

Release Information

Compatible versions: 9.5.3 build 14 onwards

Upgrade Information

Upgrade type: Manual upgrade

Upgrade procedure

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

Compatibility Issues: None

Contents

Release Information	1
Introduction	3
Features	3
1. Filter HTTPS traffic based on Domain names	3
2. Multiple Syslog server support.....	3
3. Support BGP protocol for Dynamic Routing	3
4. HTTP upload report.....	4
Enhancements	5
1. Optimization of Startup time.....	5
2. Support Asymmetric routing environment.....	5
3. Multiple Active directory support.....	5
4. Configurable action for Mid-stream TCP connections	5
5. VLAN tags preservation in bridge mode for scanned traffic	5
6. Spam detection performance improvements	6
7. Support multiple Host Group membership.....	6
8. Dependency of restarting management services removed	6
9. Ability to switch on/off traffic discovery history log.....	6
10. Utility to monitor dropped packets	6
11. Visibility to Spyware infected computers on Dashboard	6
12. CLI console improvements	7
13. Dashboard Alert message on failure to apply Firewall rule.....	8
14. Configurable action for ICMP error message tracking	8
Behavior information	8

Discontinued Feature	8
Bugs solved.....	9
General Information	20
Technical Assistance.....	20
Technical Support Documents	20

Introduction

This document contains the Release Notes for Cyberoam version **9.5.4 build 66**. The following sections describe the release information in detail and provide other information that supplements the main documentation.

This is a performance and maintenance release in response to bug reports and beta version feedback that improves quality, reliability, and performance with significant enhancements.

Features

1. Filter HTTPS traffic based on Domain names

Cyberoam now filters HTTPS traffic based on Domain names using site Certificates.

Most of the content filtering solutions can detect and block the websites accessed over the HTTP protocol. To bypass these kinds of solutions, users use URL Translation or HTTP proxy websites hosted on HTTPS to access blocked sites. With this development, Cyberoam would be able to block these kinds of attempts to bypass the web content filter and sites hosted on SSL.

Protocols supported - SSLv2, SSLv3 and TLS

Certificate supported – X.509

By default, this option is enabled and can be disabled from Internet Access policy (IAP). Access denied message will not be displayed when access is denied.

2. Multiple Syslog server support

Cyberoam now supports multiple syslog server for remote logging. One needs to configure the facility, severity and log file format for syslog servers and logging location if multiple syslog servers are configured.

Maximum 5 syslog servers can be defined from Logs Configuration page of Web Admin Console.

Apart from firewall and Intrusion Detection and Prevention (IDP) logs, Cyberoam now also supports logging of following activities on syslog server:

- AntiVirus
- AntiSpam
- Content Filtering
- Traffic Discovery

Except for Traffic discovery logs, all the logs can be stored on the syslog server also.

Logging of various activities to syslog server can be enabled or disabled from the Logs Configuration page of Web Admin Console.

3. Support BGP protocol for Dynamic Routing

Cyberoam now supports Border Gateway Protocol (BGP) for dynamic routing.

BGP is a path vector protocol that is used to carry routing between routers that are in the different administrative domains (Autonomous Systems) e.g. BGP is typically used by ISPs to exchange routing information between different ISP networks.

Cyberoam has implemented BGP version 4 as described in RFC 1771. Additionally, RFC 1997 (Communities Attribute), RFC 2796 (Route Reflection), RFC 2858 (Multiprotocol extensions) and RFC 2842 (Capabilities Advertisement) are also supported.

CLI Console provides the Cisco compliant CLI for routing configuration. Additionally, a firewall rule is to be configured for the zone for which the BGP traffic is to be allowed i.e. LAN to LOCAL or WAN to LOCAL.

