

Product Release Information

Product: Cyberoam
Release Number: 9.4.2 build 0
Release Date: 30th April, 2007

Compatible versions: V 9.4.1.2

Upgrade type: Auto upgrade

Upgrade procedure:

By default, AutoUpgrade mode is ON/Enabled so Cyberoam will be upgraded automatically. It is possible to disable the automatic upgrade. Follow the procedure to disable the AutoUpgrade mode:

- Log on to Telnet Console
- Go to option 4 Cyberoam Console
- At the prompt, type the command, cyberoam autoupgrade off

If automatic upgrade is disabled, you have to upgrade manually. Refer to <http://kb.cyberoam.com/default.asp?id=346&SID=&Lang=1> for manual upgrade details.

Downtime: Upgrade process is expected to take around 2 minutes.

Customer Support: For more information or support, please visit www.cyberoam.com or email at support@cyberoam.com

Contents

Introduction	2
New Features	2
1. Cyberoam Central Console	2
2. VPN Fail over	3
3. CIPA Compliance	3
Enhancements	5
1. 3 rd party Certificate Authority	5
2. Cyberoam Dashboard	5
3. Search option in Anti Spam reports	5
4. True bridge mode	5
5. Generate binary file of traffic log generated with custom parameters	6
6. Maximum Transmission Unit (MTU) fine-tuning option	6
7. IM Client blocking – Skype, Windows live and Rediff bol	6
Bugs Solved	7
How to Report Problems	10

Introduction

This document contains the release notes for Cyberoam version 9.4.2 build 0. The following sections describe the release in detail and provide other information that supplements the main documentation.

This is a major release with few new features and features enhanced in response to several bug reports that improves quality, reliability, and performance without adding any new functionality.

New Features

1. Cyberoam Central Console

With the introduction of this tool, Cyberoam now helps Managed Security Service Providers, Enterprises – multiple branch offices same city multiple locations or in different Cities and Universities – multiple departments same campus or multiple campuses to manage and monitor their multiple Cyberoam Installations centrally.

Cyberoam Central Console is an integrated management and monitoring tool allows to manage multiple, dispersed Cyberoam Installations centrally. It establishes a central point for monitoring and maintaining multiple Cyberoam Installations.

Cyberoam Central Console is an independent and a separate hardware from Cyberoam i.e. not the part of Cyberoam Appliance, is to be purchased, installed, and registered separately.

Prerequisite: Each Cyberoam Appliance should allow HTTPS access for Cyberoam Central Console.

Web Admin Console

Web Admin Console is provided to configure and manage Cyberoam Central Console Appliance which can be accessed through HTTP or secure HTTPS connection.

Only configuration required on Cyberoam Central Console is the registration of all the Cyberoam Appliances that are to be managed and monitored through Cyberoam Central Console. To register a Cyberoam Appliance with Cyberoam Central Console, one needs to add IP address, Local administrator Username and password.

Additionally, from Web Admin console, one can also create/update following policies and rules and apply to any of the registered Cyberoam Appliances:

- Firewall rule
- Internet Access policy
- Categories
- IDP policy
- Custom IDP signature

Dashboard

Dashboard helps to watch all the registered Cyberoam Appliances for outages and events that requires attention. Cyberoam Central Console gets all the required information from Cyberoam Appliances which is displayed on Dashboard. This saves you from time consuming manual monitoring of multiple Cyberoam Appliances individually.

Dashboard displays live status / severity of following parameters of all the registered Cyberoam Appliances:

- Connectivity – Connectivity of Cyberoam with Cyberoam Central Console and connectivity of Cyberoam with its gateway (Mostly in case of Multiple gateway in Cyberoam)
- IDP Threats – Severity depends on number of events generated in last 5 minutes
- Virus Attack – Severity depends on % of Viruses detected with respect to total number of sites visited and mails received
- Spam Mails – Severity depends on % of SPAM mails received with respect to the total mails received
- Compatibility – Cyberoam Central Console will not be able to manage Cyberoam if not compatible, either Cyberoam Central Console / Cyberoam needs to be upgraded
- Subscription - Severity depends on number of days left in expiration for any module

Status and severity are classified as Dangerous, Warning, OK which is based on the preconfigured threshold values in Cyberoam Central Console.

