Release Dates

Version 9.6.0 Build 78 – 24th February, 2010
Version 9.6.0 Build 76 – 19th January, 2010
Version 9.6.0 Build 62 – 24th November, 2009
Version 9.6.0 Build 60 – 2nd October, 2009
Version 9.6.0 Build 34 – 4th July, 2009
Version 9.6.0 Build 30 – 26th June, 2009
Version 9.6.0 Build 16 – 30th April, 2009

Release Information

Release type: GA

Compatible versions: 9.5.3 build 14 onwards

Upgrade requirement (only for the versions below 9.6): 24 X 7 or 8 X 5 valid Support License, IPS Signature Database v 2.4.27 or higher

Upgrade Information

Upgrade type: Manual upgrade

Upgrade procedure

1. Download upgrade from http://downloads.cyberoam.com
2. Log on to Cyberoam Web Admin console
3. Go to menu IPS > Manage IPS and check the IPS Signature Database version. If database version is lower than v 2.4.27, upgrade the version.
4. Go to menu Help> Upload Upgrade and upload the file downloaded in step 1
5. Once the file is uploaded successfully, log on to CLI console and go to menu “Option 6 Upgrade Version” and follow the on-screen instructions.

Compatibility Issues: Upgrade not applicable for CR15i appliances

Contents

Introduction

This document contains the release notes for Cyberoam version **9.6**. The following sections describe the release in detail.

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

Features & Enhancements

Build 76

1. DHCP Server Logs

For monitoring and troubleshooting the DHCP lease traffic, Logging functionality is extended to include DHCP Server events log. With the inclusion of DHCP Server log, Cyberoam can now log following different network activities and traffic including: overall network traffic i.e. firewall and traffic discovery, IPS anomaly and signature, anti virus - URL and mails blocked, spam filtering and content filtering - access allowed and blocked.

The DHCP event log contains events that are associated with activities of the DHCP service and DHCP server, such as DHCP leases, renewal and expiry.

By default, DHCP server log is disabled and can be enabled from Logs Configuration page of Web Admin console. Logs can be forwarded to Syslog server but cannot be stored on the Appliance.

For details on log event ID and description, refer to User Guide, Appendix B.

2. NAT support for Cyberoam initiated Outbound traffic

Now it is possible to configure source NAT i.e. specific IP address for the outbound traffic initiated by Cyberoam itself e.g. upgrade traffic.

This is useful is network environments where Cyberoam is hosted behind ISP and ISP is leasing private IP address to Cyberoam i.e. private IP address is configured on WAN interface.

CLI command “set advanced-firewall cr-traffic-nat” is added for configuring the source NAT.

3. Configurable Mailing frequency of Proactive reports

Mailing frequency of the Proactive reports can now be configured. Prior to this version, reports were mailed at the predefined time.

Administrator can configure time and day for the daily and weekly reports respectively from the Reports Notification page.

4. Secure Access for Web Client

Web client can be now accessed through a secure channel i.e. HTTPS access of the Web Client login page. When enabled, user can logon to the Web Client page through a secure channel using:

https://<IP Address>: 8090.

By default, it is disabled and can be enabled from the Customize Client Preferences page of Web Admin console.

5. Simplified User Login Restriction Configuration

Build 74 now supports adding range of IP addresses for Node restriction in one go. Prior to this, one had to specify multiple IP addresses one-by-one that became a tedious administration task incase of restricting more number of nodes.

With this functionality, one has to specify just the starting IP address of the required range and total number of IP addresses.

This functionality will be useful in network environments where administrator requires restricting user login from multiple nodes.

User and Group pages of Web Admin console are updated for these changes.

Build 60

1. SSL VPN - Threat Free Tunneling for Full Access mode

Threat Free Tunneling feature is extended to SSL VPN traffic i.e. firewall rules can now be applied to the SSL VPN traffic also. As a result, SSL VPN traffic can be subjected to viruses, spam, intrusion attempts, inappropriate web content and unwanted network applications scanning.

From now on, VPN zone firewall rules will be applicable to SSL VPN (connections established through Full Access) besides IPSec, L2TP and PPTP traffic.

There are no Web Admin or CLI console changes for this feature.

2. SSL VPN - User based Certificate support for Authentication

The current feature of authenticating all the users through single System wide certificate is extended one step further to provide an option of authenticating through individual user certificates also. These certificates not only provide granular control in Certificate management but also create a user identity which can be used beyond SSL VPN implementation.

Certificates for all the users added in Cyberoam are generated automatically.

It is a Web Admin console feature available from submenu “Global Settings” of “SSL VPN” menu.

One can configure either common certificate or individual certificate authentication. By default, authentication through common certificate is configured.

3. SSL VPN - HTTP/SOCKS Proxy support for Clients

The SSL VPN functionality is extended to the SSL VPN Clients who are not able to access the Internet directly by providing an option to configure HTTP or SOCKS proxy server.

Proxy can be configured from the SSL VPN Client's Proxy Setting menu.

By default, proxy is not enabled but one can use proxy configured in the Browser - Internet Explorer or can configure manually.

4. SSL VPN – Single-Click Client Installer

Installation process has been optimized as a single step process. It is not required to import the configuration separately, as it is now a part of the installation itself. This makes installation and re-installation of SSL VPN client easier.

The Client Configuration needs to be downloaded and imported only when the server settings are changed.

The installer is available as Bundled SSL VPN Client from SSL VPN End User Portal under "Full Access mode".

5. SSL VPN - Two factor Authentication solution

To enhance password security and reduce the risk posed by weak user passwords for SSL VPN user, Cyberoam has extended its authentication solution by providing 2 factor authentication with One time password (OTP) through external authentication server RADIUS and LDAP.

