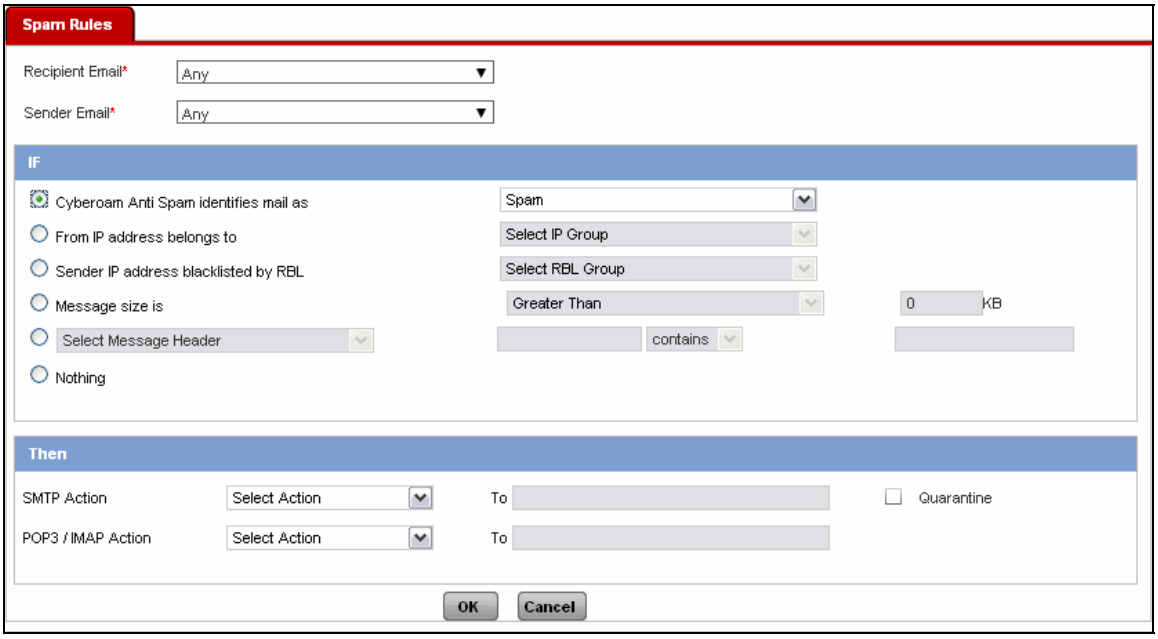
Screen – Manage Spam Rules

Screen Elements	Description
Add button	Add a new Spam Rule
Sender	Sender Email ID
Recipient	Recipient Email ID
Rules	Conditional Rule for restricting spam mails.
Action	
SMTP	Conditions applied for the SMTP mails.
POP3/IMAP	Conditions applied for the POP3 mails.
Edit Icon	Edit the Spam Rule
Delete Button	Delete the Spam Rule Alternately, click the Delete icon against the spam rule to be deleted.

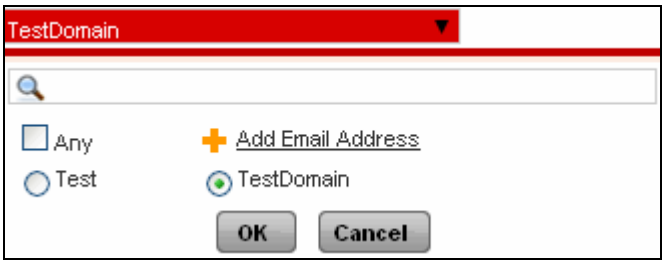
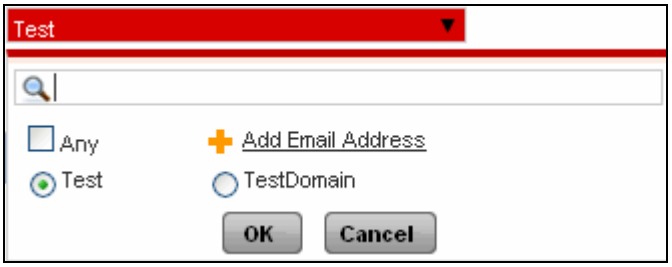
Table – Manage Spam Rules screen elements

Spam Rule Parameters

To add or edit a spam rule, go to **Anti Spam → Spam Rules → Spam Rules**. Click the Add button to add a spam rule. To update the rules, click on the Spam Rule or Edit icon in the Manage column against the rule to be modified.



