

Release Information

Compatible versions: V 9.4.2.0, 9.4.2.8, 9.4.3.0, 9.4.3.5

Upgrade Information

Upgrade type: Manual upgrade. **After upgrade, reboot is required for the changes to take effect.**

Upgrade procedure

1. Download upgrade from <http://downloads.cyberoam.com/version9/>
2. Log on to Web Admin console and go to Help> Upload Upgrade and upload the file downloaded in step 1
3. Once the file is uploaded successfully, log on to Telnet console and go to option 6 Upgrade Version and follow the on-screen instructions.

Compatibility Issues: None

Contents

Introduction	2
New Features	2
1. Virtual LAN (802.1q) support in Route mode	2
2. High Availability (HA) with Load balancing and failover protection...	2
3. Dynamic Routing.....	3
4. Anti spam module - Virus Outbreak Detection Technology.....	4
5. TCP MSS Configuration option	4
6. Hard disk drive Check feature.....	4
Enhancements.....	5
1. Anti Virus (AV) and Anti Spam (AS) reports Improvement.....	5
2. Report titles.....	5
3. Network Configuration Improvement.....	5
4. Web Categories	5
General Availability of Beta Version 9.4.3.0 and 9.4.3.5.....	6
1. Performance improvement.....	6
2. Authentication Session timeout per Group.....	8
3. Personalized Dashboard.....	8
Discontinued CLI options and commands.....	9
Bugs Solved.....	9
General Information	12
Technical Assistance.....	12
Technical Support Documents	12

Introduction

This document contains the release notes for Cyberoam version 9.5.0 build 21. The following sections describe the release in detail and provide other information that supplements the main documentation.

This is a major release with new features and several bug solved that improves quality, reliability, and performance.

New Features

1. Virtual LAN (802.1q) support in Route mode

Cyberoam 9.5.0.1 release, support 802.1q VLAN processing to provide granular virtualization, scalability, and improved security through logical network segmentation by the means of virtual interface. Security zones can now include Virtual Interface and/or physical ports; inter-zone policies enable complete granularity and control.

VLAN technology allows implementing multi-tier security domain network design concept to secure discrete departments, project teams, or applications without regards to the physical location of users through single Cyberoam appliance only.

Network throughput improvement is achieved by introducing this feature as VLAN confines broadcast domain.

Virtual interface has most of the capabilities and characteristics of a physical interface, including zone membership, security services, routing, access rule controls, IDP, virus, and spam scanning.

For the ease of use, VLAN configuration and management is provided from the View Network Interface page of Web Admin Console.

2. High Availability (HA) with Load balancing and failover protection*

To minimize the single point of failure, Cyberoam offers an integrated high availability solution providing efficient, continuous access to critical applications, information, and services. High availability is critical to maintaining network protection from an attack, even in the event of a device failure.

To achieve high availability, HA cluster is to be defined which consists of two Cyberoam appliances and both appliances in the cluster share session and configuration information.

Active-Passive HA

In Active-Passive HA, primary appliance processes the entire traffic and Auxiliary appliance is in standby mode. Auxiliary appliance processes the entire network traffic only incase of primary appliance failure.

Active-Active HA

Session persistent Load balancing

* High Availability feature would be enabled on demand.

Active-Active HA increases overall network performance by sharing the load of processing network traffic and providing security services. The cluster appears to your network to be a single device, adding increased performance without changing your network configuration.

Primary appliance acts as the load balancer and load balances all the TCP communications including TCP communications from Proxies but will not load balance VPN traffic.

Failover

In Active-Active HA both Primary and Auxiliary appliances process the network traffic and Auxiliary appliance takes over the primary appliance and processes complete traffic in case of primary appliance failure or link/monitored interface failure.

Session failover

Session failover occurs for forwarded TCP traffic except for virus scanned sessions that are in progress, VPN sessions, UDP, ICMP, multicast, and broadcast sessions and Proxy traffic.

Synchronization

Cluster configuration, routing tables, and individual cluster appliance status between Cluster appliances are synchronized automatically when a configuration event occurs.

Additionally, Web Console Admin provides the option for Manual synchronization also.

In addition, Cyberoam now has inbuilt monitoring services that monitor critical services in the appliance and even take the corrective and preventive actions to ensure availability.

Prerequisite: Both the Appliances must have same number of Interfaces, same software version and deployed in Route mode.