All the hardware and software token generating Agents that can communicate with RADIUS and LDAP are supported.

Build 30

1. Parent Proxy Authentication

The parent proxy feature is extended to include the authentication parameters. This feature will be helpful in the deployment where parent proxy is configured to ask for authentication before serving the requests. For example, Head office and Branch office deployment where parent proxy is deployed at Head office and configure for authentication and Cyberoam is deployed at branch office.

2. Beta Feature -Turkish language support for Web Admin Console

To cater to the Turkish speaking customer, Cyberoam has added support of turkish language in Web Admin console. Following elements of Web Admin Console will be displayed in Turkish:

- Dashboard Alerts
- Dashboard contents
- Navigation menus
- Screen elements including field labels and tips

- Error messages

It would also be possible to provide description for firewall rule, various policies, services and various custom categories in Turkish language.

This feature should be considered as **Beta** from this version. It will be communicated when feature will be made generally available in the subsequent builds.

Build 16

1. SSL VPN within Cyberoam Appliance

The VPN feature is extended to include SSL VPN functionality within Cyberoam to provide secure access for the remote users. It delivers set of features and benefits to make them easier to use and control to allow access to the Corporate network from anywhere, anytime.

Cyberoam SSL VPN is platform, device and location independent as it supports site-to-site and road warrior tunneling. It offers granular access policies, bookmarks to designated network resources and portal customization.

Two operational modes are provided:

Web access mode allows remote users to access Enterprise Web applications/servers just the Web browser through an End-user Web Portal and without the need of any additional Client. Cyberoam authenticates the users and redirects to the End-user Web Portal through which Enterprise Web applications/servers can be accessed.

In Full access mode remote users requires the SSL VPN Client for access. The mode is ideal when Corporate network is to be accessed from Internet cafes, hotels etc.

Full access mode can provide full as well as split tunneling. Split tunneling ensures that only the traffic for the private network is tunneled and encrypted while in full tunneling private network traffic as well as other Internet traffic is also tunneled and encrypted.

Further, it is also possible to restrict the access to the certain hosts of the private network. User's access to private network is controlled through his SSL VPN policy while Internet access is controlled through his Internet Access policy. SSL VPN policy of the user can be configured at the time of adding user or later whenever required.

As End-user Web Portal is an entry point to the Corporate network, it is possible to customize the portal interface by including company logo and a customized message to be displayed to users when they log in to the portal to access network resources.

Compatible Browsers: Microsoft Internet Explorer 6.0, Mozilla/Firefox 1.5

Supported Clients: Windows

Default settings:

- Full access mode enabled and can be disabled from SSL VPN Policy
- SSL VPN as a Network Services enabled for all the zones except VPN zone and can be disabled from Local ACL.

End-user Web Portal Access

Browse to https://<WAN IP address of Cyberoam:port>

Default port: 8443

SSL VPN Client & Configuration Download Path

End-user Web Portal

Feature available in Web Admin console as menu “SSL VPN” and few fine-tuning and troubleshooting commands are added CLI console. Refer to Console guide for details.

2. Category based Bandwidth Allocation

Unmanaged bandwidth leads to poor productivity due to delay in critical applications and sometimes even lost opportunities. Hence, now Cyberoam also allows allocating bandwidth based on the Web category apart from allocating and prioritizing bandwidth based on users. It will not only improve the network productivity by limiting the bandwidth used by the recreational applications but also guarantees the performance of the critical business application.

To achieve high degree of network utilization and fairness, Cyberoam:

- Classifies traffic based on Web Category
- Provides differentiated bandwidth based on the Web Category under which the URL is categorized.

A Web Admin feature implemented through Bandwidth policy, Web Category and Firewall rule. When configured, bandwidth will be applicable, whenever the URL falling under the Web category is accessed.

3. MAC and IP-MAC filtering

To improve the security of the network, now one can enable MAC address filtering. By enabling “MAC Filtering”, Cyberoam will drop the packets received from all the MAC addresses not configured in the “Trusted MAC address” list.

Using MAC address filtering makes it more difficult for a hacker using random MAC addresses or spoofing a MAC address to gain access to your network as the traffic does not even reach firewall.

Similarly, it is also possible to filter packets based on IP-MAC pair. Feature prevents hosts which try to violate trusted IP-MAC pair. For this, Administrator has to configure the list of trusted MAC address and bind with IP address.

When IP spoofing is enabled, Cyberoam will reverse lookup for the route and if not available will log and drop the packets.

One can even enable restriction on zones for granular restriction.

A Web Admin console feature available as submenu “Spoof Prevention” of “Firewall” menu

4. ARP Poisoning Control

ARP poisoning is a layer-2 attack, where the attacker sends spoofed ARP packets to the network, with a purpose of advertising its own MAC address for some IP address that does not belong to the attacker’s host. In this way, the attacker makes the devices in the LAN to send the Ethernet frames to the attacker instead of the intended destination. Generally the ARP poisoning is used to capture all traffic intended for the default gateway or other important IP address, such as a server.

Cyberoam provides a protection from this poisoning by associating IP address, MAC address and Port and storing this association as a Static ARP entry. Whenever ARP packets arrive on the Interface, Cyberoam will check the ARP entries and considers it as an attack if mismatch is found. If it is an attack, Static ARP entry will not be updated and logged.

A Web Admin console feature available as submenu “ARP” of “System” menu

5. Cyberoam Transparent Authentication Suite – Clientless SSO

From this version onwards, Cyberoam introduces clientless Single Sign On as a Cyberoam Transparent Authentication Suite (CTAS).

