Product Release Information

Product: Cyberoam
Release Number: 9.4.0 build 2
Release Date: 16th November 2006

Compatible versions: 9.2.x build x and 9.3.0 build 5

Upgrade procedure: Manual[1]
URL to download upgrade: http://download.cyberoam.com/version9/upgrade.cyberoam.9402

Important note

- Direct upgrade to Version 9.4.0 build 2 is recommended if you are upgrading from Version 9.2.0 build 4
- Version 9.4.0.2 includes all the features and enhancement of V 9.3.0 build 5 also
- Refer to Cyberoam Release Notes 9.3.0 build 5 in case of direct upgrade
- Reboot Cyberoam after upgrading to version 9.4.0 build 2

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

[1] ***See Cyberoam User Guide*** ***(Document Version 9402-1.0-18/11/2006 - page number 221)*** ***for more information on how to upgrade.***

Contents

Product Release Information 1

Introduction 3

New Features 3
1. 24x7 High Availability 3
2. Dynamic DNS Support 3
3. FTP Scanning Support for Anti Virus 3
4. CPU Burn test 4
5. Protection against next generation Pharming attacks 4
6. HTTP Proxy 4

Enhancements 5
1. ActiveX, Cookie and Java Applet Content Filtering 5
2. RADIUS authentication 5
3. Custom signature support for IDP 5
4. SMTP Authentication 5
5. Dynamic IP support 5
6. VPN enhancements 5
7. Diagnostic Tool 6
8. Updated SSL (HTTPS) security 6
9. Enhanced Web Admin Console 6
10. FTP reports 6
11. HTTP Proxy support for Chinese characters in URL 6

Bugs fixes 7

Discontinued Feature 10

How to Report Problems 11

Introduction

This document contains the release notes for Cyberoam version 9.4.0 build 2. The following sections describe the release in detail and provide other information that supplements the main documentation.

This is a major release with many 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. 24x7 High Availability[2]

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

When deployed in Gateway mode, Cyberoam can be configured for Active-Passive HA in which secondary appliance processes the network traffic only when the primary appliance fails.

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.

Cyberoam also provides HA logs to aid troubleshooting which can be access from Telnet Console.

Prerequisite: Both the Appliances of the same model and software version.

2. Dynamic DNS Support[3]

Cyberoam adds Dynamic DNS (DDNS) support to map Cyberoam's dynamic WAN IP address to a static hostname/domain name. DDNS servers supported include:

- dyndns.org
- zoneedit.org
- easydns.com
- OrgDNS.org
- dnspark.org

With introduction of this feature now it is possible to manage Cyberoam remotely.

3. FTP Scanning Support for Anti Virus[4]

Now one can configure anti virus protection for FTP protocol also in addition to HTTP, IMAP, POP3, and SMTP protocols

To review and analyze the FTP activities on your network, the Cyberoam now provides two FTP activity reports – User wise FTP data transfer and FTP virus report.

Note:

Make sure FTP server supports passive mode before enabling FTP scanning

[2] ***See High Availability Configuration Guide 9402-1.0-03/11/2006 for more information***
[3] ***See User Guide (Document Version 9402-1.0-18/10/2006 page number 148) for more information***
[4] ***See Cyberoam Anti Virus Implementation Guide (Document Version 9402-1.0-18/10/2006 page number 23) for more information***

4. CPU Burn test

To help administrators check the appliance hardware health, CPU Burn test is included in the Appliance itself.

5. Protection against next generation Pharming attacks[5]

Option has been added in HTTP proxy configuration to enable protection against pharming attacks. If protection is enabled, users are directed to the legitimate web sites instead of fraudulent web sites.

6. HTTP Proxy[6]

Cyberoam can now be configured as an HTTP proxy to provide Content filtering and Anti Virus scanning.

[5] ***See User Guide (Document Version 9402-1.0-18/10/2006 page number 175) for more information***
[6] ***See Cyberoam Anti Virus Implementation (Document Version 9402-1.0-18/10/2006 page number 25) Guide for more information***

Enhancements

1. ActiveX, Cookie and Java Applet Content Filtering[7]

Cyberoam's Web and application filtering feature is extended to include the ability to block ActiveX, Cookie and Java Applet for improved access control and enhanced network security and performance.

For this, 3 new web categories are added:

- Active X
- Cookie
- Applets

2. RADIUS authentication[8]

User Authentication capability has been extended to include RADIUS authentication.

