Cyberoam Anti Virus Configuration Guide

Version 10

Document version 10.00.0302 - 1.0-27/07/2010

Important Notice

Elitecore has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement.

Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

LIMITED WARRANTY

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and Commtouch respectively and the performance thereof is under warranty provided by Kaspersky Labs and by Commtouch. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

DISCLAIMER OF WARRANTY

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In no event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.

In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

RESTRICTED RIGHTS

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 4
About this Guide 5
Typographic Conventions 5
Report 5
Introduction 5
Notation conventions 5
Technical Support 6
Virus 7
Cyberoam Gateway Anti Virus 8
Enable Anti Virus scanning 8
Mail 9
Configuration 9
SMTP Scanning Rules 10
POP/IMAP Scanning Rules 15
Address Group 15
HTTP Configuration 18
Configuration 18
HTTP Scanning Rules 19
HTTPS Scanning 20
HTTPS Scanning Exception 21
FTP 23
Quarantine 24
Quarantine Area 24
V 9 Quarantine 24

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 virus solution and helps you manage and customize Cyberoam to meet your organization's various requirements including creating groups and users and assigning policies 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): +91-79-66065777
Email: support@cyberoam.com
Web site: www.cyberoam.com

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

Virus

Virus is a self-replicating malicious code that spreads by attaching itself to an application program, any executable system component, or documents and leaves no obvious signs of its presence.

Viruses are hard to detect, easy to propagate, and difficult to remove.

With the number of computer users growing and the exchange of information via the Internet and email increases in volume, virus scares are becoming an almost everyday occurrence. Real mass attacks have become commonplace, and the consequences are serious, resulting in financial loss for individuals and corporations alike.

The number of threats and frequency and speed of attacks is increasing every day. Antivirus protection is therefore a priority for anyone who uses a computer.

Although viruses are transmitted mainly through emails or attachments to an e-mail note and Internet downloads, a diskette or CD can also be a source of infection. Therefore, the task of comprehensive protection against potential threats now extends beyond simple regular virus scans to real time anti virus protection.

Cyberoam Gateway Anti Virus

Cyberoam Gateway Anti Virus provides you with powerful tools for scanning and detecting infection and spam in the incoming e-mail traffic. For detecting virus, Cyberoam uses its built-in signature database.

Cyberoam Anti Virus scans:

- HTTP
- HTTPS
- FTP
- SMTP
- POP3
- IMAP

traffic as it passes through the Cyberoam. For extra protection, you can configure to block specified file types from passing through the Cyberoam. You can use this feature to stop files that might contain new viruses. Additional filtration of messages from configured IP address and URL decreases the load on the server when scanning email traffic for viruses.

Cyberoam Anti Virus allows to:

- Scan email messages for viruses
- Detect infected, suspicious, and password-protected attachments and message
- Stop users from sending/receiving messages with any type of attachments
- Perform anti-virus processing of infection revealed in email messages by scanning
- Define policies to take appropriate action based on the protocol i.e. define action policy on how to handle for SMTP, POP3, FTP traffic and HTTP and HTTPS traffic if infection is detected
- Limit HTTP and FTP download file size
- Notify senders, recipients, and the administrator about messages containing infected, suspicious, or password protected attachments
- Quarantine messages - Quarantine feature allows to isolate and move infected and suspicious mails in a quarantine directory defined by a network administrator.
- Customize the anti virus protection of incoming and outgoing e-mail messages by defining scan policies.

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

Gateway Anti Virus module is an add-on module, which needs to be subscribed before use.

Enable Anti Virus scanning

Enable anti-virus scanning from firewall rules. While anti-virus settings can be configured for system-wide use, they can also be implemented with specific settings on a per user basis. Refer to Cyberoam User Guide, Firewall section for creating firewall rules for enabling the anti-virus scanning.

You can enable anti virus scanning by creating firewall rule for:

- Zone
- User/User Group
- Host/Host Group

Mail

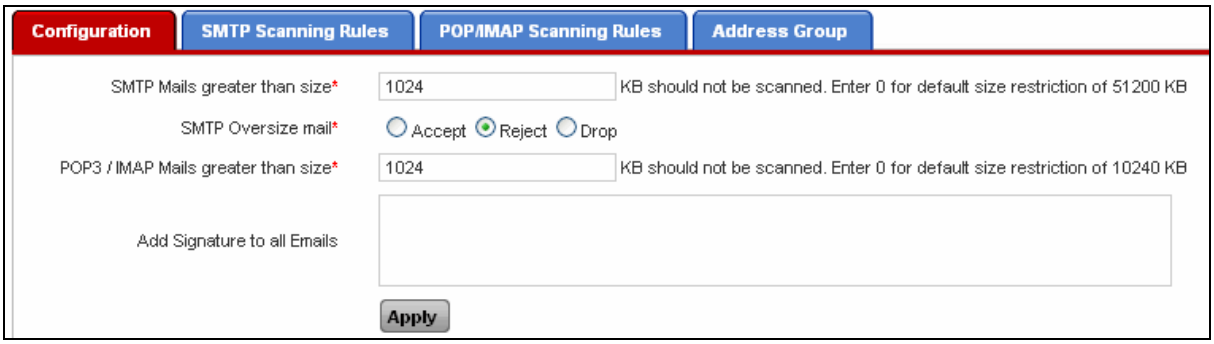
This chapter describes how to configure email security for the files received HTTP, FTP, SMTP, POP/IMAP. Following topics are included in this chapter:

- General Configuration
- SMTP Scanning Rules
- POP/IMAP Scanning Rules
- Address Group

Configuration

General Configuration allows Administrator to configure restrict file size for scanning.