With Single Sign On authentication, user automatically logs on to the Cyberoam when he logs on to Windows through his windows username and password. Hence, eliminating the need of multiple logins and username & passwords.

But, Clientless Single Sign On not only eliminates the need to remember multiple passwords – Windows and Cyberoam, it also eliminates the installation of SSO clients on each workstation. Hence, delivering high ease-of-use to end-users, higher levels of security in addition to lowering operational costs involved in client installation.

CTAS Download path

http://www.cyberoam.com/clientless_sso.html

6. Layer 2 Firewall support

The Firewall feature is extended to include MAC address to provide secure access. It means now, access to the internal resources can be granted based on the MAC address.

Till previous versions, firewall rules were created based on source and destination IP addresses services and user identity but now they can be created based on MAC address also.

A Web Admin console feature available in “Add” page of “Host” submenu and implemented through a MAC based Firewall rule.

7. L2TP and PPTP VPN traffic scanning support

Till previous versions, it was not possible to apply firewall rules to the L2TP and PPTP VPN traffic and due to this, such traffic was not scanned. This resulted into unprotected VPN traffic.

Now, threat free tunneling i.e. scanning for viruses, spam, intrusion attempts, inappropriate web content and unwanted network applications is extended to the L2TP and PPTP traffic also. Hence, firewall rules can be applied even to the L2TP and PPTP VPN traffic resulting into the clean VPN traffic.

Hence from this version onwards, VPN zone firewall rules will be applicable to the IPSec, L2TP and PPTP traffic.

There are no Web Admin or CLI console changes for this feature.

8. DHCP Relay support

With DHCP, clients send requests to locate the DHCP server(s) using broadcast messages. However, broadcasts are normally only propagated across the local network. This means if DHCP server and client are not on the same physical network, they will not be able to communicate.

To solve this problem, Cyberoam can now be configured as a DHCP Relay Agent which acts as a link between the client and the remote DHCP server. Cyberoam intercepts internal client's DHCP requests and relays to the pre-configured DHCP server. The server then responds to the Cyberoam which in-turn forwards the response to the client.

If DHCP Relay Agent is not configured, clients would only be able to obtain IP addresses from the DHCP server which is on the same subnet.

A Web Admin feature available as submenu "DHCP Relay" of menu "Configure Network"

At a time, Cyberoam can either act as a Relay agent or an IP leasing agent i.e. DHCP server. Hence, if server is configured, one will not be allowed to configure relay agent and vice-versa.

9. Spam Digest support

The Spam Digest is an e-mail message that will be received by administrator and/or users. The digest with the listing of all the quarantined messages is mailed to the user as per the configured frequency. It will contain hyperlink to MyAccounts page where user can login and manage his quarantined mails.

A Web Admin console feature available as submenu "Spam Digest Setting" of "Anti Spam" menu.

Prerequisite - "Gateway Anti-Spam" module subscribed.

10. "Release" Action for False positive or Quarantined Spam mails

Now, Quarantined spam mail can be released to the intended recipient. Administrator can release the mail from the Quarantine area (AntiSpam → Configuration → General Configuration) while user can release from his my account page (Quarantine Mails → Spam).

Till previous version, it was not possible to release the spam mail to the intended recipient.

11. "IP Reputation" – additional layer for Spam filtering

Cyberoam has now added an "IP reputation" layer for email filtering to its existing Anti spam detection technology along with the Recurrent Pattern Detection technology.

It dynamically classifies and reclassifies the reputation of each source IP and maintains a database of addresses used spammers and legitimate mailers.

It fights the unwanted mail at the perimeter, reducing the incoming spam messages at the entry-point, before these messages enter the network resulting into reduced system resources and bandwidth usage.

A Web Admin console feature available as “Verify Sender’s IP reputation” in “General Configuration” page of “Anti Spam” menu. If enabled, Cyberoam dynamically checks the sender IP address and rejects the SMTP connection if IP address is found to be responsible for sending spam mails.

As it is a global option, if spam scanning is enabled, all the mails will be first subjected to IP reputation filtering followed by filtering based on actions configured in spam policy.

At the time of v 9.6 upgrade, if the Gateway Anti Spam module is already subscribed, the option will not be visible on the Web Admin console. But, if upgrade is applied on the trial version of the Gateway Anti Spam module, the option will be displayed.

To use the feature, one has to purchase a new license of Gateway Anti Spam module and re-subscribe the module with the new key. Subscribing with the new key will allow to filter spam mailed based on IP reputation as well as RPD (recurrent pattern technology) technology.

12. RBL-based Spam filtering without Anti Spam License

Cyberoam detects spam mails based on:

- RBL (Realtime Blackhole List)
- Mass distribution pattern using **RPD (Recurrent Pattern Detection) technology**

Till previous versions, to use any of the above specified methods, a valid license for “Gateway Anti Spam” module was required.

But now, RBL-based spam filtering can implemented without subscribing to “Gateway Anti Spam” module. By implementing, only the RBL-based filtering, chances of receiving more number of false-positives cannot be ruled out.

There is no Web Admin or CLI console change for this feature.

13. Full tunnel support for IPSec VPN

With full tunnel support, entire branch office Internet traffic can be routed through a single gateway. This type of configuration is needed for head office (HO) and branch office (BO) networks where the entire branch office Internet traffic is to be routed through gateway of HO i.e. the access to the Internet for BO is provided through HO.

Additionally, there are minimal chances of branch office network compromise as traffic to the destination will always appear to originate from the gateway of the head office irrespective to its actual origin i.e. branch or head office.

Again as entire traffic traverses through HO, administrator can define the access policy in HO to control and monitor traffic centrally from Cyberoam deployed at HO.