Known Behavior

1. **DHCP & PPPoE** – High Availability (HA) cluster cannot be configured if any of the Cyberoam Interfaces is dynamically configured using DHCP and PPPoE protocols.
2. **Cyberoam upgrade** - AutoUpgrade mode will automatically be disabled on both the cluster appliances once High Availability (HA) cluster is configured. To upgrade HA cluster appliances, HA mode is to be disabled and each appliance has to be upgraded individually.
3. **HA Session failover** – AV Scanned sessions, VPN sessions, UDP, ICMP, multicast, and broadcast sessions and Proxy traffic sessions are not maintained when HA cluster is configured.
4. **Masqueraded Connections** – In case of the following events from any of the HA cluster appliances, all the masqueraded connections will be dropped:
 - Restart Management Service (RMS)
 - Execution of Network Configuration
 - Manual Synchronization
5. **HA Load balancing** – Active-Active HA cluster does not load balance VPN sessions, UDP, ICMP, multicast, and broadcast sessions. TCP traffic for Web Admin Console or Telnet Console and VLAN traffic sessions are also not load balanced between the cluster appliances.

3. Dynamic Routing

Earlier Cyberoam versions used static routing method whereby routes for each network were to be defined manually. This was a handy process for a small network with very few routes and also when links go down corrections are to be done manually. It becomes a cumbersome process when network grows.

By introducing Dynamic routing feature in this version, Cyberoam has overcome the limitations of static routes configuration. General benefits of dynamic routing are:

- More automation: Routing updates are automatically sent to all other routers.
- Change notification: The dynamic routing protocol will reroute traffic around a link that is down or congested.
- Greater uptime for users: Because the routing protocol has intelligence and can react faster, the users may see more uptime.
- Greater network throughput: Because the routing protocol may be able to calculate the most responsive network link to use, the users may see less latency and more performance out of the network.
- Less work for administrators: As the network grows, the administrator does not have to worry about configuring all the other routers on the network.

Cyberoam has implemented **RIP (Routing Information Protocol)** - version 2 as described in RFC2453 and version 1 as described in RFC1058 - and **OSPF (Open shortest Path First)** - version 2 as per RFC 2328, routing protocols for dynamic routing.

Telnet Console provides the Cisco compliant CLI for routing configuration.

4. Anti spam module - Virus Outbreak Detection Technology

To provide protection against new email-borne virus outbreaks, hours before the signatures are released, Cyberoam has introduced the proactive virus detection technology which detects and blocks the new outbreaks immediately and accurately.

It provides a critical first layer of defense by intelligently blocking suspicious mail during the earliest stage of a virus outbreak.

Defining outbreak security actions in the Spam policy from Web Admin Console allows to proactively detect, prevent, or contain, and eliminate outbreaks.

5. TCP MSS Configuration option

The TCP MSS Adjustment feature enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, when PPP over Ethernet (PPPoE) is being used in the network. PPPoE truncates the Ethernet maximum transmission unit (MTU) 1492, and if the effective MTU on the hosts (PCs) is not changed, the router in between the host and the server can terminate the TCP sessions.

Option for TCP MSS adjustment is provided on Telnet Console.

6. Hard disk drive Check feature

With this version, Cyberoam is introducing a feature to check the Hard disk drive partition size. This feature will check hard disk drive on every reboot and will increase the partition size if a different layout from the minimum requirement is found.

Enhancements

1. Anti Virus (AV) and Anti Spam (AS) reports Improvement

For identifying virus and spam source, AV and AS now include:

- Reference Id - Reference Id is the message pattern identification tag as classified by Cyberoam Spam Detection Center and is added in the Email header for each mail.
- Source and Destination IP address.

2. Report titles

To effectively communicate with the International customers and project a strong international image, reports menu and titles are changed.

3. Network Configuration Improvement

To improve ease of use and maintenance, Interface Alias can be added from View Network Interface page of Web Admin Console.

Till previous versions, one had to add Alias from Telnet Console.

4. Web Categories

Cyberoam provides a new category for web filtering called 'Hacking' making total of 68 categories. Category includes Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases.

Till previous versions such sites were categorized under the category 'ComputerSecurityandHacking'.

General Availability of Beta Version 9.4.3.0 and 9.4.3.5

Cyberoam announces the General Availability for the following Beta features of Version 9.4.3.0 and 9.4.3.5

1. Performance improvement

Content filtering and Anti Virus Scanning

Earlier versions of Cyberoam used the most common synchronous I/O model. After a request is made in this model, the application blocks until the request is satisfied. The calling application requires no central processing unit (CPU) while it awaits the completion of the I/O request. So the serving thread gets blocked while waiting for the completion of the I/O request. But in some cases there is a need to overlap an I/O request with other processing like serving other requests, virus scanning, etc.