To configure restrictions, go to **Anti Virus → Mail → Configuration**.



Screen – Mail Configuration

Parameters

Screen Elements	Description
SMTP Mail Size	Specify maximum size (in KB) of the file to be scanned. Cyberoam will not scan files exceeding this size received through SMTP protocol. Specify 0 for default size restriction of 51200 KB i.e. files exceeding 51200 KB will not be scanned if 0 is configured. For CR15i models, default size restriction is 1024 KB

SMTP Oversize Mail	Specify the action for the oversize mails. 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. Cyberoam will forward all the POP/IMAP mails exceeding this size received to recipients without scanning. By default, Specify 0 for default size restriction of 10240 KB and files exceeding 10240 KB will not be scanned if 0 is configured. For CR15i models, default size restriction is 1024 KB
Add Signature	
To All Emails	Specify signature to be added to all the outgoing mails. Only text signatures are allowed.

Table – Mail Configuration screen elements

SMTP Scanning Rules

Cyberoam allows to define policies to take appropriate action based on the protocols i.e. define separate action policy on how to handle for SMTP, POP3, FTP and HTTP traffic if infection is detected.

SMTP policy is applied to the SMTP traffic only i.e. when the virus is detected in SMTP traffic, SMTP policy is applied. Depending on the action specified in the policy, mail is quarantined /cured/removed thus preventing virus from being circulated.

As soon as you register Cyberoam Gateway Anti Virus, default SMTP policy is applicable to the all inbound and outbound email traffic. Default policy is the general policy and not fit-for-all policy and hence might not fit in your network requirement.

Cyberoam allows you to define multiple policies instead of one global policy, as per your requirements. Fine tuning the policies means reducing the virus attacks.

SMTP Scan policy defines:

- whether to quarantine the message or not
- what action is to be taken if mail is infected
- whether to block the message containing the specified file type
- whether sender, receiver and Administrator are to be notified or not

To configure SMTP Scanning rules, go to **Anti Virus → Mail → SMTP Scanning Rules**.

- Add
- View
- Edit – Click the Edit icon  in the Manage column against the Scanning Rule to be modified. Edit Scanning Rule window is displayed that has the same parameters as the Add Scanning Rule window.
- Search – Click the Search icon  in the Sender and Recipient columns to search for SMTP rules with specific Sender and Recipients. All the columns can be searched on the following

criteria: is, is not, contains and 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.

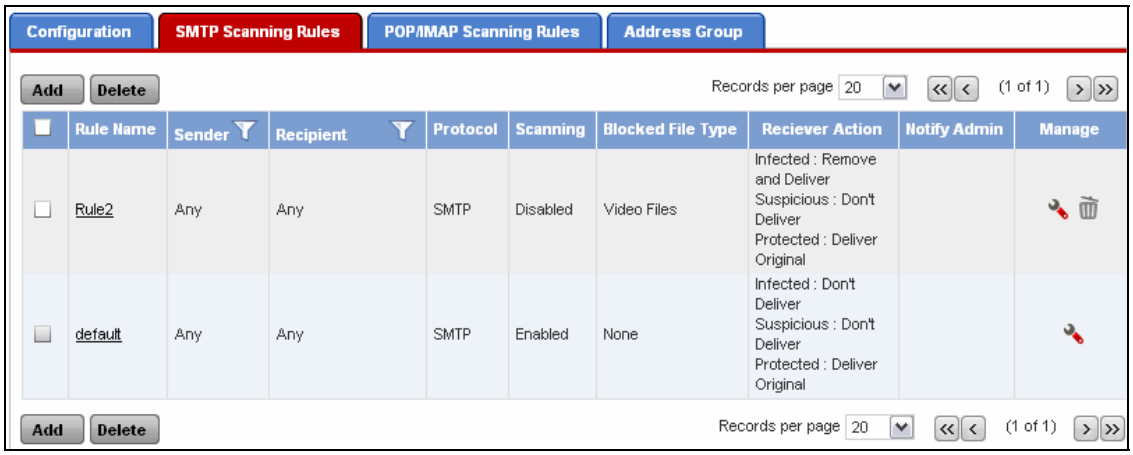
Screen – Search Sender/Receiver

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 Scanning Rule to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Scanning Rule. To delete multiple Scanning Rules, select them and click the Delete button.
- Default Rule - As soon as you subscribe Cyberoam Gateway Anti Virus, default SMTP policy is applicable to the all inbound and outbound email traffic. You can modify default policy to fit in your network requirement but cannot delete.