Screen – Add Spam Rule

Screen Elements	Description
Recipient Email	Select Recipient Email Address. You can also add a list of Email address using 'Add Email Address' link. 
Sender Email	Select Sender Email Address. You can also add a list of Email address using 'Add Email Address' link. 
IF Conditions	
When Cyberoam Anti Spam identifies Mail as "SPAM"	Cyberoam accepts and delivers the mail to the intended receiver but only after adding a prefix 'SPAM' to the original subject of the mail. You will be able to define the action but will be applicable only if Anti Spam module is subscribed. Original subject: 'This is a test' Receiver will receive the mail with subject line as: 'SPAM: This is a test'

	You can customize the subject in such a way that the receiver knows that the mail is a spam mail. To specify the contents to be prefixed to the existing subject line, select 'Prefix Subject' as action. You can set different actions for SMTP and POP mails.
When Cyberoam Anti Spam identifies Mail as "PROBABLE SPAM"	Cyberoam accepts and delivers the mail to the intended receiver but after adding a prefix 'PROBABLE SPAM' to the original subject of the mail. You will be able to define the action but will be applicable only if AntiSpam module is subscribed. Original subject: 'This is a test' Receiver will receive the mail with subject line as: 'PROBABLE SPAM: This is a test' You can customize the subject in such a way that the receiver knows that the mail is a spam mail. To specify the contents to be prefixed to the existing subject line, select 'Prefix Subject' as action. You can set different actions for SMTP and POP mails.
When Cyberoam Anti Spam identifies Mail as "VIRUS OUTBREAK"	Cyberoam accepts and delivers the mail to the intended receiver but only after adding a prefix 'SPAM' to the original subject of the mail. You will be able to define the action but will be applicable only if AntiSpam module is subscribed. Receiver will receive the mail with subject line as: 'SPAM: This is a test' You can customize the subject in such a way that the receiver knows that the mail is a spam mail. To specify the contents to be prefixed to the existing subject line, select 'Prefix Subject' as action. You can set different actions for SMTP and POP mails.
When Cyberoam Anti Spam identifies Mail as "PROBABALE VIRUS OUTBREAK"	Cyberoam accepts and delivers the mail to the intended receiver but only after adding a prefix 'SPAM' to the original subject of the mail. You will be able to define the action but will be applicable only if AntiSpam module is subscribed. Receiver will receive the mail with subject line as: 'SPAM: This is a test' You can customize the subject in such a way that the receiver knows that the mail is a spam mail. To specify the contents to be prefixed to the existing subject line, select 'Prefix Subject' as action. You can set different actions for SMTP and POP mails.
IP Address	Specified action will be taken if the mail sender IP address matches the specified IP address. You can set different actions for SMTP and POP mails.
Sender IP Address Blacklisted by RBL	Specified action will be taken if the sender is listed in the specified RBL Group. You can set different actions for SMTP and POP mails.

Message Size	Specified action will be taken if the mail size matches the specified size. You can set different actions for SMTP and POP mails.
Message Header	Specified action will be taken if the message header contains the specified text. You can set different actions for SMTP and POP mails. You can scan message header for spam in: Subject – Specified action will be taken if the header contains the matching subject. From - Specified action will be taken if the header contains the matching text in the From address. To - Specified action will be taken if the header contains the matching text in the To address. Others – Specified action will be taken if the matching text is found in the headers
Nothing	Select 'Nothing' when you want to create a rule between specific sender and recipient without any conditions. You can set actions for SMTP and POP3/IMAP mails only on the basis of sender and recipient.

Table – Add Spam Rule screen elements

Following actions can be taken on the mail identified as the SPAM, Probable SPAM, VIRUS OUTBREAK or Probable VIRUS OUTBREAK.