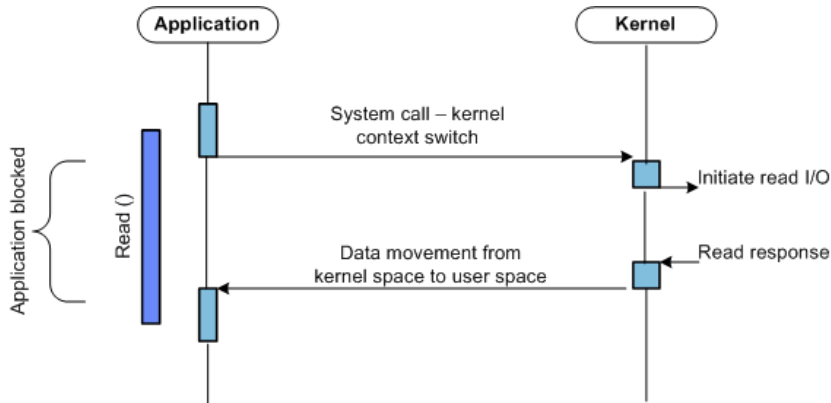
Types of I/O

	Blocking	Non-Blocking
Synchronous	Read/Write	Read/Write (O_NONBLOCK)
Asynchronous	I/O multiplexing (select/poll)	AIO

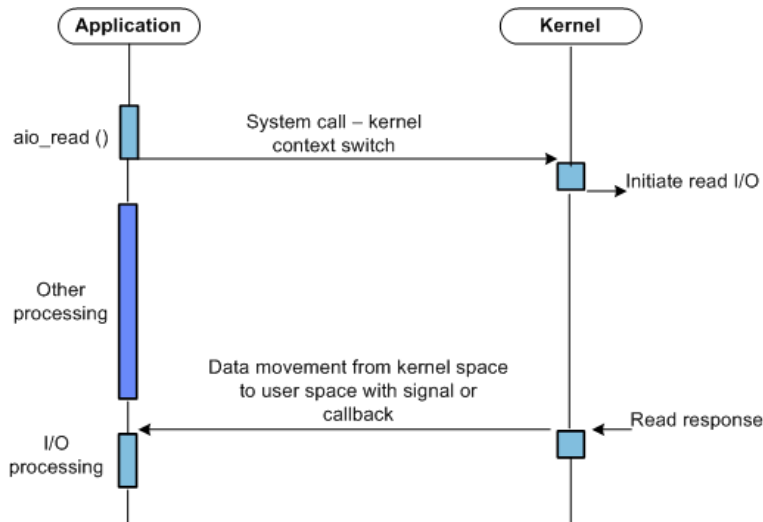
Till the earlier versions, Cyberoam proxy subsystem was built on Threaded Synchronous Blocking I/O Architecture. Higher throughput and concurrency (number of concurrent connections) was achieved by using threaded model proxy subsystem. But concurrency achieved by system was restricted by number of threads. High number of threads can achieve higher concurrency but at the same time it will degrade system performance and reduce overall throughput. Threads waiting for I/O completion in case of slow response or antivirus processing latency will decrease the connection rate drastically.

To optimize the performance, Cyberoam architecture is changed. New architecture of Cyberoam Proxy Subsystem uses single threaded Asynchronous I/O. Load on the system will not be increased as new architecture uses single thread. With the non-blocking I/O asynchronous architecture, it can perform other tasks like serving other connections, virus scanning, etc... instead of waiting for I/O completion.

Typical flow of the synchronous blocking I/O model (Previous Architecture)



Typical flow of the asynchronous non-blocking I/O model (New Architecture)



Earlier versions of Cyberoam used the most common synchronous method for DNS lookups. In this method, the requesting process blocks until a response is received i.e. DNS lookup is complete or a timeout occurs. These timeouts are fairly long and absolutely nothing is done by the requesting process during this time.

Asynchronous DNS lookup

To optimize the performance and robustness, from the current Cyberoam has implemented asynchronous DNS lookup method.

Asynchronous DNS lookup means processing continues without waiting for the completion of the lookup. By taking this approach, nothing is blocked while waiting for a reply that comes late.

With this implementation, the performance will increase, particularly of those applications which need to perform DNS queries without blocking or need to perform multiple DNS queries in parallel. The primary examples of such applications are servers which communicate with multiple clients and programs with graphical user interfaces.