Manage SMTP Scanning Rules



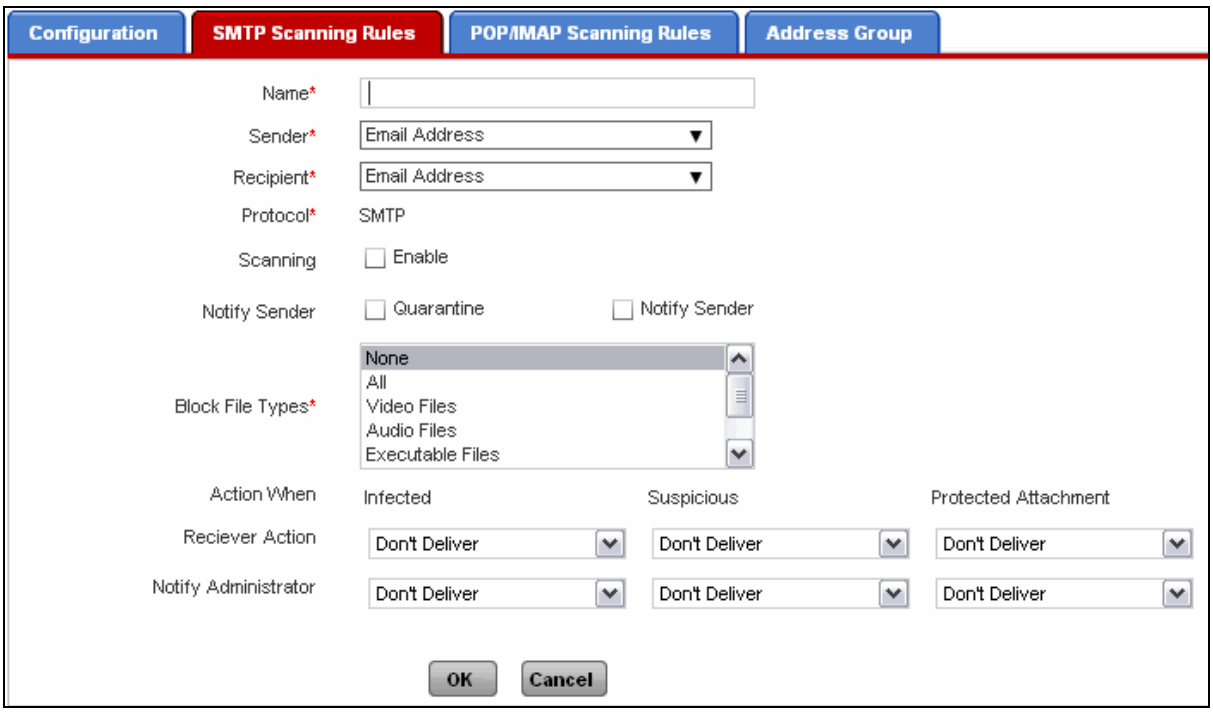
Screen – Manage SMTP Scanning Rules

Screen Elements	Description
Add Button	Add a new SMTP Scanning Rule
Rule Name	Name of the SMTP Scanning Rule
Sender	Username of the Sender
Recipient	Username of the Recipient
Protocol	SMTP Protocol
Scanning	Scanning Enabled or Disabled
Quarantine (Not for CR15i models)	Quarantine Enabled or Disabled
Blocked File Types	File Types that are blocked
Receiver Action	Receiver Action specified for Infected, Suspicious and Protected Attachments
Notify Admin	Notification Message to Admin for Infected, Suspicious and Protected Attachments
Edit icon	Edit the SMTP Scanning Rule
Delete Button	Delete the SMTP Scanning Rule Alternately, click the Delete icon against the scanning rule to be deleted.

Table – Manage SMTP Scanning Rules screen elements

SMTP Scanning Rule Parameters

To add or edit SMTP scanning rules, go to **Anti Virus → Mail → SMTP Scanning Rules**. Click Add Button to add a new rule or click Edit Icon against the rule to be modified.



