

Contents

Introduction	2
Version 9.5.3.14.....	2
Release Information	2
Features.....	2
1. Quarantine Area for Spam emails.....	2
2. Active Directory (AD) groups import wizard	2
3. Multicast Forwarding	3
4. HTML Editor to customize HTTP Client page	3
Enhancements.....	3
1. Virtual Host.....	3
2. Active Directory Group Search Order	3
3. HTTP Proxy Performance Statistics and session capture	3
4. DHCP leased IP list.....	4
Renamed Feature.....	4
Obsolete Feature.....	4
Version 9.5.2 build 19	5
Features.....	5
1. FQDN for Parent Proxy server	5
2. Configurable Gateway failover detection time (only for Multiple Gateway)	5
3. High Availability (HA) with Load balancing and failover protection.....	5
Version 9.5.2 build 15	6
Features.....	6
1. Regulatory Compliance Reports	6
Enhancements.....	6
1. Performance Enhancements for better support multi-Core and multi-processor appliances.....	6
2. IDP alerts over Syslog.....	6
3. Ability to switch on/off traffic discovery report	6
4. HTTP Keep-Alive Support.....	6
5. Extended SNMP Traps support	6
6. DHCP client support for "DNS server" parameter.....	7
Bugs solved.....	8
Bugs solved in 9.5.3 build 14.....	8
Bugs solved in 9.5.3 build 07.....	8
Bugs solved in 9.5.2 build 15.....	11
General Information.....	12

Introduction

This document contains the release notes for Cyberoam version 9.5.3 build 14 and the two intermediate builds - 9.5.2 build 19 and 9.5.2 build 15. The intermediate builds were distributed to the beta customers only and now as an part of this release are made available to all the customers.

This is a major release with new features and enhancements in response to several bug fixes that improves quality, reliability, and performance.

The following sections describe the release in detail and provide other information that supplements the main documentation.

Version 9.5.3.14

Release Information

Upgrade applicable to: version 9.4.2.0 onwards

Upgrade Information

Upgrade type: Manual upgrade.

Upgrade procedure

1. Download upgrade from <http://downloads.cyberoam.com>
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

Features

1. Quarantine Area for Spam emails

Cyberoam appliance now provides a spam quarantine folder for each user where it stores the quarantined spam mail sent to the user's email address. The user can view the quarantined emails from the user my account page and download the email.

The global quarantine area can also be accessed by the appliance administrator to download the quarantined emails.

Quarantine can be configured as an SMTP action in the spam policies. Currently quarantine support is available only for the SMTP protocol.

2. Active Directory (AD) groups import wizard

Cyberoam Web Admin Console now includes the "Active Directory Group Import Wizard" that allows to import groups from Active Directory. The Wizard can be accessed from User → Authentication setting page of Web Admin Console. You can also define different Cyberoam policies for the imported groups using this wizard.

3. Multicast Forwarding

Cyberoam can now support applications like stock ticker that multicast stock quote information.

Multicast support includes:

- Multicast forwarding (for both Gateway and Bridge modes)
- Configuring static routes (for Gateway mode only)

Telnet Console provides the option to configure multicast static routes when Cyberoam is deployed in Gateway mode. Router Management menu changes:

- Sub menu – Configure Unicast Routing includes previous version's option for unicast dynamic routing configuration
- Sub menu - Configure Multicast Routing

4. HTML Editor to customize HTTP Client page

HTML Editor is provided to customize GUI components of the HTTP client login page.

The Editor also supports customization in 24 different languages including Hindi.

The Default template can be accessed from the System menu of Web Admin Console.

Enhancements

1. Virtual Host

Till previous versions, 3 different steps were required to provide access of servers hosted in the LAN segment of Cyberoam to WAN. One was required to define alias, DNAT policy and firewall rule for each server.

Virtual host has been designed to overcome this shortcoming. Virtual Host will map services of a public IP address to services on an internal host and will be used as the Destination address to access internal server. Proxy ARP is automatically enabled for the respective virtual host so that the Cyberoam can respond to ARP requests for public IP address.

SNAT policy is renamed to NAT policy and one needs to assign only the NAT policy to the Firewall rule to provide the outbound access for any of the internal servers.

Telnet Console can be used for managing Proxy ARP manually.

2. Active Directory Group Search Order

The Cyberoam administrator can now define the Group Search Order for Active Directory users who are part of multiple groups.

Cyberoam would decide the group membership of the authenticated users based this group search order. Based on the group membership the respective access control policies would be applied on the users.

3. HTTP Proxy Performance Statistics and session capture

The "HTTP Proxy Statistics" link in the Cyberoam Diagnostic Tool provides real-time outputs of various statistics about proxy configuration and performance.

Some key information and statistics provided by this tool are:

- DNS request time
- Total HTTP requests served by number and data transfer
- Failed requests
- Live session information

The live session information provides an in-depth view with a detailed time wise breakup of various actions by the proxy. In addition the HTTP session information can be captured and downloaded as a file to aid in further troubleshooting and performance tuning if required.