4. HTTP upload report

Cyberoam Web Surfing report now provides details of HTTP upload activity carried out by each user. The following information will be available from the report:

- User name / IP address
- URL
- File name and size

Enhancements

1. Optimization of Startup time

Startup time is reduced by approximate 35% to 45% across various models. This was achieved by performing some maintenance tasks like re-arranging booting sequence, removing obsolete files. But Cyberoam may take time to startup if goes down abruptly e.g. after power failure.

2. Support Asymmetric routing environment

Cyberoam being a stateful firewall, tracks the traffic connection state. Due to this, Cyberoam drops the packets if both the outbound and return packets do not traverse through Cyberoam.

In asymmetric routing environments, only outbound or return packets are seen by Cyberoam. Up till previous versions, it was not possible to deploy Cyberoam in such environments.

Administrator can now configure source and destination host or network tuple from which such traffic is to be allowed from CLI console.

By default, Cyberoam will drop the packets if both the outbound and return packets do not traverse through Cyberoam. Use "set advanced-firewall-bypass-stateful-firewal-config" command to set such networks.

3. Multiple Active directory support

Cyberoam now supports configuration of multiple Active Directory servers for user authentication. Cyberoam can be configured to authenticate users via HTTP client or Single Sign on Client. To logon using HTTP Client, users are required to specify user name along with the domain name.

4. Configurable action for Mid-stream TCP connections

Cyberoam can now be configured to pick up TCP connections in mid stream. Enabling midstream pickup of TCP connections will help while plugging in the Cyberoam appliance as a bridge in a live network without any loss of service. It can also be used for handling network behavior due to peculiar network design and configuration. E.g. atypical routing configurations leading to ICMP redirect messages.

The configuration can be done via the "set advanced-firewall midstream_connection_pickup" command option in the CLI Console.

By default, Cyberoam is configured to drop all untracked (mid-stream session) TCP connections in both the deployment modes.

5. VLAN tags preservation in bridge mode for scanned traffic

From this version onwards, VLAN (Virtual LAN) tags will be preserved even when antivirus scanning, spam filtering and web filtering using Internet Access Policy (IAP) are applied to VLAN tagged traffic in Bridge mode.

In the earlier versions, VLAN tags were not preserved when scanning or Internet Access Policy was applied on the traffic.

By default Cyberoam will not preserve VLAN tag. Please refer to the Cyberoam Console Guide on

how to support VLAN tags.

6. Spam detection performance improvements

- Enhanced image-spam detection algorithms
 - Optimized operation by fine-tuning parameters to improve performance and to save bandwidth
 - Improved detection of spam and malware in nested messages
 - Add HTTP connection pooling between the Anti Spam Engine and the Anti Spam Center
- Improved local caching and classification performance

7. Support multiple Host Group membership

Cyberoam now supports membership of single host in multiple host groups.

8. Dependency of restarting management services removed

It is now not required to restart management services (RMS) for the following actions:

- defining Network in Auth Network¹
- subscribing any of the modules
- enabling or disabling any of the System modules

9. Ability to switch on/off traffic discovery history log

Traffic discovery history log can now be turned off from the Configure Autopurge Utility page of Web Admin Console.

If logging is enabled, then one can also specify number of days up to which logs should be retained. For example, if you specify 5 days, on the 6th day, the logs of the first day will be removed.

By default, logs are retained for 7 days.

10. Utility to monitor dropped packets

A Packet dump command is added on the CLI console to help Administrators view dropped packets. It will provide connection details and details on which module is dropping packets e.g. firewall, IDP along with information like firewall rule number, user, Internet Access policy number etc. This will help Cyberoam administrators to troubleshoot errant firewall rules.

Use CLI command “packet-capture” to generate the packet dump. Refer to Cyberoam Console Guide for details.

11. Visibility to Spyware infected computers on Dashboard

“Recent Spyware Alerts” - doclet is added on the Dashboard to provide an instant visibility to spyware infected hosts. Alert provides username to help identify the spyware infected computer and take the immediate corrective action.