It can be implemented simply by configuring 0.0.0.0 as local and remote network respectively in VPN policy for head office and branch office.

There is no Web Admin or CLI console change for this feature.

14. French language support for Web Admin Console

To cater to the French speaking customer, Cyberoam has added support of French language in Web Admin console. Following elements of Web Admin Console will be displayed in French:

- Dashboard Alerts
- Dashboard contents
- Navigation menus
- Screen elements including field labels and tips
- Error messages

It would also be possible to provide description for firewall rule, various policies, services and various custom categories in French language.

Behavior change

Build 16

LAN Bypass

By default, LAN Bypass will be enabled and hence whenever Cyberoam gets rebooted or halted manually, Cyberoam will automatically go in bypass mode. Once the system is rebooted successfully, traffic will flow normally.

LAN Bypass can be disabled from CLI console.

LAN Bypass is supported only when Cyberoam is deployed in transparent mode and for CR500i, CR1000i and CR1500i appliances.

Anti Spam

Anti spam General Configuration for SMTP connections' spam checking - "Enforce Anti Spam policies for SMTP Authenticated Connections" is renamed as "Bypass Spam check for SMTP authenticated connections".

As a default behavior, SMTP authenticated connections will now be bypassed from RBL and RPD based spam checking.

Miscellaneous changes

Build 74

1. Manage Live Users page – 'Bandwidth' column is renamed as 'Data Transfer Rate'.

Build 60

1. SIP (Session Initiation Protocol) - signaling protocol support which enables the controlling of media communications such as VOIP. Support is added in the form of System module which can be enabled when required from Web Admin Console, System Modules Configuration page.
2. SSL VPN connections can be disconnected from "Manage Live SSL VPN Users" page
3. CLI command "set http_proxy multiple-webcategory" is added to enable categorization of a single URL into multiple Web Categories. Command can be executed from Option 4 Cyberoam Console. By enabling this categorization, Bug ID 1168 of categorization can be solved.
4. Option to configure HTTP Download file size limit is provided on Web Admin Console from Internet Access Policy.
5. To reduce the support calls on how to retrieve Customer Account details - email address and password if forgotten, Forgot Email Address and Forgot Password links are provided on Add On Modules Subscription page of Web Admin Console.

Build 30

1. Following CLI command added (Menu Option 4. Cyberoam Console)

- To set the link bandwidth i.e. bandwidth provided by Service Provider and can be used as "set bandwidth max-limit <number>" and to view the configured limit, use the command "show bandwidth max-limit". Default=100mbps
- To enforce bandwidth restriction on the traffic on which the bandwidth policy is not applied so that guaranteed bandwidth is available to the users to whom the guaranteed

bandwidth policy is applied, configure “set bandwidth guarantee enforced”.

- If guarantee is enforced, default bandwidth policy will be applicable to the traffic on which bandwidth policy is not applied. You can set the guaranteed and burstable bandwidth and priority on this traffic. This bandwidth is applicable on Internal (LAN and DMZ) to External zone (WAN and VPN) traffic and External to Internal zone traffic. Default Guaranteed bandwidth = 0 kbps, Burstable bandwidth = max-limit, priority = 7 (lowest). Guaranteed and burstable bandwidth can be defined as “set bandwidth default-policy guaranteed <number> burstable <number> priority <number>”
- If you do not want to enforce the bandwidth restriction on the traffic on which the bandwidth policy is not applied, configure “set bandwidth guarantee lenient”.
- To view the default policy configuration, use “show bandwidth default-policy”

Build 16

1. Certificate Management is now the part of System Management.
2. DHCP server can now be configured on all the Internal Interfaces i.e. LAN and DMZ
3. For a single Interface, it is now possible to configure multiple dynamic IP address range.

Known Behavior

Build 30

1. Link Bandwidth configuration - It will take approximately 5 minutes for the link bandwidth value to be effective.

Discontinued Feature

Build 16

- Logon Pool from Web Admin Console - As logon pool is a collection of IP addresses of Authenticated Networks, instead of creating them separately, Authentication network nodes are now provided directly on the configuration pages whenever required. For example, in “Add User” page, under “Login Restriction”, one can type Authenticated Networks IP address directly. Deployments where logon pool is configured will not have to do any configuration changes.
- CLI Console command to set number of simultaneous DNS requests that can be handled by Proxy server i.e. set http_proxy dns_threads (Menu Option 4. Cyberoam Console)
- CLI console – Menu Option 5. Cyberoam Management, Option 15. Logging Management and its submenu Option 5.15.1 Network Logging Management
- CLI console - Option to restore backup of v 7.4.2.x from (Menu Option 5. Cyberoam Management, Option 16. Restore Backup of Version 7.4.2.x)

Bugs solved

Build 78

Backup & Restore

Bug ID – 2067

Description – Backup and restore process takes long time, as incorrect report tables were included in backup.

HA

Bug ID – 1505

Description – When one of the nodes in HA cluster gets rebooted, both the nodes get deactivated. This happens only when either of the cluster node is CR50ia or CR100ia models.

Bug ID – 2066

Description – HA failover takes long time as incorrect report tables were synchronized.

Proxy

Bug ID – 2905

Description – Due to assertion failure, proxy connection breaks.

Build 76

Anti Spam

Bug ID – 1973

Description – Contents of Quarantine Mails page of My Account are not displayed in web browser - IE version 6 and 8.

Backup and Restore

Bug ID – 895

Description – When backup of appliance configured in HA is restored on a single appliance i.e. not configured in HA, Anti spam server does not start

Group

Bug ID – 1885

Description – Even after changing the user group, previous user group policies are applied. This situation observed for CTAS user only.