The information available in the HTTP session capture is:

- HTTP Request Headers
- HTTP Response Headers
- Proxy tasks statistics

4. DHCP leased IP list

The DHCP server now gives a list of IP addresses that have been leased to DHCP clients.

The following information is available in the leased IP list:

- Leased IP address
- Lease start and end time
- Physical address of Client
- Client host name

Renamed Feature

SNAT (Source NAT policy) is renamed to NAT policy

Obsolete Feature

DNAT policy

Version 9.5.2 build 19

Following features were made available to the beta customers only and were release candidate for testing purpose. From this version onwards, as an part of v 9.5.3 build 14, all the features are now made generally available.

Features

1. FQDN for Parent Proxy server

Now FQDN or IP address can be configured for Parent Proxy server. This will help service provider in load balancing and failover.

2. Configurable Gateway failover detection time (only for Multiple Gateway)

One can now configure the time interval for checking the health of the gateway link. It can be configured from Manage Gateway page of the Web Admin Console.

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

In previous version, this feature was enabled only on demand but from this version onwards, this control has been removed. This feature should be considered as Beta from this version. It will be communicated when HA feature will be made generally available in the subsequent builds on further deployments on the field.

Version 9.5.2 build 15

Following features were made available to the beta customers only and were release candidate for testing purpose. From this version onwards, as an part of v 9.5.3 build 14, all the features are now made generally available.

Features

1. Regulatory Compliance Reports

The Cyberoam On Appliance Reports suite has been expanded to include approximately 45 reports for SOX, HIPPA, PCI, FISMA and GLBA compliance.

Enhancements

1. Performance Enhancements for better support multi-Core and multi-processor appliances

The Cyberoam operating system and applications have been tuned to better support the Cyberoam appliances with multi processor and multi core CPUs.

Performance improvement of 20% to 50% has been achieved for policy scanning and IDP, especially in the 1000i and 1500i appliances

2. IDP alerts over Syslog

It is now possible to log IDP alerts to remote syslog servers.

IDP reports are the most performance intensive reports on the appliance, thus being one of the key factors affecting the appliance real time performance.

This feature gives an option to the Cyberoam administrator to choose between on appliance logging, Syslog logging or disabling logging totally. By default on-appliance logging and reporting would be disabled after applying this upgrade.

It will aid in fine tuning Cyberoam's on-appliance features in high traffic environments without compromising Appliance features as well as performance.

3. Ability to switch on/off traffic discovery report

Traffic discovery reports can now be turned off.

4. HTTP Keep-Alive Support

HTTP proxy now supports HTTP Keep-Alive thus allowing persistent connections. This can provide up to 50% speedup in latency times for web pages with lots of components. E.g. lots of images

5. Extended SNMP Traps support

Cyberoam generates SNMP traps for the following SNMP Get events:

Traps	Description
highCpuUsage	High CPU usage i.e. CPU usage exceed 90%

highDiskUsage	High Disk usage i.e. Disk usage exceed 90%
highMemUsage	High Memory usage i.e. memory usage exceed 90%
httpVirus	HTTP virus detected by Cyberoam
smtpVirus	SMTP virus detected by Cyberoam
pop3Virus	POP3 virus detected by Cyberoam
imap4Virus	IMAP virus detected by Cyberoam
ftpVirus	FTP virus detected by Cyberoam
linkToggle	Change of link status (up or down)
synFlood	DoS attack – SYN flood detected by Cyberoam
tcpFlood	DoS attack – TCP flood detected by Cyberoam
udpFlood	DoS attack – UDP flood detected by Cyberoam
icmpFlood	DoS attack – ICMP flood detected by Cyberoam

6. DHCP client support for “DNS server” parameter

Cyberoam DHCP client now uses the "DNS Server" configuration parameter obtained from the DHCP Server. This parameter would override any DNS Server configured manually on the Cyberoam appliance.

Bugs solved

The purpose of this list is to give an overview of the bugs fixed in various builds of version 9.5.3, 9.5.2.15. The ID denotes the internal Cyberoam bug tracking ID and the description explains problem.

Bugs solved in 9.5.3 build 14

Bug ID – 2088

Description – SFP ports I and J are not displayed on Web Admin Console and Network Configuration wizard for Cyberoam 1000i and 1500i Appliances.

Bug ID – 2157

Description – VPN Client cannot be registered from any of the LAN machines behind Cyberoam.

Bug ID – 2201

Description – Create Firewall rule page in Web Admin Console displays incomplete IP address (Source and Destination) and bandwidth policy name.

Bug ID – 2338

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

Bug ID – 4266

Description – Cyberoam deletes previously created ARP entry if ARP entry for the same IP address is added manually from Telnet console. In other words, ARP entry created on creation of Virtual host gets deleted if ARP entry for the same IP address is added manually from Telnet console.