¹ RMS is required after adding a superset range for an existing subnet range

Cyberoam constantly monitors and provides alert on the Dashboard on detecting spyware and also blocks Spyware “phone-home” traffic and other related backdoor traffic. Dashboard alert will be provided if any applications, laptops or desktops are secretly phoning home.

Cyberoam detects “phone-home” traffic with IDP signature.

12. CLI console improvements

- Show network interface will now display interface information as per the Cyberoam nomenclature e.g. Port A, Port B instead of eth0, eth1
- MTU can now also be configured when Cyberoam appliance is configured in transparent mode
- MTU and MSS values can now be configured from the Cyberoam Console option (set network command) and Cyberoam will now automatically configure MSS value on enabling PPPoE on the WAN interface. MTU and MSS configuration option from Network Configuration menu has been removed.
- Cyberoam Console option – “set network interface” command now allows configuration for the physical interfaces only. In case Cyberoam is deployed in transparent mode, only one interface would be available for configuration. In the earlier versions, Cyberoam displayed all the Ethernet interfaces including alias, ipsec and lo.
- Following HTTP proxy commands are added

Command	Description	Default value
set http_proxy av_session	No. of files scanned simultaneously	20 Allowed range:1 to 64
set http_proxy dns_threads	No. of simultaneous DNS requests that can be handled by Proxy server	5 Allowed range: 1 to 128 One may need to increase when Cyberoam is used as Proxy server or DNS response time is high (when DNS server is responding slowly)
set http_proxy client_session	No. of simultaneous client session	1024 Allowed range: 1024 to 8192 One may need to increase when DNS server is responding slowly or number of simultaneous requests are high
set http_proxy rw_buffer_size	Size of read/write buffer	4 Kbytes Allows range: 1 to 16 Kbytes One can increase in-case of high speed WAN link.
set http_proxy x_forwarded-For	Include/Exclude X-Forwarded-For header information from outbound HTTP requests	OFF Applicable only in transparent mode.
set http_proxy deny_unknown_proto	Allow/deny traffic not following HTTPS protocol i.e. invalid traffic through HTTPS port	YES

set http_proxy debug	Run proxy in debug mode	OFF
set http_proxy core_dump	Generate dump	OFF

13. Dashboard Alert message on failure to apply Firewall rule

Cyberoam will now display Alert messages on Dashboard incase Cyberoam fails to apply any of the firewall rule on RMS (Restart Management Service), appliance reboot, or after adding, deleting or updating firewall rule. Message will prompt to "Rebuild Firewall state" from CLI console.

14. Configurable action for ICMP error message tracking

In the earlier versions, in-case of ICMP error, by default, Cyberoam deleted existing connection from its internal connection state.

This option can now be disabled from the "Advanced firewall" command from CLI Console.

Behavior information

- Web Surfing logs can be retained for 365 days instead of 60 days
- HA failover timeout is increased to 3 seconds. In earlier version failover used to happen instantly so now it will wait for 3 second.
- When HA failover occurs, all the sessions transferred to Auxiliary will timeout in 5 minutes if no traffic is seen on a particular connection.
- When Cyberoam is deployed in transparent mode and is used as a direct proxy, LAN to WAN or WAN to LAN firewall rule is to be defined.
- For PPPoE connections, LCP echo request and reply can be disabled by setting LCP Interval and LCP Failure as zero from the Manage Interface page of Web Admin Console.
- After disabling HA, network configuration will be preserved on Auxiliary appliance. Till previous versions, factory defaults were restored on Auxiliary appliance on disabling HA. After disabling HA, to remove Auxiliary appliance from the cluster and use independently, reset HA from Auxiliary appliance and change IP schema through Network Configuration Wizard.
- Report are not synchronized when HA is configured.
- Cyberoam will now automatically reboot on kernel crash. Till previous versions, Administrator had to manually restart the system.

