



Cyberoam Multi link Implementation Guide

Version 9

Document version 9402 -1.0-18/10/2006

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 the performance thereof is under warranty provided by Kaspersky Labs. 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 the 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 of or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

RESTRICTED RIGHTS

Copyright 2000 Elitecore Technologies Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Elitecore Technologies Ltd. Information supplies by Elitecore Technologies Ltd. Is believed to be accurate and reliable at the time of printing, but Elitecore Technologies assumes no responsibility for any errors that may appear in this documents. Elitecore Technologies reserves the right, without notice, to make changes in product design or specifications. Information is subject to change without notice

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-26405600
Fax: +91-79-26407640
Web site: www.elitecore.com , www.cyberoam.com

Guide Sets

Guide	Describes
User Guide	
Console Guide	Console Management
Windows Client Guide	Installation & configuration of Cyberoam Windows Client
Linux Client Guide	Installation & configuration of Cyberoam Linux Client
HTTP Client Guide	Installation & configuration of Cyberoam HTTP Client
Analytical Tool Guide	Using the Analytical tool for diagnosing and troubleshooting common problems
LDAP Integration Guide	Configuration for integrating LDAP with Cyberoam for external authentication
ADS Integration Guide	Configuration for integrating ADS with Cyberoam for external authentication
PDC Integration Guide	Configuration for integrating PDC with Cyberoam for authentication
RADIUS Integration Guide	Configuration for integrating RADIUS with Cyberoam for external authentication
High Availability Configuration Guide	Configuration of High Availability (HA)
Data transfer Management Guide	Configuration and Management of user based data transfer policy
Multi Link Manager User Guide	Configuration of Multiple Gateways, load balancing and failover
VPN Management	Implementing and managing VPN
Cyberoam IDP Implementation Guide	Configuring, implementing and managing Intrusion Detection and Prevention
Cyberoam Anti Virus Implementation Guide	Configuring and implementing anti virus solution
Cyberoam Anti Spam Implementation Guide	Configuring and implementing anti spam solution

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: +91-79-26405600
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.

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	Group Management → Groups → Create it means, to open the required page click on Group management then on Groups and finally click Create tab
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

Overview

Welcome to the Cyberoam's – Multi Link Manager User Guide.

Cyberoam's integrated Internet security solution is purpose-built to meet the unified threat management needs of corporate, government organizations and educational institutions. It also provides assistance in improving Bandwidth management, increasing Employee productivity and reducing legal liability associated with undesirable Internet content access.

Cyberoam's - Weighted Load Balancing feature enables Network Managers to optimize network traffic and balance the load between multiple gateways/links. It also supports the failover detection and switchover mechanism to an alternate link when an active link goes down.

Introduction

Load balancing is a mechanism that enables balancing traffic between various links. It distributes traffic among various links, optimizing utilization of all links to accelerate performance and cut operating costs. Employing a weighted round robin algorithm for load balancing, Cyberoam enables maximum utilization of capacities across the various links.

In addition to distributing traffic, Cyberoam detects link failure i.e. when a gateway stops responding or goes down and passes the traffic to the operating link. This safeguard helps you provide uninterrupted, continuous Internet connectivity to your users.

Using link load balancing provides organizations a way to achieve:

1. Traffic distribution that does not overburden any link
2. Automatic ISP failover
3. Improved User performance because of no downtime
4. Increased bandwidth scalability

How it works

Load balancing is determined by the load metric i.e. weight. Each link is assigned a relative weight and Cyberoam distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link relative to the other link.

Administrators can set weight and define how the traffic should be directed to providers to best utilize their bandwidth investments. Weight can be selected based on:

1. Link capacity (for links with different bandwidth)
2. Link/Bandwidth cost (for links with varying cost)

Configuring Gateways

Basic load balancing consists of defining multiple gateways. During the installation, you have already configured the IP address of the default Gateway. Apart from defining gateway, configuration also consists of:

1. Assigning weight to each link
2. How to check for the link failure
3. What action to take in case of link failure

Add Gateway

Select **System** → **Gateway** → **Manage Gateway(s)**

Manage Gateway(s)				Logout	Help	Cyberoam
Gateway Name	Gateway IPAddress	Weight	Select			
DefaultGateway	192.168.4.1	1	<input type="radio"/>			
elticor	203.88.135.209	1	<input type="radio"/>			
				Failover Conditions	Add	Delete

Screen – Multiple Gateway Configuration

Screen Elements	Description
Gateway Name	Displays Gateway name
Gateway IP address	Displays IP address of the Gateway configured IP address of a device Cyberoam uses to reach devices on different Network, typically a router
Weight	Displays weight assigned to the Gateway Used for load balancing and failover
Select	Allows to select the Gateway for adding failover condition or deleting the gateway itself
Failover Conditions button	Allows to add failover rules for the selected gateway Refer to Define Failover rules for more details
Add button	Allows to adds a new Gateway Refer to Add Gateway for more details
Delete button Option available only if more than one gateway is defined	Deletes the selected gateway Refer to Delete Gateway for more details