Protocol	Action	Meaning
SMTP	Reject	Mail is rejected and rejection notification is send to the mail sender
SMTP	Drop	Mail is rejected but rejection notification is not send to the mail sender
SMTP, POP3	Accept	Mail is accepted and delivered to the intended receiver
SMTP	Change Recipient	Mail is accepted but is not delivered to the receiver for whom the message was originally send. Mail is send to the receiver specified in the spam policy
SMTP, POP3	Prefix Subject	Mail is accepted and delivered to the intended receiver but after tagging the subject line. Tagging content is specified in spam policy. You can customize subject tagging in such a way that the receiver knows that the mail is a spam mail. For Example Contents to be prefixed to the original subject: 'Spam notification from Cyberoam – ' Original subject: 'This is a test' Receiver will receive mail with subject line as: 'Spam notification from Cyberoam - This is a test'

SMTP	Quarantine	Mail is quarantined and can be viewed or downloaded from the quarantine area.

Table – Manage Actions screen elements

Quarantine

Spam digest is an email and contains a list of quarantined spam messages filtered by Cyberoam and held in the user quarantine area. If configured, Cyberoam mails the spam digest as per the configured frequency to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action.

Note

Entire Quarantine menu is not available for Cyberoam CR15i models.

Spam Digest Settings

Digest service can be configured globally for all the users or for individual users. Cyberoam mails the spam digest as per the configured frequency to the user.

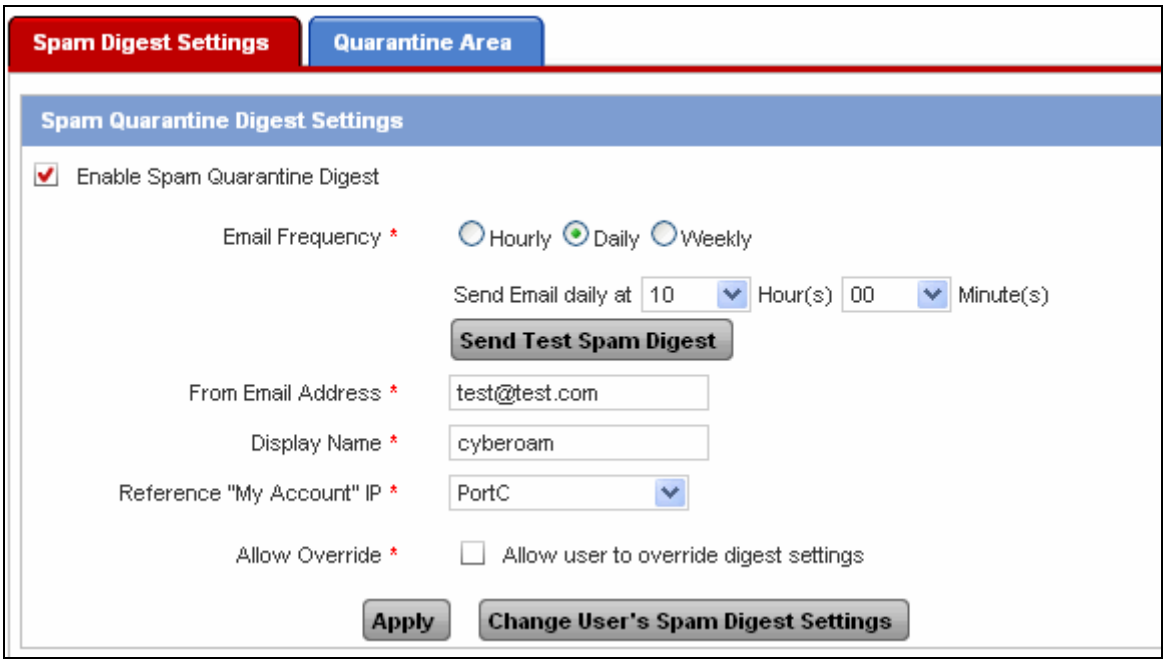
The Spam Digest provides following information for each quarantined message:

- Date and time: Date and time when message was received
- Sender: Email address of the sender
- Recipient: Email address of the receiver
- Subject: Subject of the message

To manage spam rules, go to **Anti Spam → Quarantine → Spam Digest Settings**. You can:

- Configure
- Change User's Spam Digest Settings

Configure Spam Digest



Screen – Spam Digest Settings

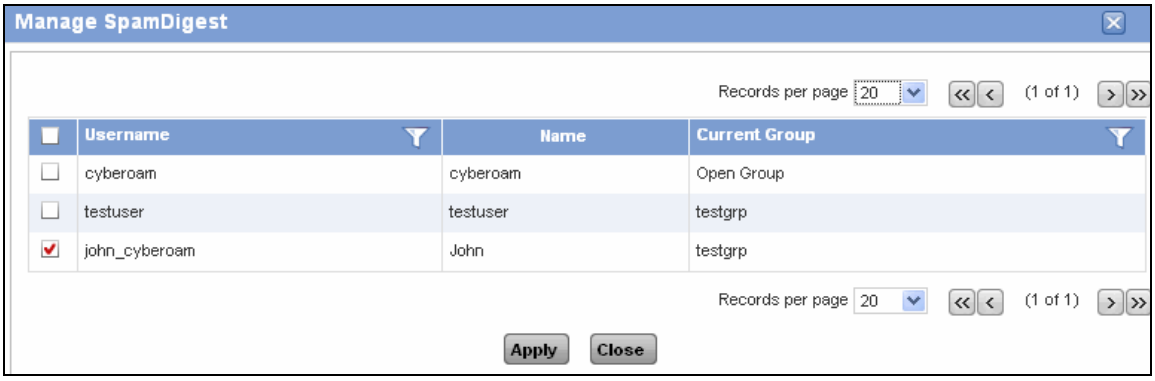
Screen Elements	Description
Enable Spam Quarantine Digest	Enable Spam Quarantine Digest to configure digest service for all the users.
Email Frequency	Specify the spam digest mail frequency. Digest can be mailed every hour, every day at configured time or every week on the configured day and time. Click “Send Test Spam Digest” and specify the email address to send the test spam digest mail. 
From Email Address	Specify email address from which the mail should be sent. Digest mail will be send from the configured mail address.
Display Name	Specify mail sender name. Digest mail will be send with the configured name.
Reference “My Account IP”	Select Interface/Port IP from the ‘Reference “MyAccount” IP’ dropdown list. User My Account link in Digest mail will point to this IP address. User can click the link to access his quarantined messages and take the required action. The users not falling under the specified Interface will have to access the quarantine mail directly from their MyAccount.

Allow Override	Enable “Allow user to override digest setting”, if you want each user to override the digest setting i.e. user can disable the digest service so that they do not receive the spam digest.
Change User’s Spam Digest Settings	Click “Change User’s Spam Digest Settings” button to change the digest setting of the individual users. It allows to select group and update the spam digest setting of group members.

Table – Spam Digest screen elements

Change User’s Spam Digest Settings

Click “Change User’s Spam Digest Settings” button to change the digest settings of the individual users. It opens a new page which allows you to search groups and users for updating the spam digest settings of group members.



Screen – Change User’s Spam Digest Settings

You can individually search for user and user groups.

- Search – Click the Search icon in the Username and Current Group columns to search for specific users and groups. Users and Groups can be searched on the following criteria: is, is not, contains, does not contain. A pop-up window is displayed that has filter conditions for search. Click OK to get the search results and Clear button to clear the results.

Screen – Search Username

Screen – Search Current Group

Search Criteria	Search Results
is	All the users or groups that exactly match with the string specified in the criteria. For example, if the search string is Test, only users/groups with the name exactly matching “Test” are displayed.
is not	All the users or groups that do not match with the string specified in the criteria. For example, if the search string is Test, all users/groups except with the name exactly matching “Test” are displayed.
contains	All the users or groups that contain the string specified in the criteria. For example, if the search string is Test, all the users/groups containing the string “Test” are displayed.
does not contain	All the users or groups that do not contain the string specified in the criteria. For example, if the search string is Test, all the users/groups not containing the string “Test” are displayed.

Table – Search Username/Group screen elements

Select the checkbox  against the user to enable the Spam Digest. If enabled, configured spam digest settings are applicable for the user.