Discontinued Feature

High Availability from CR25i Appliances

Bugs solved

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

Bug ID – 2322

Description – When same network is specified as local and remote network in Connection, VPN tunnel is not establish.

Bug ID – 2336

Description - Allowing Application categories or file type categories in “Deny All” Internet Access policy does not work. From the current version onwards, support to allow Application category in “Deny All”, Internet Access policy is removed.

Bug ID - 2437

When Cyberoam is deployed in transparent mode, Manage Gateway page on the Web Admin Console displays incorrect Ethernet Port IP address.

Bug ID – 3315

Description – DHCP server does not lease IP address from the secondary interface when two LAN interfaces are configured.

Bug ID – 3476

Description – When no matching URL is found as per the search criteria, the “Search URL” option of Web category displays incorrect message.

Bug ID – 3549

Description – Cyberoam does not detect spam mails if parent proxy is configured.

Bug ID – 3934

Description – If a DHCP service is configured on the Interface Alias, DHCP server is not able to lease IP address. From the current version onwards, one will not be able to enable DHCP server on Alias IP Interface

Bug ID - 3942

Description - If “Restrict HTTP Upload” category is denied, users are not able to send mails using Gmail. Instead of blocking the messages with attachment, user is denied the access to Gmail itself.

Bug ID - 4157

Description - Even when Anti virus scanning is disabled in the Firewall rule, HTTP Live session statistics display AV scan time as 1 second

Bug ID - 4159

Description - Mismatch in AV scan time displayed on Captured Connection page and "Search Captured Sessions" page of HTTP Statistics when AV scanning disabled.

Bug ID - 4276

Description – Web Surfing reports display User name as "Unknown" if user tries to download virus when Cyberoam is configured as HTTP Proxy.

Bug ID – 4179

Description – Even when custom login and logoff messages are configured, instead of custom login and logoff messages, Cyberoam displays default messages.

Bug ID – 4325

Description – After changing default HTTP proxy port, web surfing reports are not generated.

Bug ID - 4345

Description - Priority level 4 is not displayed in Bandwidth policy

Bug ID - 4414

Description – HA synchronization process does not synchronize BGP configuration

Bug ID - 4415

Description – Cyberoam allows to configure (add and delete) BGP routes from the Auxiliary appliance of HA cluster.

Bug ID - 4430

Description – If SSH communication on the dedicated link fails, synchronization process remains incomplete. Due to this, Configure HA page displays primary appliance as Active and auxiliary as a stand-alone appliance even when HA is enabled.

Bug ID - 4441

Description – It is possible to configure static routes from Auxiliary appliance of HA cluster.

Bug ID - 4455

Description – Incorrect message "Applicable for primary node only when both nodes are UP" is displayed when HA load balancing is disabled from Auxiliary appliance (CLI console).

Bug ID - 4457

Description - L2TP tunnel gets disconnected while copying file

Bug ID - 4466

Description - It was possible to create multiple VPN connections with the same subnet configured for Remote LAN network.

Bug ID – 4490

Description – Due to incorrect HTTP header parsing, certain sites like www.cada.fr were not accessible.

Bug ID - 4493

Description - Yahoo messenger disconnects frequently when parent proxy is configured.

Bug ID - 4494

Description – Even when gateway is not reachable, Dashboard displays gateway status as reachable.

Bug ID - 4511

Description – Change in Administrator Email id for Anti virus and Antispam notifications from Web Admin console is not reflected on CLI Console.

Bug ID - 4519

Description – Cyberoam allows to configure file size threshold as zero for HTTP scanning. Cyberoam does not scan files when file size threshold is configured as zero.

Bug ID - 4522

Description – Incomplete virus name is displayed in "Recent FTP Viruses detected" section of Dashboard

Bug ID – 4525

Description – HTTP downloads fail with AV scanning and transfer-encoding is set to chunk. Due to this, websites like <http://www.anindakapinda.com> failed to open.