Table - Gateway Configuration screen elements

Add Gateway

Gateway Details

Gateway Name*	<input type="text"/>
IP Address*	<input type="text"/>
Ethernet Port*	Select Here ▼
Weight*	<input type="text"/>

Screen - Add Gateway

Screen Elements	Description
Gateway Details	
Gateway name	Assign unique name to the Gateway
IP address and port	IP address port of the Gateway
Weight	Assign weight to the gateway Depending on the weight assigned, Cyberoam will select gateway for load balancing Set weight as 0 (zero) to disables load balancing and pass the traffic through the default gateway Set same weight to all the links to distribute traffic equally among all the links Set different weights to various links to distribute traffic in the ratio of the proportions of the weight set
Add button	Defines a new Gateway
Cancel button	Cancels the current operation and returns to Manage Gateway page

Table - Add Gateway screen elements

Delete Gateway

Select **System** → **Gateway** → **Manage Gateway(s)**

Manage Gateway			
		Logout	Help
		Cyberoam	
Gateway Name	Gateway IPAddress	Weight	Select
DefaultGateway	192.168.1.254	1	<input type="radio"/>
gateway	192.168.1.203	2	<input checked="" type="radio"/>
		Add	Delete

Screen - Delete Gateway

Screen Elements	Description
Select	Selects Gateway for deletion Click <i>Select</i> to select
Delete button	Deletes selected gateway Click to delete

Table - Delete Gateway screen elements

Note

If only one gateway is defined then it cannot be deleted

Source Network routing

Source Network routing allows Administrators to direct traffic generated from particular Network over designated links according to the business policies.

When you define Source based routing for a particular subnet, all the traffic coming from that subnet will be forwarded to the defined Interface.

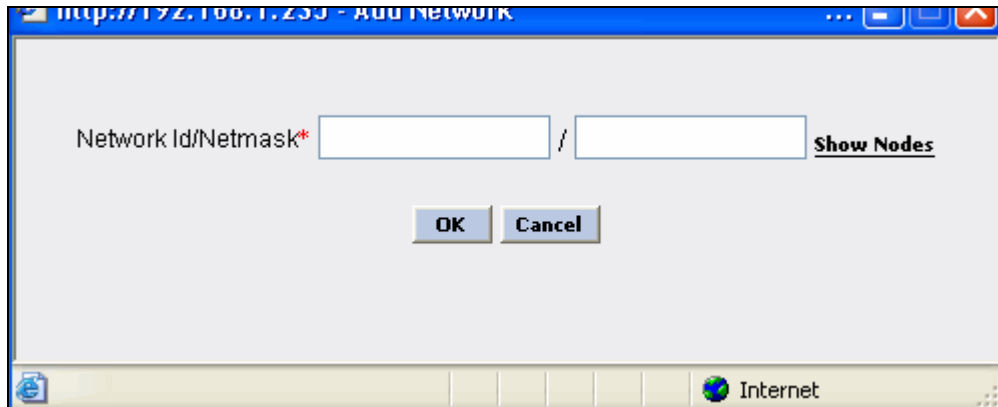
Select **System** → **Gateway** → **Manage Gateway(s)** and click gateway through which Network traffic is to be routed

Screen – Configure Gateway

Screen Elements	Description
Gateway details	
Gateway name	Displays Gateway name through which the Network traffic will be routed, modify if required
IP address and port	Displays Gateway IP address and port, modify if required
Weight	Displays the weight assigned to the gateway, modify if required
Save button	Saves the modified details
Cancel button	Cancels the current operation
Networks explicitly routed through this gateway	
Add Network button	Allows to add network which will be routed through the selected gateway Click <i>Add Network</i> to add Refer to Add Network for more details
Remove Network button	Allows to remove network Refer to Remove Network for more details

Table – Configure Gateway screen elements

Add Network

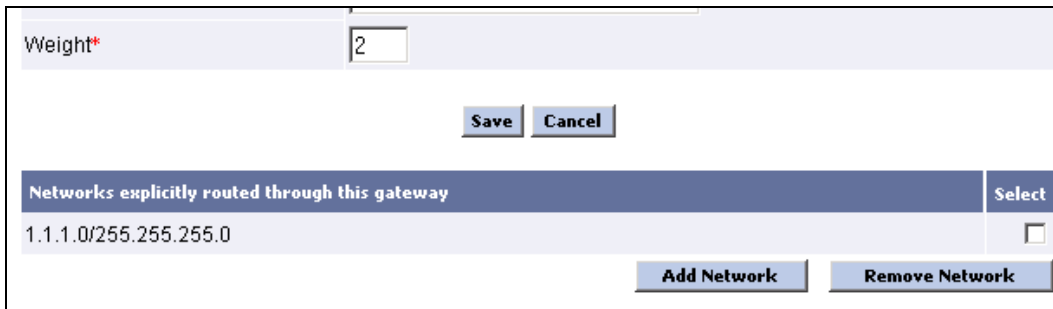


Screen - Add Network screen

Screen Elements	Description
Network ID	Specify Network ID for the Network to be added to the selected Gateway
Net mask	Specify Net mask for the Network
Show Nodes link	Opens a new window and displays list of Nodes in the Network
Ok button	Adds Network to the Gateway
Cancel button	Cancels the current operation

Table - Add Network screen elements

Remove Network



Screen - Remove Network screen

Screen Elements	Description
Select	Selects Network for deletion Click <i>Select</i> to select
Remove Network button	Deletes selected Network Click to delete

Table - Remove Network screen elements

Gateway failover

Gateway failover provides link failure protection i.e. when one link goes down; the traffic is switched over to the active link. The transition is seamless and transparent to the end user with no disruption in service i.e. no downtime.