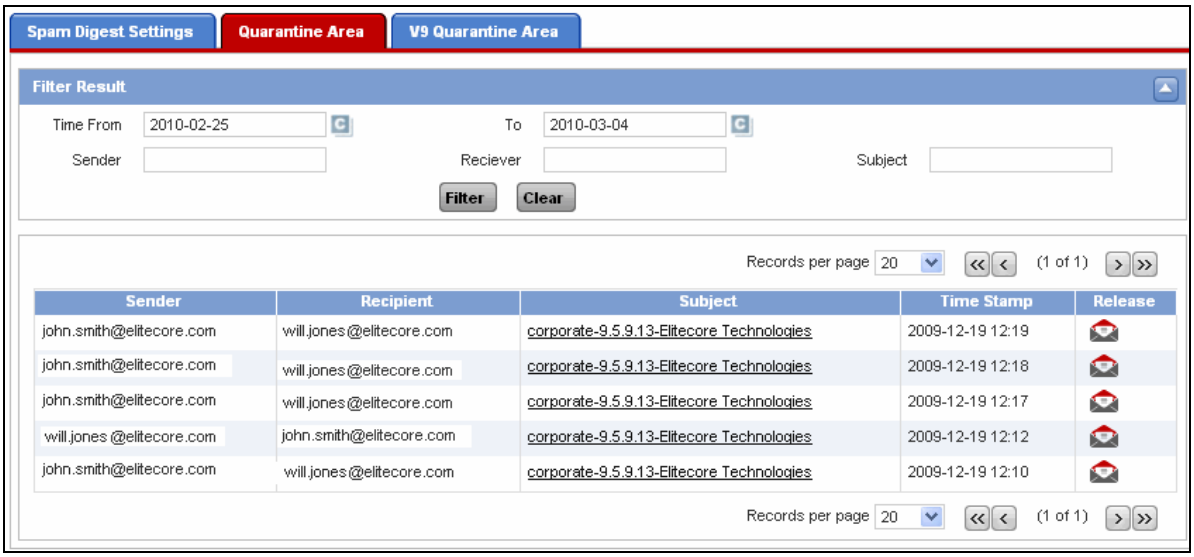
Quarantine Area

Under Quarantine Area, Quarantined mails can be searched based on sender email address, receiver email address, and subject.

Cyberoam reserves 5GB for Quarantine area. To maintain the total size of Quarantine area, Cyberoam removes older mails once the repository is filled by 80% i.e. once the repository level crosses 4GB, Cyberoam automatically deletes the oldest quarantined mails.

Use ‘Filter Result’ section to search for mails from the list of Quarantined Mails. To view and release the quarantined mails go to, **Anti Spam → Quarantine → Quarantine Area**.

Manage Quarantined Mails



Screen – Manage Quarantine Mails

Screen Elements	Description
Sender	Sender of the Mail
Recipient	Recipient of the Mail
Subject	Mail Subject
Time Stamp	Timestamp when the mail was received.
Release Icon	Click on the Release Icon to move the mails from Quarantine area to recipient's inbox.

Table –Manage Quarantine Mails screen elements

Release Quarantined Spam Mails

Either Administrator or user himself can release the quarantined spam mails. Administrator can release the quarantined spam mails from Quarantine area while user can release from his 'My Account'. Released quarantined spam mails are delivered to the intended recipient's inbox.

Administrator can access Spam Quarantine area from **Anti Spam → Quarantine → Quarantine Area**, while user can logon to My Account and access Spam Quarantine area from **Quarantine Mails → Spam → Spam Quarantine Area**.

If Spam Digest is configured, user will be mailed Digest everyday which consists of all the quarantined spam mails.