Screen – Add SMTP Scanning Rule

Screen Elements	Description
Name	Name to identify the Scanning Rule
Sender	Select the sender name from the list of users. Select "Any" if the rule is to be applied on all the senders.
Recipient	Select the recipient name from the list of users. Select "Any" if the rule is to be applied on all the recipients.
Protocol	SMTP Protocol
Scanning	Specify whether the policy should be enabled for use or not. If enabled, policy will be used for virus scanning and blocking the attachments of specified file types.
Notify Sender	Specify action to be taken on the mails received for notifying the sender. Click on Quarantine and Notify Sender checkbox to take appropriate action. **Available Options**: • **Quarantine** – If enabled, does not deliver mail but copies the mail to the quarantine file list. You can view the mail details like sender and receiver of the mail in the quarantined file list. **Note** Quarantine option is not available in Cyberoam CR15i models. • **Notify Sender** - If enabled, sends a notification to the

	sender that the mail was infected.
Block File Types	Specify file types to be blocked as an attachment to remove all the files that are a potential threat and to prevent virus attacks. More than one file type can be selected using ctrl/shift keys. The list of file types is preconfigured with a list of default file extensions. Refer to Default File Types to view the list of file extensions which will be blocked. Selected Blocked file types will not be scanned. Instead of creating individual policies to block the messages with different file types, you can simply create a single policy and select 'ALL' in block file types to block messages with any type of file attachment. Using Block File Types, you can also stop users from sending/ receiving the messages with attachments. **Available Options**: • All – Messages with any type of file as an attachment will be blocked. • None – Do not block messages with attachment • Video Files – Block messages with video file attachment • Audio Files – Block messages with audio file attachment • Executable Files – Block messages with any executable file as an attachment • Dynamic Files – Block messages with any dynamic file as an attachment • Image Files – Block messages with images files
Action When (Message is:)	
Infected	Specify action to be taken Receiver Action – Receiver will be notified according to the action specified if the message has infected attachments. Notify Administrator – Administrator will be notified according to the action specified if the message has infected attachments.
Suspicious	Specify action to be taken Receiver Action – Receiver will be notified according to the action specified if the message has suspicious attachments. Notify Administrator – Administrator will be notified according to the action specified if the message has suspicious attachments.
Protected Attachment	Specify action to be taken Receiver Action – Receiver will be notified according to the action specified if the message has protected attachments. Notify Administrator – Administrator will be notified according to the action specified if the message has protected attachments.
Receiver Actions:	

• **Don't Deliver** – Receiver will not be delivered the message and will not be notified that the mail was infected. • **Remove and Deliver** – Will remove the infected part of the mail before delivery. Receiver will also receive the notification stating that the mail was infected and infected portion of the mail is removed. Not applicable for Blocked Attachments (Block File Type). • **Deliver Original** – Will deliver the original mail and the receiver will receive the notification along with the mail stating that mail is infected but not cured or removed. Cyberoam will not scan the protected attachment but receiver will be notified if not specified otherwise.
Administrator Actions: • **Don't Deliver** – Administrator will not be notified that the mail was infected on delivery • **Remove Attachment** – Will remove the attachment from the mail before delivery. Administrator will also receive the notification stating that the mail attachment was infected and removed. • **Send Original** – Will deliver the original mail without removing infected portion. Administrator will receive the notification stating mail is infected but not removed. Cyberoam will not scan the protected attachment but receiver will be notified if not specified otherwise.

Table – Add SMTP Scanning Rule screen elements

POP/IMAP Scanning Rules

Cyberoam allows to define policies to take appropriate action based on the protocols i.e. define separate action rule on how to handle for SMTP, POP3, FTP and HTTP traffic if infection is detected.

POP/IMAP rule is applied to the POP3 or IMAP traffic. When the message containing virus is detected, Cyberoam strips the infected attachment and simply sends the notification to the receiver stating that mail was not delivered because it was infected.

SMTP rule is not applicable to POP3 and IMAP traffic.

Sample Message (send to the receiver)

Subject: **VIRUS FOUND MAIL REJECTED**

Virus infected attachment(s) have been removed from this mail.
Virus Name(s): "Virus name list"
Attachment Name(s): "File names list" [From > sender name] [Date]

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.

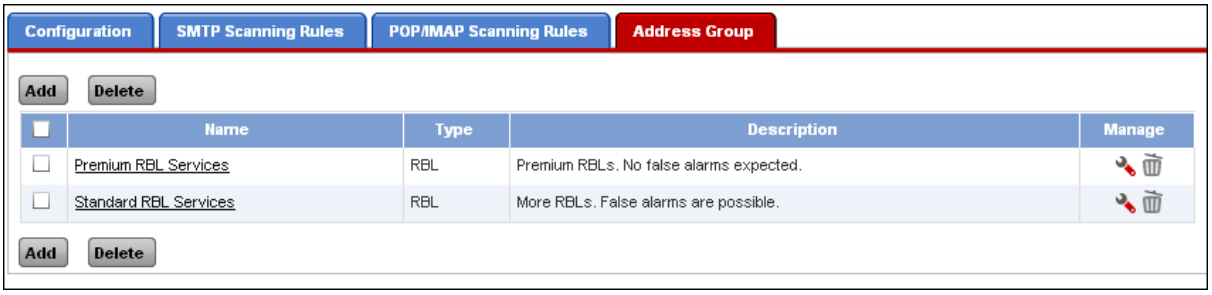
RBL is a list of IP addresses whose owners refuse to stop the proliferation of spam i.e. are responsible for spam or are hijacked for spam relay. This IP addresses might also be used for spreading virus.