Whenever Cyberoam detects a failed link, it stops sending traffic to the failed link and sends traffic to the other available link. If two or more links are active when failure is detected, traffic is distributed among the active links in the ratio of the weights assigned to them.

Cyberoam continuously checks for the status of dead link and when the dead link is available again, it is reused.

Configuration

Once the links are configured for load balancing, define link failover rule.

Failover rules

The transition from dead link to active link is based on the failover rule defined for the link. Failover rule specifies:

1. how to check whether the link is active or dead
2. what action to take when link is not active

Failover rule has the form:

```
IF
  Condition 1
  AND/OR
  Condition 2
then
  Action
```

Depending on the outcome of the condition, traffic is shifted to any other available gateway.

By default, Cyberoam creates Ping rule for every gateway. Cyberoam periodically sends the ping request to check health of the link and if link does not respond, traffic is automatically sent through another available link.

Select **System** → **Gateway** → **Manage Gateway(s)**

Select Gateway for which the failover rule is to defined and Click Failover Conditions

The screenshot shows the 'Manage Gateway(s)' interface. At the top, there are navigation links for 'Logout', 'Help', and 'Cyberoam'. Below this is a table with the following data:

Gateway Name	Gateway IPAddress	Weight	Select
DefaultGateway	192.168.4.1	1	<input type="radio"/>
eltiecor	203.88.135.209	1	<input type="radio"/>

Below the table are buttons for 'Failover Conditions', 'Add', and 'Delete'. A 'Configure Failover conditions' dialog box is open, showing the following details:

Gateway details

Name	second
IP Adress	192.168.1.203

Failover Rules

Buttons: Add, Edit, Delete

IF... Not able to PING on IP Address '192.168.1.203'

Then... "SHIFT to another available Gateway"

Buttons: Add, Edit, Delete

Screen – Manage Gateway

Screen Elements	Description
Gateway details	
Name	Displays Gateway name for which the failover rule will be created
IP Address	Displays Gateway IP address
Failover Rules	
Add button	Allows to define a rule Click to add Refer to Add Failover rule for more details
Edit button	Allows to edit a rule Click to edit Refer to Edit Failover rule for more details
Delete button	Allows to remove a rule Refer to Remove Failover rule for more details

Table – Manage Gateway screen elements

Add Failover rule

1. Select **System → Gateway → Manage Gateway(s)**
2. Select Gateway and Click Failover Condition
3. Click Add
4. Specify communication Protocol i.e. TCP, UDP, PING (ICMP). Select the protocol depending on the service to be tested on the host.
5. Specify Port number for communication
6. Specify Host

Host must be represented by the computer or Network device which is permanently running or most reliable.

Specify whether all of the rule conditions must be met before the specified action occurs (AND) or whether at least one must be met (OR) by selecting AND or OR

A request on the specified port is send to the Host. If Host does not respond to the request, Cyberoam considers the Host as 'dead', stops sending traffic to the Host and sends traffic through another available Host

7. Click Save

Configure Failover conditions
Logout
Help

Gateway details	
Name	second
IP Adress	192.168.1.203

Failover Rules

IF...

Not able to **Connect** **Port** **on IP Address**

Not able to **Connect** **Port** **on IP Address**

Then...

"SHIFT to another available Gateway"

Screen – Add Failover rule

Edit Failover rule

1. Select **System** → **Gateway** → **Manage Gateway(s)**
2. Select Gateway and Click Failover Condition
3. Click Edit
4. Modify condition as per requirement
5. Click Save

Configure Failover conditions Logout Help

Gateway details

Name	second
IP Address	192.168.1.203

Failover Rules

IF...

Not able to **Connect** **Port** on **IP Address**

Not able to **Connect** **Port** on **IP Address**

Then...

"SHIFT to another available Gateway"

Screen – Edit Failover rule

Remove Failover rule

1. Select **System** → **Gateway** → **Manage Gateway(s)**
2. Select Gateway and Click Failover Condition
3. Click the condition to be removed
4. Click Delete
5. Click OK to save

Configure Failover conditions

Gateway details	
Name	second
IP Address	192.168.1.203

Failover Rules

Add **Edit** **Delete**

IF...

Not able to **PING** on **IP Address '192.168.1.203'**

OR

Not able to **Connect TCP Port '23'** on **IP Address '192.168.1.203'**

Then...

"SHIFT to another available Gateway"

Add **Edit** **Delete**

OK

Screen – Delete Failover rule