IPS

Bug ID – 1915

Description – It is not possible to change the default action "detect" of certain IPS signatures of Web Access category. This is observed when one tries to change the action of all or the individual signatures in the category.

Reports

Bug ID – 1510

Description – In Data transfer reports, total monthly data transfer exceeds the sum of the daily data transfer.

Bug ID – 1693

Description – When the report flows through multiple pages, instead of including all the records in CSV report file, only those records which are displayed on the current page are included. For example, if report has 200 records but on the current page only 50 records are displayed than the CVS file contains only 50 records.

Bug ID – 1908

Description – Column headings of the Reports in CSV format displays HTML tag information.

SSL VPN

Bug ID - 1761

Description - In case of external certificate, SSL VPN connection cannot be established if the user does not have SSL Client certificate i.e. user needs certificate with "client support".

System

Bug ID – 269

Description – NTP Client when installed, CPU performance is affected due to high CPU utilization by NTP Client.

Bug ID – 1781

Description – DHCP Lease Type cannot be changed from dynamic to static and vice versa for the same IP addresses.

For example, after configuring static lease type with IP address 10.8.5.29, lease type cannot be changed to dynamic with lease range 10.8.5.1 – 10.8.5.50.

User

Bug ID – 1055

Description – SSO client user session is not getting disconnected after the configured session timeout. User login time automatically gets changed every 3 minutes and due to this, session start time (login time) of the live user is changed to the current time.

Bug ID – 1172

Description – User authentication session does not timeout at the configured time.

Bug ID – 1666

Description – If the user is configured in the External authentication server as well as Cyberoam then instead of External server, Cyberoam authenticates the user. This situation occurs only when CHAP authentication is configured for PPTP connections.

Bug ID – 1953

Description – When deactivated, Single Sign On (SSO) live user gets deactivated only at next login. Ideally, user should get deactivated immediately.

VPN

Bug ID – 1944

Description – Net-to-Net VPN connections for the WAN port for which the gateway is not configured cannot be activated.

Bug ID – 1964

Description – All the Cyberoam users even when they are not allowed to access through PPTP, can establish PPTP connection. Ideally, only those Cyberoam users who are allowed access through PPTP should be able to establish PPTP connection.

Web Admin console

Bug ID – 1659

Description – In the Chinese GUI, on the User > User Add user page, the User Type drop-down lists the same options.

Bug ID – 1896

Description – At the time of creating custom Web category, it is possible to add foreign language keywords in category name.

Bug ID - 1958

Description - When Cyberoam Central Console (CCC) pushes the already existing firewall rule again in Cyberoam, Manage firewall page of Cyberoam displays only the recently pushed rule and does not display any other firewall rules.

Build 62

HA

Bug ID – 1505

Description – When one of the nodes in HA cluster gets rebooted, both the nodes get deactivated. This happens only when either of the cluster node is CR50ia or CR100ia models.

Routing

Bug ID – 1927

Description - OSPF routes are not synchronized in Active-Active HA cluster, due to which Auxiliary appliance is not able to serve the HTTP request.

SSL VPN

Bug ID – 1981

Description –When more than 1000 users are registered at the time upgrade and Certificate Authority is configured, it is not possible to upgrade from v 9.6.0.34 to any higher versions.

System

Bug ID – 1966

Description – When Cyberoam is configured as direct proxy in version v 9.6.0.60, users face following issues:

1. Unable to send mails through Gmail
2. Not able to connect to MSN messenger
3. Some contents of website are not displayed

Work around - Enable "multiple category" from CLI using following command:

set http_proxy multiple-webcategory enable

Build 60

Anti-Spam

Bug ID – 1178

Description – Spam policy events – add, update, delete were not logged in Audit logs.

Bug ID – 1655

Description – Even if mail is successfully released from the Quarantine area, successful release message is not displayed. This is observed only with browser Internet Explorer 6.

Bug ID – 1656

Description – It is not possible to download the quarantined mail through the browser Internet Explorer 6 but it is possible through browser Firefox Mozilla.

Anti-Virus

Bug ID – 1605

Description – Even when virus scan policy is configured to allow mails with protected attachments, such mails are getting blocked.

Bug ID – 5513

Description – When virus scanning and Internet Access policy is applied, one cannot access URLs e.g. http://webcam.www.gov.tw/index.htm which requires connecting to port 20480 through Internet Explorer browser but the same sites accessible through Mozilla Firefox.

Bug ID – 5704

Description – When Cyberoam detects and strips the protected attachment from the mail, Administrator and Mail Receiver is sent a Notification mail with incorrect reason. Notification mail reads as “Infected attachment removed” but should read as “Attachment removed”. Even the name of the file which was stripped is not included in the mail.

Administrator receives only the Notification mail without the original message even if “Send Original” action is configured in the Virus Scan policy.

Dashboard

Bug ID – 1452

Description – Some of the IPS Alerts are displayed without Signature definitions in the IPS Alerts Doclet of Dashboard.

Bug ID – 1653

Description – After closing any of the doclets, Dashboard cannot be reset with the “Reset” button.

Bug ID – 1712

Description – If the user has saved Web Admin Console password, on updating any parameter of VPN connection, Preshared key gets replaced with this saved password. This is observed only when Web admin console is accessed via Firefox Mozilla.

Bug ID – 1827

Description – Mismatch in count of concurrent sessions displayed on Dashboard - System Usage doclet and Live User page on Web Admin Console.

Bug ID – 1877

Description – Mismatch in count of concurrent sessions displayed on Dashboard - System Usage doclet and Live User page on Web Admin Console. Due to this, sometimes users are not able to logon where CR25i models are deployed as concurrent sessions count exceeds the user license.