Bug ID - 4526

Description – Custom Web category cannot be created if HTTP Proxy is not running.

Bug ID - 4536

Description – Cross model appliance backup cannot be restored.

Bug ID - 4553

Description - When Cyberoam is configured as a DHCP client on the WAN interface, Cyberoam Gateway becomes unreachable at times. This happens because; when Cyberoam DHCP client on the WAN interfaces failed to fetch the IP address from the ISP DHCP server it does not retry again leading to loss of Internet connectivity. It was necessary to restart management services (RMS) for Cyberoam DHCP client to request again. Cyberoam DHCP client is now updated and will keep on retrying until it receives IP address from the ISP DHCP server.

Bug ID - 4567

Description – In Active-Passive HA cluster, if HA is disabled while synchronization process is going on, cluster becomes unstable.

Bug ID - 4572

Description – Backup of v 7.4.2.x cannot be restored on v 9.5.4.xx

Bug ID - 4574

Description – Incorrect proxy status is displayed on Web Admin console.

Bug ID - 4604

Description – When HTTPS Categorization (from Internet Access policy) is enabled in transparent mode, users are not able to access secure (HTTPS) sites.

Bug ID - 4605

Description – When Cyberoam is deployed in transparent mode, after changing the default HTTP port one could not access Web Admin Console.

Bug ID - 4616

Description – Sometimes "NULL" is displayed as Category name in "Top 10 Categories (by Hits)" web surfing report when Cyberoam is configured in transparent mode.

Bug ID – 4618

Description – User wise Web Surfing report displays junk characters in IP address column

Bug ID - 4625

Description – In an Active-Passive HA cluster, deleting VPN connection on the Primary appliance does not delete connection from the Auxiliary appliance.

Bug ID - 4633

Description – SMTP Email scanning rule names can include special characters like !@\$

Bug ID - 4634

Description – "From Email Address" field accepts invalid email address in the Spam policy

Bug ID - 4635

Description – When action defined for spam mail is "Prefix Subject" and MIME header filter contains a comma (,), Cyberoam forwards scanned mails without adding prefix to the original subject.

Bug ID - 4643

Description – After failover in Active-Passive HA Cluster, it is not possible to establish Certificate based Net-to-Net VPN connections.

Bug ID - 4645

Description – Manage Group page displayed "Data Transfer Policy Bean" (incorrect spelling) instead of "Data Transfer Policy Name"

Bug ID - 4644

Description – CLI Console command "cyberoam service status" gives following error and does not generate a Debug log file. This situation occurs only if log file generation command is executed when Cyberoam is writing log records to a log file.

Error:

```
tar: cyberoam_tomcat.log: file changed as we read it
```

```
tar: Error exit delayed from previous errors
```

Bug ID - 4651

Description - In Active-Passive HA cluster, after changing any network configuration from CLI console (Option 1 Network Configuration), all the logged in users on Primary appliance do not get logged in automatically on Auxiliary appliance.

Bug ID - 4655

Description – When Cyberoam upgrade is applied after System date is updated to the current date, Web UI upgrades are not applied. This situation occurs only when system date was by mistake configured to some future date.

Bug ID - 4678

Description – Cyberoam does not preserve Syslog configuration on upgrading from V 9.3.0 build 09 to V 9.5.3 build 18. Hence, one has to re-configure Syslog after upgrading.

Bug ID - 4664

Description - When Cyberoam is configured as DHCP Client, Cyberoam does not forward the IP lease request to DHCP server if not leased on the initial request.

Bug ID – 4665

Description – When HTTP scanning is enabled in Real mode, browser hangs while accessing following sites: <http://tw.movie.yahoo.com>, <http://www.ipower.com/support>, <http://ctworld.org.tw>

Bug ID – 4667

Description – Cyberoam failed to display virus alerts on Dashboard and generate Syslog report in high traffic environment.

Bug ID – 4681

Description – An invalid URL can be configured as a Home page from Custom Client Preferences page of Web Admin console.