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 Virus → Mail → 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 Groups



Screen – Manage Address Groups

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 Groups screen elements

Address Group Parameters

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. Specify Domain Name to be added as RBLs to the Address Group. • **IP address** - Specify IP address or IP range to be added to the Address Group. • **Email address/Domain** - 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

HTTP Configuration

Use HTTP Configuration to

- Define file size threshold
- Define HTTP scanning rule
- Delete HTTP scanning rule
- Update scanning order

Apart from mails, virus can infect your network through HTTP downloads also. Define HTTP scanning rules to protect against this.

Cyberoam can be configured for real time or batch mode scanning for HTTP traffic.

You can configure the maximum file size that can be buffered to the memory for scanning. This will also prevent the unintentional download of virus file hidden in the fragmented files.

By default, Cyberoam will not scan HTTP traffic. HTTP scanning is to be enabled from firewall rule, You can also define the rule to bypass scanning of the traffic from specific source and destination. If virus scanning is enabled and virus is detected, receiver will receive a notifying message.

Sample message

Cyberoam Anti virus Alert

The URL you are trying to access has been blocked as it contains the virus "**Constructor.BAT.BVGHH.11**"

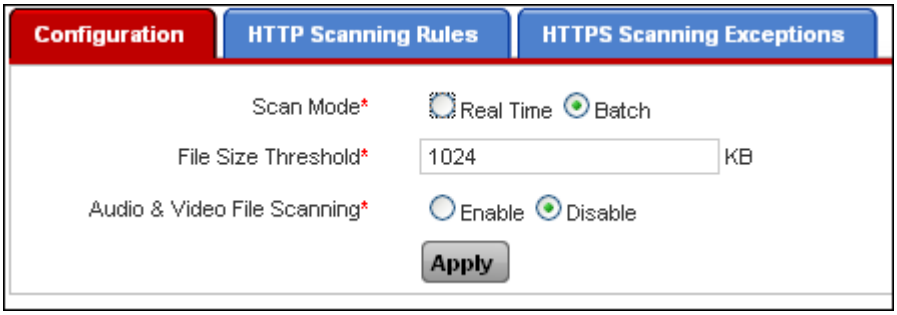
URL : **vx.netlux.org/dl/vir/Constructor.BAT.BVGHH.11.zip?x=13&y=17**

Configuration

Use configuration page to set the scanning criteria for the HTTP traffic.

To configure restrictions on HTTP traffic, go to **Anti Virus → HTTP/S → Configuration**.

Configure Parameters



Screen – Configure Parameters

Screen Elements	Description
Scan Mode	Specify scanning mode. Cyberoam can be configured for real time or batch mode scanning for HTTP traffic. In batch mode, virus scanning will start only after the complete file will be downloaded. As complete file is to be downloaded before scanning can start, if the size of the file is large it will take some time. To avoid the delay, configure scan in real mode if you have to download bulky files.
File Size Threshold	Specify File Size Threshold (in KB). Files that exceed configured threshold will not be scanned. Default value is 1024 KB
Audio & Video File Scanning	Enable to bypass HTTP scanning of video and audio streams in order to avoid delays caused by scanning and downloading the entire stream prior to playing. By default, audio and video files scanning is disabled.

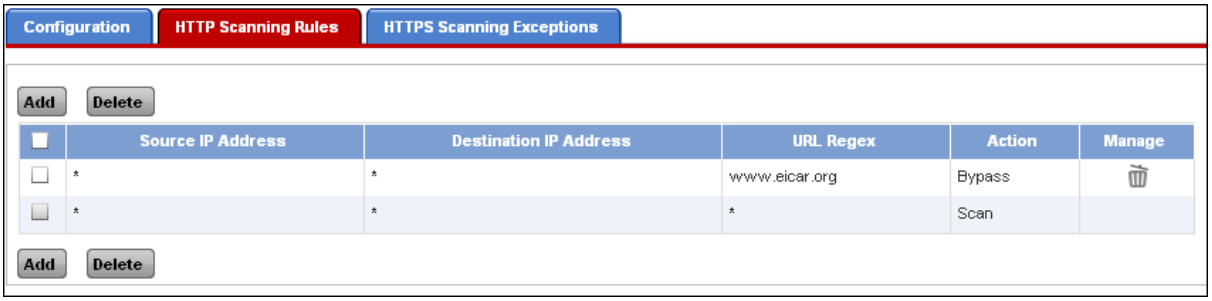
Table – Configure Parameters screen elements

HTTP Scanning Rules

To configure HTTP Scanning rules, go to **Anti Virus → HTTP/S → HTTP Scanning Rules**.

- Add
- View
- Edit – Click the Edit icon in the Manage column against the Scanning Rule to be modified. Edit Scanning Rule pop-up window is displayed that has the same parameters as the Add Scanning Rule window
- Delete – Click the Delete icon in the Manage column against a Scanning Rule to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Scanning Rule. To delete multiple Scanning Rules, select them and click the Delete button.