2. Authentication Session timeout per Group

For finer granularity, Cyberoam now supports authenticated session timeout on per-group basis. Authentication session timeout is the number of minutes that after which the user will be logged out automatically.

By default this option is disabled and can be enabled and configured from Create/Manage Group page of Web Admin Console.

The minimum timeout that can be configured is 3 minutes and maximum is 1440 minutes (24 hours).

3. Personalized Dashboard

Dashboard page is now completely customizable. Each section (System Information, License Information, Gateway status information, Usage summary etc.) can be closed or repositioned simply by dragging and dropping. Personalized Dashboard allow repositioning of the sections that requires special attention on the top and the information less used, moved to the bottom.

This feature also provides a flexibility to define multiple layouts of Dashboard view for multiple Administrators and layout will persist till it is explicitly reset to the default layout.

The screenshot displays the Cyberoam Dashboard interface with a navigation bar at the top containing links for Register, Support, Wizard, Cyberoam, Help, and Logout. A 'Reset' button is located in the top right corner of the dashboard area.

Alert Messages

09.05.2007 2:08:06 AM	The default Web Admin Console password hasn't been changed
09.05.2007 2:08:07 AM	The default CLI Console password hasn't been changed
09.05.2007 2:08:06 AM	Your Cyberoam Appliance is not registered
12.05.2007 11:13:44 AM	HTTPS,SSH, based management is allowed from the WAN. This is not a secure configuration. It is recommended to use a good password.
12.05.2007 11:13:44 AM	HTTP based management is allowed from the WAN. This is not a secure configuration. It is recommended to use a good password.

HTTP Traffic Analysis

Distribution by Hits	10%	42%	48%
Distribution by Data Transfer	10%	29%	60%

Usage Summary

HTTP Hits	1945
Search Engine Queries	Google

User Surfing Pattern

Users visiting Unhealthy Sites	75%
Users visiting Non-working Sites	75%
Users visiting Productive Sites	-
Non-working Surfing Time*	5 Hrs. and 12 Mins.
Unhealthy Surfing Time*	2 Hrs. and 15 Mins.

Installation Information

Appliance Key	0%
Appliance Model	-
Cyberoam Corporate Version	9.4.3 build 0 [Check for Upgrades]
Web Category Database Version	1.0.0.182
Cyberoam Operation mode	Route

Recent FTP Viruses detected

Time	User	Domain	Name
12/May/2007 14:44:16	10.10.10.19	203.88.135.198	Email-Worm
12/May/2007 14:44:08	10.10.10.19	203.88.135.198	EICAR-Test

Recent HTTP Viruses detected

Time	User	Domain	Name
2007-05-12 15:44:15	unknown	www.eicar.org	EICAR-Test44:15

Gateway Status

Gateway Name	Gateway IP Address	Status
Default	203.88.140.113	●

Discontinued CLI options and commands

- Command removed from Telnet Console - show memory
- Option for configuring Alias IP address from Network Configuration menu is removed from Telnet Console. A similar option is now provided on Web Admin Console.

Bugs Solved

The purpose of this list is to give an overview of the bugs fixed in the current release. The ID denotes the internal Cyberoam bug tracking ID and the description explains problem.

Bug ID – 2079

Description – When FTP scanning is enabled, bandwidth restriction is not applied as per the configuration on FTP data transfer done through Windows Operating System.

Bug ID – 2158

Description – Interface Info graphs from DG.HTML displays Ethernet ports as eth0, eth1, eth2 etc. instead of ports A, B, C, D, etc.

Bug ID – 2338

Description – Mismatch in IDP alerts details displayed on the Dashboard and in the Recent IDP Alerts page.

Big ID - 2365

Description – Same IP address can be assigned to the multiple Ethernet ports via Network Configuration Wizard and Cyberoam CLI Console.

Bug ID – 2368

Description – L2TP VPN tunnel cannot be established when Cyberoam is assigned non-routable IP address (private IP address).

Bug ID – 2401

Description – Cyberoam does not provide PPPoE Interface link status information in Web Admin Console.

Bug ID – 2460

Description – Mails could not be detected and filtered as spam mails if the Email address specified in Mime Header From or To option include character "." (dot)

Bug ID – 2535

Description -

Single Alias IP address can be binded to multiple Interfaces.

It is not possible to remove multiple IP addresses binded to the Interface in single attempt but one has to delete IP addresses one by one.