Bug ID – 4682

Description – An invalid IP address can be configured for Syslog server from Manage Syslog page of Web Admin console.

Bug ID – 4688

Description – Syslog configuration is not included in backup.

Bug ID – 4689

Description – Update successful confirmation message is not displayed after updating log configuration from Logs Configuration page.

Bug ID – 4694

Description – In Active-Passive cluster, cluster becomes unstable when multiple events occur simultaneously e.g. dedicated link status changes during the failover process,

Bug ID – 4697

Description – Warning or Update successful confirmation message is not displayed when IDP engine status changes or signature database is updated successfully.

Bug ID – 4700

Description – No validation is performed on email addresses configured in Bypass Email Ids page for Reports.

Bug ID – 4701

Description – If port number 2812 is not free, java does not load.

Bug ID – 4703

Description – Save operation does not ask for confirmation before saving the Login restriction changes from the Change Group IP restriction page (Web Admin Console).

Bug ID – 4704

Description – When user is allowed login from specific nodes, Edit Group page does not display login nodes details.

Bug ID – 4705

Description – After adding IP address for login restriction, Change Group IP Restriction page is displayed without header

Bug ID - 4730

Description – When the report END DATE is selected as current date for Appliance Audit log and Event log Cyberoam does not generate logs nor displays the Error message.

Bug ID – 4732

Description - When both Parent proxy and DDNS are configured, it is not possible to access the Cyberoam appliance using FQDN (hostname). This is because; proxy IP address is forwarded to DDNS instead of WAN IP address of Cyberoam.

Bug ID - 4735

Description - VPN Client always disables NAT-T parameter irrespective of the configuration imported from Cyberoam.

Bug ID – 4758

Description - When an Appliance configured with VLAN and Alias, is configured as an Auxiliary appliance in Active-Passive HA cluster, Cyberoam does not remove VLAN and Alias configuration.

Bug ID – 4748

Description – Title bar displays incorrect title for all the Compliance reports.

Bug ID – 4773

Description – Administrator receives “root partition full” error mail when an IDP alert file becomes full and the update or delete operation is not completed.

Bug ID – 4784

Description – It is not possible to remove PPPoE interface using Network Configuration Wizard.

Bug ID - 4785

Description – Cyberoam incorrectly allowed to update the gateway IP address of PPPoE-enabled interface from Web Admin Console.

Bug ID - 4786

Description – Cyberoam incorrectly allowed to update the gateway IP address of DHCP-enabled WAN interface from Web Admin Console.

Bug ID – 4790

Description – When “Video” file type attachment is blocked, Cyberoam blocks both “Video” and “Image” file type attachments.

Bug ID – 4793

Description – Cyberoam allows white space in the “Timeout session after” field while creating Group.

Bug ID – 4794

Description – Cyberoam allows to specify Web Admin console port value as a decimal number. Due to this, Web Admin console becomes inaccessible.

Bug ID – 4807

Description – After customizing contents of the HTTP client page, it is not possible to save the user password.

Bug ID - 4813

Description – Special character Hyphen is not accepted as a part of Dynamic DNS host name.

Bug ID – 4814

Description – Anti Spam General Configuration page displays incorrect status of Cyberoam Anti Spam Center.

Bug ID – 4816

Description – VPN connection running on static IP Address fails to get activated,

Bug ID – 4820

Description – When any of the Cyberoam interface is configured as Virtual host, IP address of the Virtual host does not change automatically if changed through Network Configuration wizard.

Bug ID – 4821

Description – User session timeout does not work as expected.

Bug ID – 4822

Description – Explicitly added route for DHCP-enabled interface is removed after running Network Configuration Wizard.

Bug ID - 4831

Description - Custom HTTP Client login page does not display vertical scroll bar when page contents cannot be displayed on single screen.

Bug ID – 4833

Description – When WAN port is configured as DHCP client, Gateway failover condition does not work.