Bug ID – 4365

Description – Import Group Wizard prompts to select Internet Access Policy even if policy is selected while importing AD Groups. This happened only if “Allow All” Internet Access policy.

Bugs solved in 9.5.3 build 07

Bug ID – 2411

Description – When Cyberoam is deployed as Bridge, Traffic discovery incorrectly displays that all the connections are initiated from WAN interface.

Bug ID – 2425

Description – For clientless users, web Surfing report displays duplicate entries - one with the username and another with the IP address.

Bug ID – 2789

Description – Bandwidth usage statistics displayed on Manage Live User page in Web

Admin Console does not consistently display the correct values. Sometimes it is displayed as 0.0 K bandwidth usage. The exact configuration parameters that trigger this situation are not known.

Workaround – Restart management services from Telnet Console.

Bug ID – 2932

Description – IDP module triggers high CPU usage if Cyberoam is under attack. As a workaround, enable DoS attack from Web Admin console.

Bug ID – 2935

Description – “Root partition full” problem is faced when Cyberoam is under attack due to temporary files generated by Traffic Discovery module.

Bug ID – 3478

Description – Spelling mistake in the auto-generated message send to the Administrator on the change of Gateway status.

Bug ID – 3522

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

Bug ID – 3560

Description – Cyberoam displays junk characters in HTTP Virus Alert text.

Bug ID – 3565

Description – Cyberoam does not add disclaimer or signature in outgoing mails if specified in Anti Virus General Configuration.

Bug ID – 3602

Description – Even when “User Authentication Session Timeout” and “Timeout session after” fields are not mandatory, it is not possible to create group if any value is not specified. If the fields were kept empty, “Cannot create a group” error message is displayed.

Work around – At the time of creating a Group, configure any value in these fields. After successful creation of the group, edit the group to remove these configured values.

Bug ID – 3607

Description – Cyberoam displays error page without page header when duplicate Group is created.

Bug ID – 3614

Description – Mail Recipients specified in Anti Virus General Configuration are not able to extract the mail attachment.

Bug ID – 3615

Description – FTP Configuration page of Web Admin Console does not provide any information on file size restriction for virus scanning of FTP traffic.

Bug ID – 3619

Description – If spam scanning is disabled from custom policy, default spam policy is also not applied.

Bug ID – 3710

Description – Secure sites (HTTPS) could not be accessed when Parent proxy is configured.

Bug ID – 3736

Description – Anti spam logs were not generated.

Versions Affected – 9.5.0 build 19 onwards

Bug ID – 3745

Description – FTP logs were not generated from Telnet Console.

Bug ID – 3747

Description – IDP Signatures update status is displayed as “Fail” even after successful updation.

Bug ID – 3752

Description – Cyberoam Routing table does not get updated when RIP (Routing Information Protocol) is configured.

Bug ID – 3757

Description – Customized Dashboard display is not retained on logout.

Bug ID – 3844

Description – Error 999 was displayed while trying to access certain sites like tw.stock.yahoo.com, tw.news.yahoo.com when HTTP scanning is enabled.

Bug ID – 3847

Description – “Proxy unable to comply” error is displayed at the time of enabling FTP scanning when Cyberoam is deployed as bridge.

Bug ID – 4018

Description – Cyberoam allowed to update IP address of the WAN Interface acting as DHCP server from Manage Interface page of Web Admin Console.

Bug ID – 4024

Description – Virus name is displayed in the Recent Mail Virus detected alert on Dashboard includes junk character.

Bug ID – 4150

Description – Cyberoam automatically changes its default MTU value of WAN interface if external DHCP server leases MTU. Due to this, Internet becomes inaccessible.

Bug ID – 4156

Description – If the Alias and LAN interface subnet are not same, Alias is added but is not visible Authentication Network. Due to this, user logon requests were dropped.

Bug ID – 4169

Description – Special character white space is not supported between network ID and subnet mask in IP address based Address Group. For example, **192.168.15.15**
255.255.255.255

Address groups are used in defining scanning rules.

Bugs solved in 9.5.2 build 15

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 – 4017

Description – Cyberoam could not detect and filter spam mails if email address specified in Mime Header included special characters like *, # etc.

Bug ID – 4019

Description – Not able to regularly rotate L2TP VPN logs. It is necessary to rotate logs in order to control the log size.

Bug ID – 4020

Description – Cyberoam does not synchronize static route when High Availability cluster is configured with Virtual Interfaces.

Bug ID – 4027

Description – Secure sites (HTTPS) could not be accessed when Browser HTTPS proxy is configured.

Bug ID – 4056

Description – Dashboard SMTP virus alerts includes invalid characters in the Virus name. This is a browser specific problem faced only when Internet Explorer V 6 browser is used to access Web Admin console.

Bug ID – 4060

Description – VPN connection cannot be established when endpoints are assigned dynamic IP addresses or FQDNs.

Bug ID – 4061

Description – Cyberoam Appliance models 1000i and 1500i did not display fiber ports I and J on Network configuration Wizard.

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