Bug ID – 2750

Description – Enable/disable Reporting option in Internet Access policy does not work.

Bug ID – 2929

Description – TCP MSS adjustment is required if PPPoE link is terminated on Cyberoam. Due to this, www.hotmail.com is not accessible, Windows OS could not be updated, and

downloading is not possible.

Bug ID – 2958

Description – IDP policy is not applied immediately after creation. One needs to restart management services (RMS) from Telnet Console.

Bug ID – 3221

Description – Web surfing report displays complete data transfer even if file downloading is cancelled after a partial download.

Bug ID – 3226

Description – After restarting management services (RMS), if VPN tunnel is established before the IPSec daemon starts then data transfer through that link is not possible.

Bug ID – 3264

Description – If link speed is slow and FTP scanning is enabled, it is not possible to upload large files using FTP application.

Bug ID – 3275

Description – Following Dashboard tabs were renamed to convey the appropriate meaning:

Title in earlier Version	Renamed to
Installation Information	Appliance Information
Cyberoam Corporate Version	Cyberoam Software Version
Cyberoam Operation mode	Cyberoam Deployment mode

Bug ID – 3278

Description – Incorrect message is displayed in the Audit log when Cyberoam is restarted from Manage Servers page of Web Admin Console.

Bug ID – 3318

Description – Start and stop time configured at the time of schedule creation is not retained.

Bug ID – 3344

Description – Gateway status is displayed as 'Up' in the Dashboard even if the WAN port is disconnected.

Bug ID – 3355

Description – Execution of IDP report queries triggers high CPU usage.

Bug ID – 3358

Description – PPTP VPN connection log is not generated.

Bug ID – 3377

Description – VPN service needs to be restarted to start data transfer if PPPoE leases the same IP address to the connection.

Bug ID – 3380

Description – After restarting management services from Telnet console, it is possible to establish VPN tunnel but data transfer is not possible. This situation occurs as IPSec daemon gets restarts before the firewall services are restarted.

Bug ID – 3383

Description – Correct IP address if not configured if “Backspace” or “←” key is used while configuring IP address from Serial Console of the Cyberoam Appliance.

Bug ID – 3397

Description – “BAD Traffic same SRC/DST” is displayed in Recent IDP Alerts tab of Dashboard when antivirus scanning is enabled along with DNAT and IDP policy in LOCAL zone firewall rule. This also triggers high CPU usage.

Workaround – Remove IDP policy or disable antivirus scanning from the firewall rule.

Bug ID – 3433

Description – Bandwidth restriction is not applied as per the configuration if Cyberoam is configured as proxy server.

Bug ID – 3434

Description – It is not possible to scan and filter HTTP traffic if Web Admin Console was configured on a port other than 80.

Bug ID – 3435

Description – Following services are removed: svccanboot, qmail, courierimap and heartbeat services.

Bug ID – 3583

Description – HTTP proxy configuration does not get updated automatically on updating DNS configuration from Web based Console. One had to manually reconfigure HTTP Proxy.

Bug ID – 3585

Description – Cyberoam did not support Microsoft Netmeeting software for audio and video conferencing.

Bug ID – 3588

Description – Anti spam SMTP Search report displayed SPAM mails as well as valid mails as SPAM mails. From this version onwards, SMTP spam reports will display only the spam mails where as Anti spam SMTP Search report will display list of mails as per the specified search criteria.

Bug ID – 3590

Description – Dashboard was displayed with overlapping sections when viewed in Internet Explorer Version 7.

Bug ID – 3613

Description – As Log command was disabled for OSPF and RIP configuration from Telnet console, Cyberoam generated Log file error when daemon re-starts.

Bug ID – 3639

Description – Text message for License information in the configuration file is made more informative.

Bug ID – 3640

Description – Cyberoam did not support Microsoft Exchange server when HTTP Antivirus scanning was enabled in Batch mode.

General Information

Technical Assistance

If you have problems with your system, contact customer support using one of the following methods:

- Email id: support@cyberoam.com
- Telephonic support
- Asia Pacific, Australia & New Zealand: +91-79-66065777, +91-79-26400707
- USA & Other Countries: +1-201-484-7733/7581, +1-866-663-CYBR (toll free)

Please have the following information available prior to contacting support. This helps to ensure that our support staff can best assist you in resolving problems:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or dumps

Technical Support Documents

Knowledgebase: <http://kb.cyberoam.com>

Documentation set: <http://docs.cyberoam.com>

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 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: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com, www.cyberoam.com