V 9 Quarantine Area

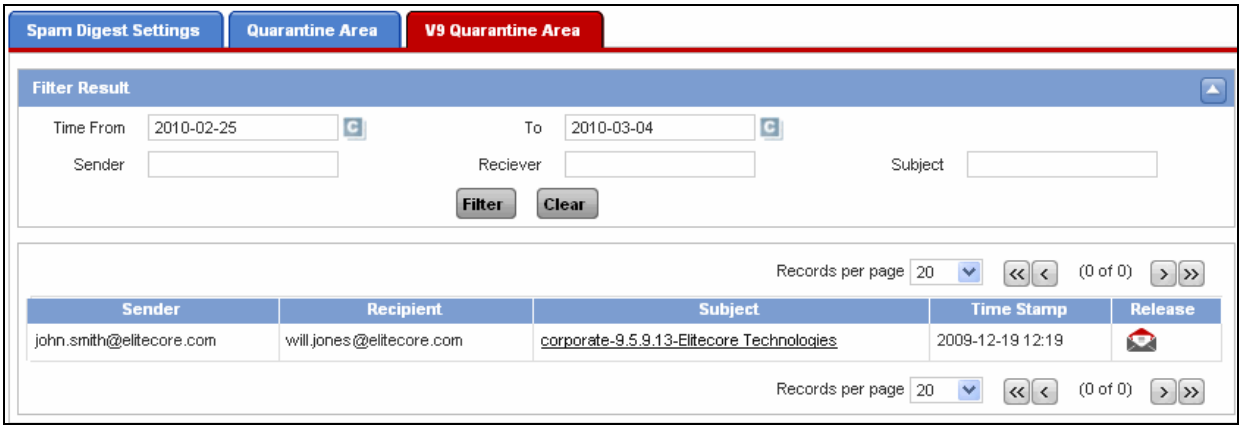
Under V 9 Quarantine Area, old Quarantined mails can be searched based on sender email address, receiver email address, and subject. These mails are migrated when Cyberoam is migrated to Version 10.

Cyberoam reserves 5GB for Quarantine area. To maintain the total size of Quarantine area,

Cyberoam removes older mails once the repository is filled by 80% i.e. once the repository level crosses 4GB, Cyberoam automatically deletes the oldest quarantined mails.

Use 'Filter Result' section to search for mails from the list of Quarantined Mails. To view and release the quarantined mails go to, **Anti Spam → Quarantine → V 9 Quarantine Area**.

Manage V 9 Quarantined Mails



Screen – Manage V9 Quarantine Mails

Screen Elements	Description
Sender	Sender of the Mail
Recipient	Recipient of the Mail
Subject	Mail Subject
Time Stamp	Timestamp when the mail was received.
Release Icon	Click on the Release Icon to move the mails from Quarantine area to recipient's inbox.

Table – Manage V 9 Quarantine Mails screen elements

Release V 9 Quarantined Spam Mails

Either Administrator or user himself can release the quarantined spam mails. Administrator can release the quarantined spam mails from Quarantine area while user can release from his My Account. Released quarantined spam mails are delivered to the intended recipient's inbox.

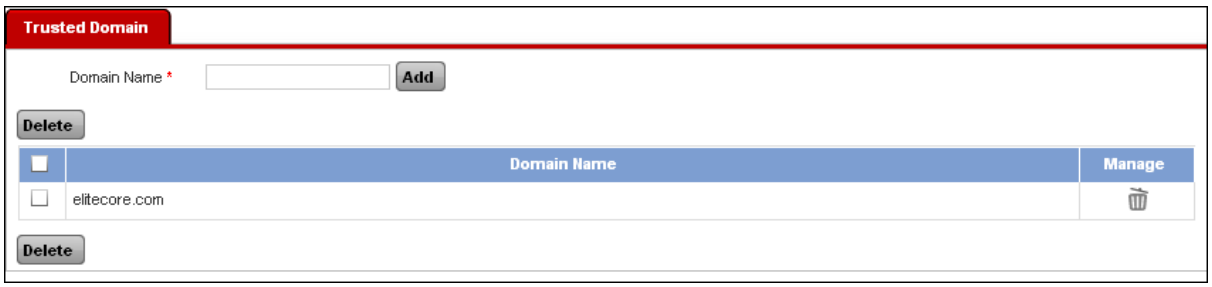
Administrator can access Spam Quarantine area from **Anti Spam → Quarantine → V 9 Quarantine Area**, while user can logon to My Account and access Spam Quarantine area from **Quarantine Mails → Spam → Spam Quarantine Area**.

Trusted Domain

Cyberoam also allows bypassing RBL scanning of mails from the certain domains. For this, you have to define the domains as the trusted domains.

To manage local domains, go to **Anti Spam → Trusted Domain**. You can:

- Add – Specify the Domain name and click the Add Button. Mails from the specified domains will not be scanned.
- Delete – Click the Delete icon in the Manage column against a Domain to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Domain. To delete multiple domains, select them and click the Delete button.



Screen – Add/Remove Trusted Domain