Firewall

Bug ID – 1170

Description – Firewall rule does not display the file upload statistics i.e. number of bytes uploaded.

Bug ID – 1179

Description – It is possible to create an “IP” Protocol based service under “Other” protocol with any protocol number.

Bug ID – 1555

Description – When Cyberoam is configured as Proxy, it is sometimes possible to access certain application even after logging out.

Bug ID – 1681

Description – When the VPN connection gets established through Cyberoam, data transfer via VPN Tunnel fails as VPN route does not get created.

Bug ID – 1720

Description - Web Filtering proxy may cause timeout issues while downloading files from the web sites if data greater than the defined content-length size is received.

Bug ID – 1762

Description – When the multiple MAC based firewall rules are created, Internet Access Policy applied to the first MAC based firewall rule is applied to all the subsequent MAC based firewall rules even if different policies are configured.

Bug ID – 5812

Description – When Strict policy is applied through Network Configuration Wizard, users are able to access the Internet but ICMP protocol is blocked as a result not able to ping any WAN IP address.

High Availability

Bug ID – 1771

Description – If HA Administrator username includes white space (blank) CLI commands do not work.

Bug ID – 1773

Description - In a HA cluster after failover, static routes configured in primary appliance are not added in secondary appliance.

Internet Access Policy

Bug ID – 1168

Description – It is not possible to categorize URL into multiple categories.

Logs and Reports

Bug ID – 402

Description – Recent Mail Viruses detected doclet of Dashboard displays recipient name with special characters. Blank report page is displayed when one clicks the link to view the details.

Bug ID - 1543

Description - When "Manager" rights is assigned to the Active Directory User in Cyberoam, user is not able logon to view reports i.e. user is of the Type "Manager"

Bug ID – 1606

Description – Session time mismatch in Internet Usage report i.e. total used time does not match with session start and stop time.

Bug ID – 1657

Description – Few signatures in the IPS Alert report do not provide hyperlink to view the signature details.

Bug ID – 1768

Description – All the reports except for Blocked Attempts reports for the previous day are generated without data i.e. blank. This issue is observed only in the CR15i models.

Bug ID – 1856

Description – If the proactive reports mail frequency is updated on Sunday or Monday then the Weekly Proactive reports for that week are not mailed.

Bug ID – 5521

Description - “Category wise trends for yesterday” proactive report is mailed without any data.

Online Help and Documentation

Bug ID – 1437

Description – The SSL VPN End User portal help included the screen images of previous version.

Bug ID – 1532

Description – The Online help text for restricting unknown IP address on trusted MAC was misleading.

Bug ID – 1684

Description – The Online help text for static ARP was confusing.

Bug ID - 1753

Description – The Online help text on Manage Live SSL VPN Users included incorrect information. It was mentioned that “Page also display their important parameters like Username, Source and leased IP address, Access mode, date and time when connection was established, tunnel type and data transferred.” But text should be “For the connections established through Web access mode only username, access mode and date and time when connection was established will be displayed.”

Single Sign On

Bug ID – 1487

Description – After SSO is configured, it is not possible to differentiate between local and domain user. As a result if user logs on as an “Administrator” user on the local system, user gets the access of all the resources allowed to the domain administrator user.

SSL VPN

Bug ID – 1669

Description – On resetting to the factory default configuration after upgrading to version 9.6.0 build 30, SSL VPN End-user Web portal becomes inaccessible.

Bug ID – 1742

Description – In SSL VPN Full tunnel mode, Cyberoam Web Admin console becomes inaccessible. This issue is found only in versions 9.6.0.16 and 9.6.034

System

Bug ID – 373

Description – Factory default retains Mail backup schedule.

Bug ID – 441

Description – After upgrading to version 95824, it was possible to rollback to the multiple versions. Ideally, rollback should be allowed only for the immediate previous version.

Bug ID - 523

Description - When DDNS is configured for multiple PPPoE links, and if both the links go down, DDNS server is not updated with the correct IP addresses after any of the links comes up.

Bug ID – 1500

Description – Interface based IPSec routes are flushed on reboot or restarting management services.

Bug ID – 1716

Description – NAT is not supported when Cyberoam is deployed in transparent mode.

Bug ID – 1729

Description – SNMP server stops responding after changing the default HTTP Proxy port. This issue is observed from version 9.6.0.16.

Bug ID – 1745

Description – When Internet Access policy is applied, Cyberoam does not allow to download any file using SVN command from Linux system but allows to download through any Windows based Browser.

Bug ID – 1832

Description – When more than 10 DHCP servers are configured by enabling Cyberoam's DNS settings, on updating DNS details, DHCP server stops responding.

Bug ID – 1882

Description – When Cyberoam is deployed as bridge and Parent Proxy authentication is enabled, it is not possible to upload any file on secure websites.

VPN

Bug ID – 1005

Description – The road warrior policy with DES-SHA1 algorithms is exported as 3DES-SHA1 i.e. wrong algorithms.

Bug ID – 1588

Description – When more than one backup links are configured, VPN connection does not failover between the other backup links.

Web Admin Console

Bug ID – 1615

Description – On Create Data Transfer Policy page, Data transfer limit "MB" is not translated correctly as "Mo" in French language.

Bug ID – 1649

Description – Manage Live users page sometimes shows upload and download data transfer value as zero.

Bug ID – 1652

Description – In the French GUI, on the VPN > Policy > Create Policy page, after selecting the template, template values are not loaded.

Bug ID – 1686

Description – Mismatch in password length on

- Add and Edit User page
- Appliance Registration page and Add on Subscription Module page

Bug ID – 1688

Description – "Back" button in View Bandwidth Usage page of Web Admin Console is not working.