3. Custom signature support for IDP[9]

Custom signatures provide the flexibility to customize IDP for diverse network environments. Now it is possible to create custom signatures, in case proprietary server, custom protocol, or specialized applications are being used in the corporate network. This ability allows the administrator to define custom IDP signatures for his own network.

4. SMTP Authentication

Cyberoam Gateway Anti Virus now supports SMTP Auth clients. In addition, it now honors SMTP Auth by not tagging SMTP authenticated mails as spam.

5. Dynamic IP support

Cyberoam Firewall NAT and DNAT rules can now handle Interfaces that are allocated IP addresses dynamically via DHCP provided they configured using Port or Interface based hosts.

6. VPN enhancements

1. Utility to export Road Warrior connection configuration file[10]

   To reduce the problems of incorrect configuration due to lack of information or wrong information passed to the remote user, Cyberoam now provides a convenient method to auto-create and export configuration file for distributing to the remote users. File is created in .tgb format which can be directly imported in Cyberoam VPN client.

   Configuration file includes Gateway IP address/host name, Local and Remote Ids, Preshared key, Certificates.

2. Generate Certificate in unencrypted form

   To reduce the task of Certificate conversion (from p12 to PEM format), now Cyberoam generates certificate in unencrypted format which can directly uploaded at the VPN client end.

---

[7] ***See User Guide (Document Version 9402-1.0-18/10/2006 page number 241) for more information***
[8] ***See RADIUS Integration Guide (Document Version 9402-1.0-18/10/2006) for more information***
[9] ***See Cyberoam IDP Implementation Guide (Document Version 9402-1.0-18/10/2006 page number 16) for more information***
[10] ***See Cyberoam VPN Management Guide (Document Version 9402-1.0-18/10/2006 page number 51) for more information***

2. Domain name support for VPN end points

Cyberoam VPN end points can now be defined as Domain names instead of IP addresses

7. Diagnostic Tool[11]

Diagnostic Tool now has the capabilities to diagnose further error conditions like Anti Virus Scanning by displaying the status of various proxy server and logs.

8. Updated SSL (HTTPS) security

SSL certificate used for HTTPS is now Self-signed.

9. Enhanced Web Admin Console[12]

Functionality to restart Anti Virus and Anti Spam Engines provided in Web Admin Console.

10. FTP reports

To review and analyze the FTP activities on your network, the Cyberoam now provides FTP reports which can be access from Dashboard.

11. HTTP Proxy support for Chinese characters in URL

Cyberoam will now allow URLs containing Chinese language characters.

[11] ***See Cyberoam Analytical Tool Guide** (Document Version 9402-1.0-18/10/2006 page number 8) for more information*

[12] ***See Cyberoam User Guide** (Document Version 9402-1.0-18/10/2006 page number 176) for more information*

Bugs fixes

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.

Defect ID – 1833

Defect Description - Cycle Hours field displayed without compulsory field label i.e. without *, in Create Surfing Quota policy page.

Defect ID - 1858

Defect Description - Page title not displayed after updating personal details from User My account page.

Defect ID – 1851

Defect Description - Change Policy page displayed without Page header while changing the Surfing Quota policy from Edit Group page.

Defect ID - 1859

Defect Description - 'Wrong Password' error page displayed without Page header when trying to change password. 'NO' button was not operational in Change Password Confirmation message. Password was changed even after clicking 'NO' button.

Defect ID – 1874

Defect Description – 'Select All' button not working on Address Group(s) page and is displayed even when one Address Group is defined.

Defect ID - 1989

Defect Description - The sequence of columns in the SMTP and POP spam reports displayed in Web Admin Console and CSV form was different.

Defect ID - 1992

Defect Description - User wise Traffic discovery reports did not display user name in the report title.

Bug ID – 1996

Description – Firewall rule blocks application protocols even if 'Web and Application Filter' module is not subscribed.

Defect ID - 1999

Defect Description – Cyberoam allowed specifying port number greater then 65536 in Mail Server Port field while configuring Antivirus Mail General Configuration.

Defect ID – 2015

Defect Description

- Duplicate Host Group name error page displayed without Page header while creating Host Group with the same name
- Duplicate Group name error page displayed without Page header while creating Group with the same name
- Duplicate Service/ Service Group name error page displayed without Page header while creating Service with the same name
- Duplicate SNAT Policy name error page displayed without Page header while creating SNAT policy with the same name
- Duplicate DNAT Policy name error page displayed without Page header while creating DNAT policy with the same name
- Duplicate Policy name error page displayed without Page header while creating Data transfer policy with the same name

Defect ID – 2017

Defect Description - Duplicate Address Group name error page displayed without Page header while creating address group with the same name and does not specify the address group type.