Manage HTTP Scanning Rules

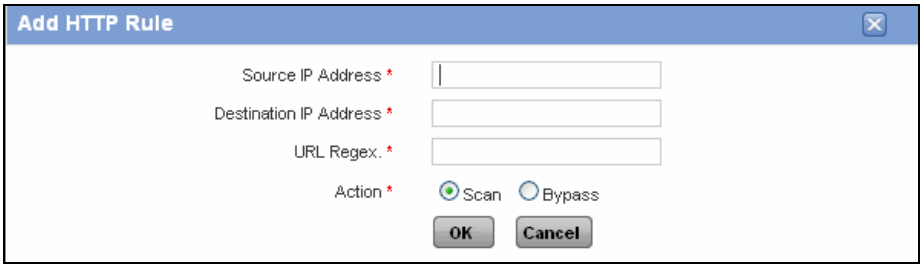


Screen – Manage HTTP Scanning Rules

Screen Elements	Description
Add Button	Add a new HTTP Scanning Rule
Sender	Sender IP address
Recipient	Recipient IP address
URL RegeX	Regular Expression for matching the pattern in URL
Action	Scanning enabled or not
Edit icon	Edit the HTTP Scanning Rule
Delete Button	Delete the HTTP Scanning Rule Alternately, click the Delete icon against the scanning rule to be deleted.

Table – Manage HTTP Scanning Rules screen elements

HTTP Scanning Rule Parameters



Screen – Add HTTP Scanning Rule

Screen Elements	Description
Source IP Address	Specify source IP address.
Destination IP Address	Specify destination IP address. Scanning rule will be applied on the mails received from the sender using specified source IP address and send to the recipient with the specified destination IP address.
URL Regex	Specify URL. You can use regular expression for matching the pattern in URL.
Action	Select whether you want to scan or bypass traffic for the specified source/destination IP address and URL.

Table – Add HTTP Scanning Rule screen elements

HTTPS Scanning

Cyberoam supports SSL content scanning and inspection to filter HTTPS traffic in the same way as HTTP traffic.

It allows administrator to control user access to web sites using encrypted HTTPS protocol. It is also possible to bypass scanning of certain encrypted sites like bank and trading sites.

As the access to encrypted sites is based on the certificates, certificate-blocking feature provides a way to specify which HTTPS certificates to block. Hence, apart from blocking the sites based on IP address, it would also be possible to block the sites, which do not provide certificate from the

trusted Certificate Authority.

By default, HTTPS scanning is disabled. To scan HTTPS traffic, enable HTTPS scanning from firewall rule and update all the Web Filter policies to allow HTTPS traffic. If you enable HTTPS scanning, you need to import Cyberoam SSL Proxy certificate in Internet Explorer, Firefox Mozilla or any other browsers for decryption on SSL Inspection otherwise browser will always give a warning page when you try to access any secure site. Import certificate for all the Instant Messengers which require certificate. Please refer, How To – Download and Install CA Certificate for details.

If you have configured HTTPS service on any other port than 443, traffic on that port will not be scanned.

Behavior

SSL Certificate Name mismatch error

The name mismatch error indicates that the common name (domain name) in the SSL certificate does not match the address that is in the address bar of the browser. To avoid this error, simply add this site as an exception. Once added as exception, warning will not be displayed next time you access the site.

Invalid Certificate error

This warning appears when the site is using an invalid SSL certificate. Cyberoam blocks all such sites. To allow access to such sites:

1. Logon to CLI with default credentials
2. Go to Option 4 Cyberoam Console and at command prompt execute the command:
   set service-param HTTPS invalid-certificate allow

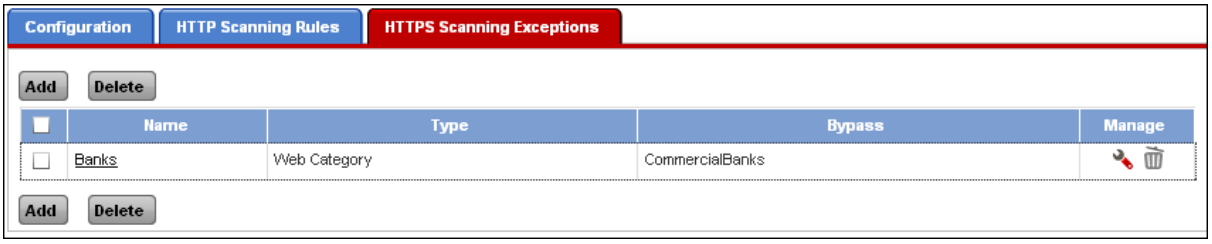
HTTPS Scanning Exception

If it is required to bypass HTTPS scanning for any web or file type category, add HTTPS Scanning Exception rule for the required category from Antivirus > HTTP/S > HTTPS Scanning Exception.

To configure HTTP Scanning Exception rules, go to **Anti Virus → HTTP/S → Scanning Rules**.