Bug ID – 1708

Description – At the time of creating Custom Web Category, only 255 characters can be specified for Domains list.

Bug ID – 1721

Description - IPSec VPN Policy does not show the configured DH Group in Browser - Internet Explorer but it is shown in Firefox Mozilla.

Bug ID – 1725

Description – At the time of creating a new VPN Policy based on the policy with which the IPSec connection is already established, “Keying Method” option is greyed and can not be configured.

Bug ID – 1770

Description - It is not possible to change the action for IPS signatures from IPS policy when Web Admin Console is accessed via a web browser IE version 8

Bug ID – 1776

Description – When VPN policy is created using "None" template, blank policy is created.

Bug ID – 1787

Description - Mail reports display junk characters if Chinese character strings in Big5 encoding is included in the mail subject.

Bug ID – 1823

Description – When user tries to login through HTTP Login page, even if user has not saved the password, password is automatically filled in i.e. auto-completed. This happens if user has disabled "Save Password" option after enabling it once.

Bug ID – 1848

Description – After restoring backup of version 9.4.2.6, users are not able to login.

Build 34

SSL VPN

Bug ID – 1442

Description – Certificate issued by external Certificate Authority is not supported.

Bug ID – 1468

Description – When third-part Certificate is used, no SSL VPN configurations are included in the VPN Client configuration file i.e. blank file is downloaded

Bug ID – 1669

Description – On resetting to the factory default configuration after upgrading to version 9.6.0 build 30, End-user Web portal becomes inaccessible.

Build 30

Anti Spam

Bug ID – 1020

Description – If SMTP authentication is configured, at the time of releasing spam mail error -

"Error while releasing email" is received.

Clientless User

Bug ID – 474

Description – It is not possible to search Clientless user with IP address.

Bandwidth

Bug ID – 535

Description – Committed Bandwidth policy does not work as per the configuration.

Bug ID – 4884

Description – User-based Shared Bandwidth policy does not work.

Firewall

Bug ID - 1060

Description – When FTP scanning is enabled, Cyberoam drops all those connection requests whose FTP server response packet length exceeds 1024 characters

Bug ID – 1238

Description – Virtual LAN does not work for appliances models – CR50ia, CR100ia

Bug ID – 1465

Description – When Parent Proxy is configured, HTTP request does not reach Proxy server and as a result, it is not possible to upgrade IPS or AV signatures database.

Bug ID – 1484

Description – When scanning is enabled, it is not possible to connect to FTP server from any of the Alias subnet.

Bug ID – 1526

Description – When sending large email, SMTP scanning sometimes caused a server timeout. This situation is observed in CR250i and CR500i appliance models only.

Bug ID – 1575

Description – Due to large IP-based Virtual hosts configuration, after rebooting or restarting management services, system takes time to come up.

Bug ID – 5925

Description – Advanced Firewall custom setting configured from CLI console are not retained after restoring backup from version 9.5.3 build 22 and version 9.5.4 build 66 to version 9.5.4 build 86.

High Availability

Bug ID – 1464

Description – In some cases, HA configuration was possible only after disabling the model check.

PPPoE

Bug ID – 3816

Description – When PPPoE is enabled, Cyberoam terminates L2TP connection within 2 minutes.

Bug ID – 1456

Description – When multiple PPPoE links configured, even if all the links are up, request goes through single gateway only.

Proxy

Bug ID – 1440

Description – Sometimes when the Interface is configured to obtain the IP address from DHCP through Network Configuration Wizard, users are not able to access the Internet.

Reports

Bug ID – 1127

Description – Internet Usage reports for previous month is not displayed.

Bug ID – 1064

Description – Traffic Discovery Connection History reports were not available from version 9.5.9 build 33 onwards

Bug ID – 1326

Description – HTTP Upload report does not display the report date and time.

Bug ID – 4208

Description – Cyberoam does not save the modified Notification Email address for Reports (through Network Configuration Wizard). Due to this, mails are send to the previously configured email address only.

SSL VPN

Bug ID - 1241

Description – SSL VPN does not work when RADIUS authentication is configured.

Bug ID – 1478

Description – When Active Directory authentication is configured, sometimes users are not able to logon through SSL VPN End-user Web Portal as currently there is no text case validation. For example, user will not be able to login if domain name is configured in Capital letter as “CYBEROM.COM” and tries to login with myname@cyberoam.com.

Bug ID – 1511

Description – In certain situations, it is observed that after changing the global settings and web access gets disabled.

Bug ID – 1519

Description – URL redirection does not work with Web Access mode.

System

Bug ID – 656

Description – Sometimes at the time of downloading an email from POP3 server, the connection drops intermittently and due to this the entire downloading process re-starts. Hence user receives each mail twice or thrice.

Bug ID – 1007

Description – After changing default Secure Web Admin Console port, reports are not accessible.

Bug ID – 1077

Description – When Cyberoam is configured as Direct Proxy, in-case of primary DNS failure, switching to secondary DNS takes time and hence the Internet browsing speed might become slow.

Bug ID – 1353

Description – Mismatch in the Google Search hit count on Dashboard and Google Search report

Bug ID – 1404

Description – It is not possible to upload third-party Certificate.

Bug ID – 1455

Description – Quarantined area is not flushed on resetting configurations to factory defaults

Virtual Private Network (VPN)

Bug ID – 616

Description – L2TP VPN does not work with Apple MacOS X 10.5

Bug ID – 1485

Description – It is not possible to delete VPN connection after updating VPN policy.

Bug ID – 1570

Description – Special character Hash (#) not supported in Preshared key.

Web Admin console

Bug ID – 1047

Description – After changing the default Secure Web Admin port it is not possible to reposition the Dashboard Doclets by dragging and dropping and upgrade Antivirus and IPS signature. Different behavior is observed for different Web Browsers.