Defect ID – 2019

Defect Description - Duplicate Group name error page displayed without Page header while creating Group with the same name.

Defect ID - 2020

Defect Description - Add Multiple Clientless user page wrongly displayed field names as 'Host group' instead of 'Logon Pool'.

Defect ID - 2029

Defect Description – Periodic Data in Anti Virus Mail Summary report displayed blank page.

Defect ID - 2032

Defect Description - 'Blocked Categories by number of Attempts' report displayed header with wrong spelling 'Cateogory' instead of 'Category'.

Defect ID - 2033

Defect Description – HTTP Access log link from DG tool displayed blank page of log details.

Bug ID – 2034

Description – DNAT rule fails when firewall rule is created for Service using multiple ports.

Bug ID – 2041

Description – Cyberoam does not display Category in the Blocked Category report mailed to the Administrator.

Bug ID – 2068

Description – Cyberoam fails to include the Category name information in the Blocked Category report mailed to the Administrator.

Bug ID – 2070

Description – Cyberoam failed to enforce the Drop Firewall rule when proxy server is configured from Browser and allows Internet access without authentication.

Defect ID - 2074

Defect Description - Page header was not displayed after changing password from Edit User page.

Defect ID - 2103

Defect Description - General Configuration page wrongly displayed field tip as 'Enter 0 for default size restriction of 10MB' instead of 'Enter 10MB for no size restriction'.

Bug ID – 2108

Description – Cyberoam failed to accept infrequent subnet mask while configuring network using Network Configuration Wizard. For example 255.255.254.0

Bug ID – 2118

Description – Manage Live User page failed to display the Client IP address when user logs in after proxy settings. Page displayed Proxy IP address instead of Client IP address in the user information.

When the user re-logs in after removing proxy settings, Cyberoam fails to remove the previous entry and displays two entries with the different IP addresses (one entry with Proxy IP address and one with Client IP address) for the same user on Manage Live User page.

Defect ID - 2123

Defect Description – Cyberoam failed to block WAN to Local interface HTTP connections when HTTP is denied from local ACL and DNAT port forward firewall rule is applied.

Defect ID - 2126

Defect Description – Online help of General Configuration page wrongly displayed Anti Virus signatures database update time as 3 hrs instead of 30 minutes.

Bug ID – 2149

Description – Cyberoam fails to enforce Internet Access policy when Proxy is configured.

Bug ID – 2153

Description – Ping, traceroute and arp ping commands executed from the Telnet Console failed to display all the configured interfaces. All Commands display the information of 8 interfaces only.

Bug ID – 2183, 2207

Description – Cyberoam fails to display Custom Signature menu before subscribing Intrusion Detection & Prevention (IDP) module.

Defect ID - 2197

Defect Description - Mail Client displayed 'Timeout error' whenever Cyberoam was not able to download mails before the default timeout of Mail Client due to slow link speed between Cyberoam and POP3 server. This happened if anti virus scanning was enabled.

Defect ID - 2195

Defect Description – Port forward rule failed when HTTP scanning is enabled.

Defect ID - 2198

Defect Description - SMTP proxy crashed when Cyberoam attempted to scan mails received with certain types and number of attachments.

Bug ID – 2202

Description – Executing 'show log all by ipaddress' fails to display the logs for the matching IP address. For example 'show log all by ipaddress 192.168.20.1' displays logs for IPs 192.168.1.10, 192.168.1.21, 192.168.1.199, 192.168.21.19 also.

Bug ID – 2205

Description – Cyberoam fails to block web surfing even if ALLWebTraffic category is denied from Internet Access policy.

Bug ID – 2233

Description – After upgrading from 9204 to 9400, Cyberoam fails to display Remote ID value. Value is not displayed even after clicking Update button on Connection page.

Defect ID - 2288

Defect Description – Disk full problem occurred when the Alert logs generated by IDP Engine exceeds predefined size.

Defect ID - 2289

Defect Description – Mail displays wrong sender's email address in Mail Backup.

Defect ID - 2294

Defect Description – VPN L2TP connections gets disconnected after every 15 minutes.

Discontinued Feature

DNS configuration option from Telnet Console.

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
- Telephone number : +91-79-26400707

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

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