- Add
- View
- Edit – Click the Edit icon in the Manage column against the Scanning Exception Rule to be modified. Edit pop-up window is displayed that has the same parameters as the Add Scanning Rule window
- Delete – Click the Delete icon in the Manage column against a Scanning Exception Rule to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Scanning Exception Rule. To delete multiple Scanning Exception Rules, select them and click the Delete button.

Manage Scanning Exceptions Rule

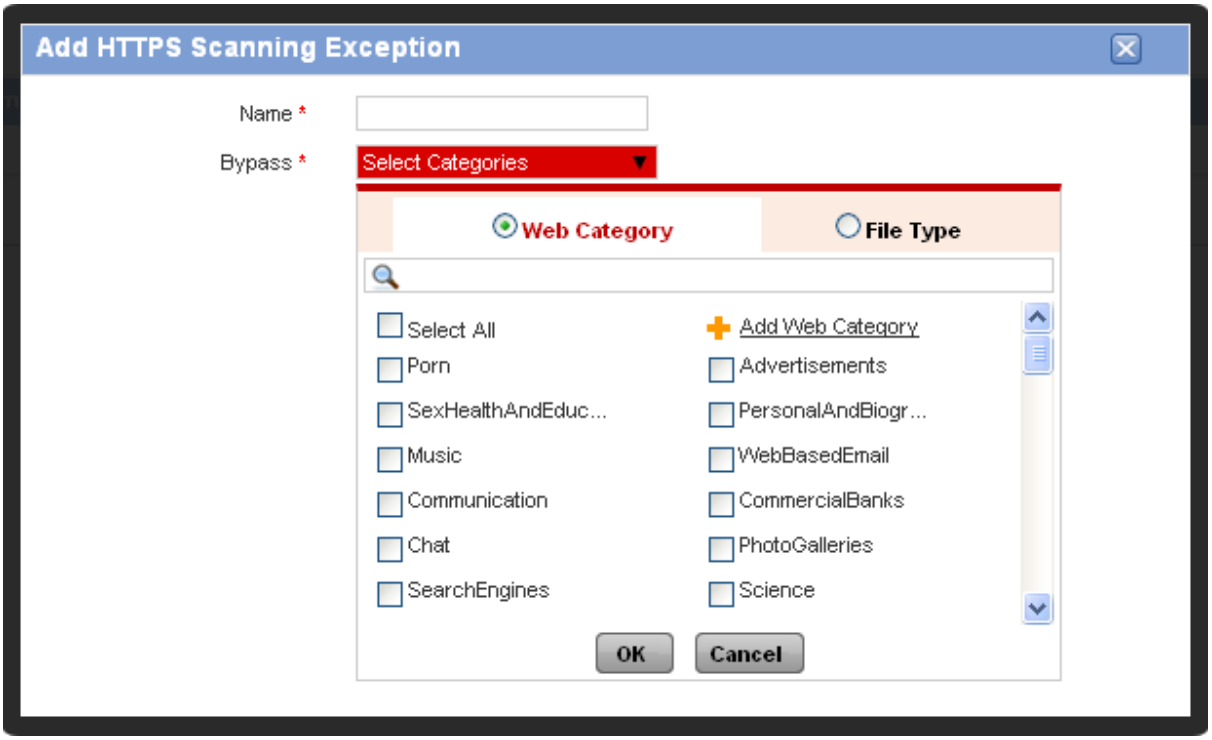


Screen – Manage HTTPS Scanning Exceptions

Screen Elements	Description
Add Button	Add a new HTTPS Scanning Exception Rule
Name	Rule Name
Type	Rule Type: Web Category, File Type
Bypass	Bypassed Category name
Edit icon	Edit the HTTPS Scanning Exception Rule
Delete Button	Delete the HTTP Scanning Exception Rule

Table – Manage HTTPS Scanning Exceptions Screen Elements

HTTPS Scanning Exceptions Rule Parameters



Screen – Add HTTPS Scanning Exception

Name Specify name for the bypass rule

Bypass Select web category or file type category to be bypassed

for HTTPS scanning

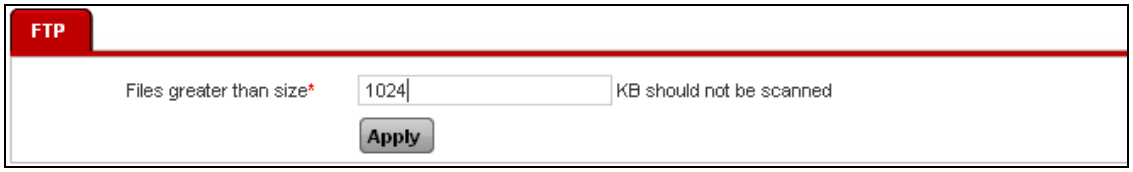
Table – Add HTTPS Scanning Exceptions Screen Elements

FTP

Cyberoam allows to define policies to take appropriate action based on the protocols i.e. define separate action policy on how to handle for SMTP, POP3, FTP and HTTP traffic if infection is detected.