Current version of Cyberoam Central Console does not support:

- Creation of Anti Virus and Anti Spam policies
- Deletion of Internet access policy, Bandwidth policy, IDP policy, IDP signature, Categories, host, and host group from Cyberoam using Cyberoam Central Console i.e. can be deleted locally from Cyberoam Central Console but can not be deleted from Cyberoam using Cyberoam Central Console.
- Access of Cyberoam Reports

2. VPN Fail over¹

Cyberoam now provides automatic failover for:

- IPSec Net-to-Net connection
- IPSec Road Warrior connection
- Host-to-Host connection
- L2TP connection

Depending on the connection type, connectivity with the remote peer or gateway is checked every 30 second. If the connectivity check fails, Cyberoam automatically re-directs the connection to the subsequent ACTIVE connection without waiting for the intervention from the Administrator.

3. CIPA Compliance

Cyberoam enables CIPA compliance for schools and libraries through its content filtering, allowing them to enforce an Internet safety policy that blocks and filters Internet access in accordance with CIPA requirements.

Sample policy

Name: Policy for minors

Policy Type: Allow

Reporting: Enable

Web Categories:

¹ Refer to VPN Management Guide (version 9420-1.0-19/04/2007 page 57) from docs.cyberoam.com for prerequisites and configuration details.

AdultContent
Alcohol/Tobacco
ComputerSecurityandHacking
CrimeandSuicide
Drugs
Gambling
MillitancyandExtremist
Nudity
PhishingandFraud
Porn
SexHealthandEducation
SwimwearAndLingerie
URL Translation sites
Violence
Weapons

Strategy: Deny

Schedule: All the time

Content filtering with CIPA compliance is required by the schools and libraries in US to receive funding under the E-Rate program which needs to have an Internet Safety Policy in place, ensuring the safety and security of minors online.

Enhancements

1. 3rd party Certificate Authority²

In this version, Cyberoam introduces significant enhancement to certificate-based authentication for VPN.

Cyberoam no longer requires uploading of the Certificates issued by the following 3rd party Certificate Authority before use:

- VeriSign Class 1, 2, 3, and 4 Primary CA
- Entrust.Net Secure Server Certificate
- Microsoft Root Certificate Authority

Till previous version, for certificate-based authentication, Cyberoam required to upload the certificates before use.

2. Cyberoam Dashboard

Noteworthy information related to configurations on the Cyberoam appliance that requires special attention such as password, access to critical security services, as well as notifications of subscription expirations are displayed in the **Alert Messages** section.

The alerts that are displayed are:

- The default Web Admin Console password has not been changed.
- Default Telnet Console password is not changed.
- <Service name(s)> base management is allowed from WAN. This is not a secure configuration. It is recommended to use a good password.
- Your Cyberoam Appliance is not registered.
- <module name(s)> modules will expire within 5/10/20 days. Be sure to buy the subscription to stay protected.
- <module name(s)> module(s) expired

3. Search option in Anti Spam reports

Search option has been added to Anti spam reports enabling to search Anti spam reports based on protocol, sender and receiver email address and email subject.

4. True bridge mode

In the previous versions of Cyberoam, one had to define routes for all the networks configured in Cyberoam. This limitation has been removed in this version.

Now multiple subnets can be used without any additional configuration i.e. without defining routes. This feature helps to maintain IP address transparency for routed IP addresses when virus and spam scanning as well as Internet Access policy is enabled from firewall rules.

Post upgrade reboot is required to use this feature.

² Refer to VPN Management Guide (version 9420-1.0-19/04/2007 page 22) from docs.cyberoam.com for details.

5. Generate binary file of traffic log generated with custom parameters

Cyberoam now supports to save and download the tcpdump output in a binary file from Telnet Console using following command: tcpdump <criteria> filedump

File tcpdump contains the troubleshooting information useful for Cyberoam Support team. Downloaded from http://<cyberooam_ip>/documents/tcpdump.out and mail this file to Cyberoam Support team at support@cyberoam.com

Please refer to <http://kb.cyberoam.com/default.asp?id=60&Lang=1&SID=> on how to understand the tcpdump output.

6. Maximum Transmission Unit (MTU) fine-tuning option

Cyberoam now allows configuring MTU as per the need whenever Cyberoam is connected with any PPPoE device such as ADSL. Fine-tuning MTU value is required due to PPPoE Architecture. Customization can be done from Option 1 Network Configuration of Telnet Console.

Default Cyberoam MTU:1500

Refer to <http://kb.cyberoam.com/default.asp?id=264&SID=&Lang=1> for more details.