Bug ID - 4853

Description – After restarting management services or rebooting Cyberoam, VPN service does not start if DHCP server is not able to lease IP address to the WAN Interface.

Bug ID - 4856

Description – When the contents of customized HTTP client page do not fit on a single page, scroll bar is not displayed and as a result users are not able to view the entire contents.

Bug ID - 4899

Description – When Cyberoam is configured in transparent mode, the Gateway IP address cannot be changed.

Bug ID - 4880

Description – Changes in grouped Services are not reflected in Service Group.

Bug ID - 4901

Description – After restarting management services from Primary appliance of Active-Passive cluster, Auxiliary appliance can not be accessed with Auxiliary Administration IP.

Bug ID – 4904

Description – It is possible to create Custom File Type category with multiple file extensions specified on multiple rows using <Enter>

Bug ID - 4906

Description – When HTTP port is configured on any of the reserved port like 3128, 8007, 8384, 8088, 8090, 9001, Web Admin console becomes inaccessible.

Bug ID – 4907

Description – It is possible to create Internet Access policy with the name including all the special

character like @ # \$%. Now Cyberoam will allow only alphanumeric characters, space and underscore (_) in the Internet Access policy name.

Bug ID – 4921

Description – Traffic discovery module cannot handle packet size greater than 2048 bytes. Due to this, packets were dropped.

Bug ID – 4925

Description – It is not possible to update the weight of the PPPoE gateway.

Bug ID – 4944

Description – Tip for configuring minimum and maximum days for log retention is not displayed on the Configure Auto Purge Utility page.

Bug ID - 4972

Description – If an Appliance configured with DHCP is configured as an Auxiliary appliance in Active-Passive HA cluster, Cyberoam does not remove DHCP configuration from the appliance.

Bug ID – 4984

Description – Quarantine Spam mails are not displayed in User My Account.

Bug ID – 4986

Description – Pie-chart for Daily and weekly proactive reports is not generated when there is no data to populate the graph. Due to this, Proactive reports are mailed without any proper message.

Bug ID – 4988

Description – HTTP Proxy sends multiple IP Address information when IP lookup sites/tools e.g. www.whatismyipaddress.com, returns multiple IP Addresses.

Bug ID – 4991

Description – Port forward rule for Virtual host fails when more than 30 ports are included in the port range.

Bug ID – 5005

Description – HTTP File Upload report provides option of viewing report in graphically format even when it is not possible.

Bug ID – 5006

Description - In case of Password Change event, action column of Audit log displays “Null” instead of the action description.

Bug ID – 5008

Description – When data for Data Transfer Report by User (Internet Usage>By User) spans over multiple pages, “Next” button is displayed but does not work.

Bug ID – 5055

Description – In case of multiple gateways, Cyberoam sends multiple email alerts of gateway status even when gateway status is not changed,

Bug ID – 5065

Description - When virus scanning is enabled, Rediffmail website does not open.

Bug ID – 5074

Description – At the time of creating or updating group, if "%" is included in group name, a Java error is displayed.

Bug ID – 5083

Description - If "Enter" is used as a separator between the extensions of file types to be blocked in Create Custom Web Category, the category becomes ineffectual.

Bug ID - 5113

Description - FTP server restarts due to assertion failure.

With Windows FTP client, Cyberoam now will give "Proxy unable to comply" message instead of restarting proxy, if server closes the connection before the process is complete.

Bug ID – 5164

Description – Certain events are not logged in IDP logs due to segmentation fault.

Bug ID – 5213

Description - Parent proxy configuration is retained even after disabling the parent proxy setting from Configure HTTP Proxy page of Web Admin Console.

Bug ID – 5219

Description – HA could not be configured due to improper configuration of HA service.

Bug ID – 5227

Description – Anti-virus engine does not start after upgrading to version 9.5.4 build 55

Bug ID – 5233

Description – Latency observed when one tries to log on to CLI console due to reverse IP address lookup.