Cyberoam detects virus and removes the infected file from FTP download or from an email message.

To configure FTP file size, go to **Anti Virus → FTP → FTP**.



Screen – Configure FTP File Size

You can configure the maximum file size (in KB) for scanning. The file size range is 1 KB to 51200 KB and the default size is 1024. Mails greater than the specified size will not be scanned.

Quarantine

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.

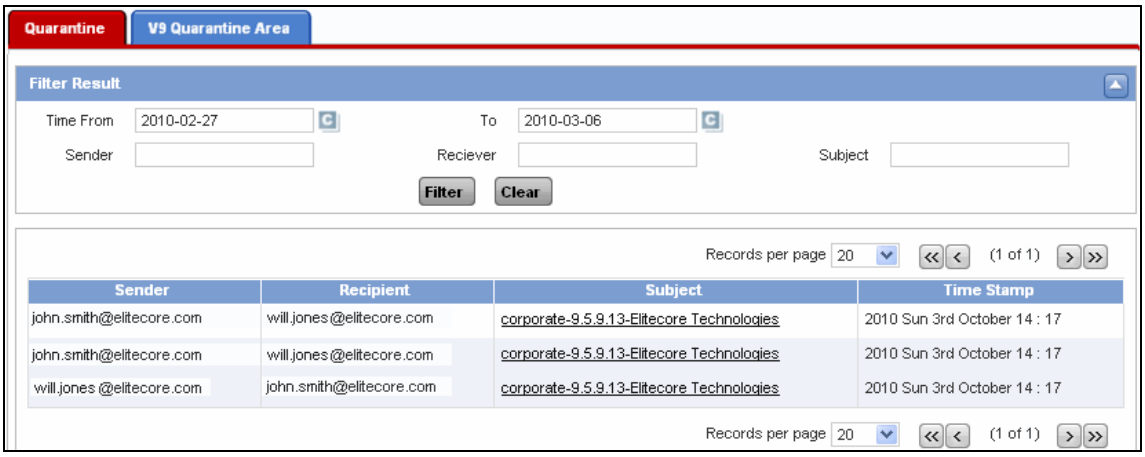
Note

Quarantine option is not available for Cyberoam CR15i models.

Quarantine Area

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

Use 'Filter Result' section to search for mails from the list of Quarantined Mails. To view the quarantined mails go to, **Anti Virus → Quarantine → Quarantine**.



Screen – View 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

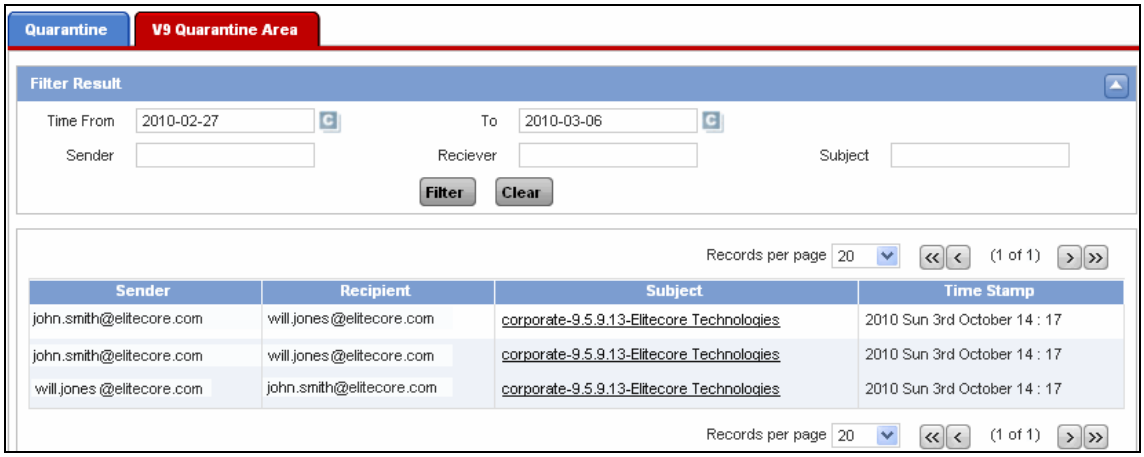
Table – View Quarantine Mails screen elements

V 9 Quarantine

Under V 9 Quarantine, old Quarantined mails can be searched based on sender email address, receiver email address, and subject. These are the quarantined mails, which are migrated after upgrading to v 10.

Use 'Filter Result' section to search for mails from the list of Quarantined Mails. To view the

migrated quarantined mails go to, **Anti Virus → Quarantine → V 9 Quarantine**.



Screen – View V 9 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.

Table – View V 9 Quarantine Mails screen elements

Change Log

Revision	Topic	Description
1.0		Initial Release for version 10
1.1		Mail Configuration - changed field name Manage Address Groups - Screen changed HTTP Configuration - Screen changed HTTP Scanning Rules - Screen changed HTTPS Scanning – entire section added