7. IM Client blocking – Skype, Windows live and Rediff bol

Popular Instant Messenger clients Skype, Windows Live and Rediff bol can now be blocked through IDP signatures.

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 – 2222

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

Bug ID – 2337

Description – Cyberoam did not allow access to web categories defined in “Deny All” Internet Access policy.

Big ID - 2339

Description - When FTP scanning was enabled, Port forward rule does not work.

Bug ID – 2405

Description – L2TP VPN connection could not be activated when DHCP was enabled on WAN interface of Cyberoam. “Unable to activate” error was displayed at the time of activation.

Bug ID – 2439

Description – Factory reset does not reset From and To email addresses configured in Reports Notification.

Bug ID: 2446

Description – Cyberoam does not purge VPN logs.

Bug ID – 2526

Description – HTTP Client Users are not able to log on to Cyberoam when external authentication is configured.

Bug ID: 2534

Description – At the time of activating VPN connection, error “Unable to activate connection” is displayed, if preshared key included special character # (hash).

Bug ID – 2536

Description – Diagnostic tool displayed Gateway status as “Critical” even when gateway was reachable and ping to the gateway is successful.

Bug ID – 2569

Description – Web surfing reports were not included in backup of Log file.

Bug ID – 2596

Description – Anti Spam reports displayed incorrect Rule Type.

Bug ID: 2602

Description – The commands cyberoam dns-menu and cyberoam dialup-menu were available on Telnet Console even after the DNS and Dialup support was deprecated in the version 9.4.0.2.

Bug ID – 2634

Description – If HTTP Proxy port was configured on port 8088, Cyberoam Web Admin Console became inaccessible.

Bug ID: 2710

Description – Cyberoam was not able to resolve a DDNS hostname to a new IP address and re-connection if connection was lost. This situation occurred as IPsec daemon caches the previous IP address and sends the connection request on the previous IP address only.

Bug ID: 2726

Description – Net-to-Net VPN connection could not be activated when DHCP was enabled on WAN interface of Cyberoam.

Bug ID: 2752

Description – Diagnostic tool displayed “root partition full” error when the average load generated was high.

Bug ID: 2753

Description - Cyberoam does not rebuild firewall state when deployment mode is changed i.e. Gateway to Bridge mode and vice versa.

Cyberoam does not rebuild firewall state even after restoring the backup.

Bug ID: 2755

Description – IDP Engine crashes if Intrusion Detection and Prevention (IDP) module is not subscribed and IDP policy is applied.

Bug ID: 2759

Bug Description – Custom Web Categories did not work after restoring backup.

Bug ID: 2764

Bug Description – When FTP scanning was enabled, Destination NAT (DNAT) rule for FTP does not work.

Bug ID: 2768

Bug Description – Cyberoam did not log reboot or shutdown event in Audit log, if Cyberoam was rebooted using commands cyberoam shutdown or cyberoam restart from Telnet Console.

When Cyberoam was rebooted using commands cyberoam shutdown or cyberoam restart from Telnet Console, reboot or shutdown event were not logged in Audit log.

Bug ID: 2862

Description - Interface Alias configuration was not removed when Cyberoam deployment mode was changed i.e. Gateway to Bridge mode and vice versa.

Bug ID: 2863

Description – When Cyberoam is configured as Proxy server and FTP scanning was enabled on Cyberoam, FTP connections were not dropped.

Similar situation occurs for SMTP and POP connections.

Bug ID: 2864

Description - Cyberoam did not block mails when mail scanning was enabled and 'Deny All' Internet Access policy was applied.

Bug ID: 2865

Description – No provision for: viewing DHCP log, changing port to which DHCP service is binded, reserving IP address range, leasing specific IP address for MAC address.

Bug ID: 2920

Description – Download and upload data transfer column are transposed in Traffic discovery reports. Upgrade has solved the issue and correct report will be displayed only after rebooting Cyberoam.

Bug ID: 2930

Description – Cyberoam did not open FTP over HTTP request with username when parent proxy is configured e.g. ftp://support@ftp.elitecore.com

Bug ID: 2931

Description – Cyberoam crashed whenever FTP server responded with the large greeting messages greater than the size permitted by FTP RFC-959.

Bug ID: 2933

Description – Location of MySQL temporary files changed to avoid “/” partition full problem.

How to Report Problems

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

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