Bug ID – 5246

Description – Cyberoam does not detect ICMP flood as per the configuration.

Bug ID – 5260

Description – Help option is removed from the Main page as it opened an obsolete page.

Bug ID - 5264

Description – HA synchronization process does not synchronize Local ACL

Bug ID – 5274

Description – Cyberoam supported only 25 characters for PPPoE username. Now it supports 60 characters.

Bug ID – 5278

Description – POP, IMAP and FTP proxy restarts frequently under heavy traffic.

Bug ID - 5282

Description - FTP Proxy hangs if session is terminated by FTP Client before file transfer process is complete.

Bug ID – 5286

Description – As DNS server could not resolve the cached name query, users were not able to access the Internet.

Bug ID - 5290

Description - User My Account Quarantine Mail reports incorrectly displays Spam mails detected by POP/IMAP proxy as Quarantine mails.

Bug ID – 5291

Description – When the Cyberoam appliance is not activated, on logging to Web Admin Console “Menu not defined” error is given.

Bug ID – 5293

Description – Only last 7 days quarantined mails were displayed in Quarantine report as well as in Self Service Quarantine area (User My Account). Due to this, there is data mismatch in Quarantine report and Quarantine utilization area.

Bug ID - 5295

Description – FTP client hangs after it receives negative response from FTP server. This behavior is observed only when the initial response of FTP server is positive.

Bug ID – 5297

Description – When HTTP scanning is enabled and Internet Access policy is configured, Yahoo mail attachment can not be send. This behavior is observed only with Internet Explorer 6.

Bug ID – 5309

Description – Due to header parsing problem, HTTP Proxy restarts.

Bug ID – 5330

Description – HA synchronization process does not synchronize date and time setting if updated from Network Configuration Wizard.

Bug ID – 5363

Description – “Disable Autostart” button does not work for DHCP server and Domain Name server.

Bug ID – 5364

Description – Firewall rule fails when virtual host is configured as Destination host and action is configured as DROP.

Bug ID - 5365

Description – After updating IDP category, one needs to restart IDP daemon manually from Web Admin console.

Bug ID - 5366

Description – ARP entry for Virtual host can not be deleted from CLI console.

Bug ID – 5367

Description – When Cyberoam is configured in transparent mode, Interface speed can not be configured.

Bug ID – 5368

Description – After changing the default port of HTTP proxy, BGP and HA cannot be configured.

Bug ID - 5369

Description - On restarting management services (RMS), PPPoE client is killed.

Bug ID – 5370

Description – Cyberoam will not classify traffic pattern even after enabling Traffic Discovery module if Traffic discovery module is disabled at the time of upgrading Cyberoam. This behavior is observed when Cyberoam is upgraded to version 9.5.4 build 55

Bug ID – 5371

Description – When HTTP proxy is configured on non-standard port, HTTP proxy does not work after restoring backup.

Bug ID – 5372

Description – Cyberoam crashes due to race condition in VPN services.

Bug ID - 5373

Description – MSS value is not retained after running Network Configuration Wizard.

Bug ID – 5374

Description – VPN connections can not be deleted after the VPN module is disabled from System Modules page of Web Admin console.

Bug ID – 5375

Description – At the time of enabling HA, sometimes both the Appliances in HA cluster respond to the ARP request.

Bug ID – 5376

Description – After HA failover, IP address added in Proxy ARP does not work as expected.

Bug ID – 5377

Description – Proxy ARP does not work after restoring backup on a different appliance, but works if backup is restored on same appliance.

Bug ID – 5378

Description – When Cyberoam DHCP client on the WAN interfaces fails to fetch the IP address from the ISP DHCP server, Interface based Virtual host does not work.

Bug ID – 5384

Description – Rules based on Custom Application Protocol category does not work as expected.

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 supplied 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