Bug ID – 1171

Description – On clicking “Next Page” button on Manage Active Page, instead of opening the next page of list of users, it is redirecting to “Deactivated Clientless Users” page

Bug ID – 1454

Description – Duplicate domain name can be configured as Local Domain in Anti Spam Configuration. As a result SMTP proxy does not start and if SMTP scanning is configured through firewall then the internal Mail Transfer Agent does not receive the mails.

Bug ID – 1467

Description – Mismatch in concurrent sessions displayed on Live User page on Web Admin Console. If there are more than 100 concurrent sessions, by default, it displays only 100 live users but “Concurrent Sessions” count includes all the sessions. One needs to click “Show All” link to view the entire list.

Bug ID – 1451

Description - After changing the Web Admin console language to French language, some of the dashboard components are not displayed in French and some components of Console itself and menu with the long names are not displayed properly.

Bug ID – 1479

Description – After changing the Web Admin console language to French language, one is not able to use Network Configuration wizard

Bug ID - 1482

Description - When one tries to change the Gateway type i.e. Active to Backup of the PPPoE link, error “Gateway name already exist” is displayed. This situation occurs when multiple ISP links with the same gateway IP address are configured.

Bug ID – 1486

Description – When Web Admin Console language is set to “French” user groups cannot be created.

Build 16

Categorization

Bug ID – 531

Description – All the URIs which include “.au” are incorrectly blocked under Audio File Type category.

Clientless User

Bug ID – 89

Description – When not a single Logon Pool based Bandwidth policy is configured, it is not possible to create Clientless user. In other words, one needs to configure at-least one log on pool based bandwidth policy to add clientless user and group.

Bug ID - 683

Description – Even when IP address (login restriction) for Clientless user is mandatory, it is possible to update the details by leaving the IP address field blank.

Dashboard

Bug ID – 950

Description – Dashboard data is not flushed when backup is restored on another Appliance.

Group

Bug ID – 972

Description – Normal users can be as the member of Clientless group but as per the default behavior, clientless group cannot have normal users as a group member.

Bug ID – 6226

Description - Error “IPs are already in use” is received when one tries to create multiple clientless users for the IP address range added to the existing logon pool. Hence, one has to create single clientless user for the individual IP address for the required range. For example, if additional 50 addresses are added in the IP range, one has to create clientless user for each IP address one by one.

Again, if the network is not in the Auth Network, users will be activated but will not be able to logon. Due to this, users will not be displayed in the Manage Live User or Manage Clientless User page but search result will display the list of newly added clientless users.

One needs to restart management services from CLI console after adding network in Auth Networks.

High Availability

Bug ID – 854

Description – Virtual host does not work when HA cluster is configured.

.

Bug ID – 648

Description – When OSPF routing is configured, connectivity delay is observed after restarting primary appliance.

Bug ID – 722

Description – In Active-Active HA cluster, gateway becomes unreachable i.e. dead if static ARP entry is added for gateway.

Bug ID - 6533

Description - Data transfer of the live users (Manage Live Users page) reflects the data transfer through primary as well as auxiliary appliance when HA is configured.

Description - User based Data transfer policy can now be configured when HA is configured.

Intrusion Prevention system

Bug ID – 826

Description – In “cyberoam signatures” category, for the signatures whose action is “OFF” are displayed with action as “ON” after editing other signature parameters.

Bug ID – 919

Description – Custom IPS signature are retained on resetting to factory default settings.

Bug ID – 5487

Description – Certain Internet Banking sites were not accessible due to Ultrasurf IPS signature.

Logs and Reports

Bug ID – 954

Description – Inconsistent Bandwidth usage graph title. Displays data transfer as Bytes/Sec instead of Bits/sec for weekly, monthly and yearly reports.

Language

Multiple language translation issues like incorrect translation, spelling mistakes are resolved.

Multiple Gateways

Bug ID – 473

Description – Gateway Status change alert messages where mailed at the HA Admin Email ID only High Availability cluster is configured. Due to this, Cyberoam Administrator does not receive such mails if HA was not configured or Appliances in which HA feature is not supported.

Now, all the gateway status related mails will be mailed at the Cyberoam Administrator Email ID configured from Network Configuration Wizard and not the HA Admin Email ID. HA Admin will receive only the mails related with the HA.

System

Bug ID – 83

Description – When the time zone is updated from Web Admin Console, time displayed on Web Admin and CLI console does not match. One needs to restart management services from CLI console to resolve this issue.

Bug ID – 316

Description – Firewall Bypass rule created from Advanced Firewall rule configuration of CLI console is not removed after resetting to factory default.

Bug ID – 455

Description – Cyberoam is not able to learn route when RIP routing is configured in plain mode i.e. when authentication is not enabled

Bug ID – 473

Description – Gateway Status change alert messages where mailed at the HA Admin Email ID only High Availability cluster is configured. Due to this, Cyberoam Administrator does not receive such mails if HA was not configured or Appliances in which HA feature is not supported.

Now, all the gateway status related mails will be mailed at the Cyberoam Administrator Email ID configured from Network Configuration Wizard and not the HA Admin Email ID. HA Admin will receive only the mails related with the HA.

Bug ID – 582

Description – When using Google Chrome browser it is not possible to configure DHCP server.

User

Bug ID – 476

Description – Single Sign On users do not receive the disconnection message sent from the Live User Page of Web Admin Console

Bug ID – 958

Description – There is mismatch in the total count and number of the live users displayed on the Manage Live User page of Web Admin Console

Virtual host

Bug ID – 6144

Description – When Alias Interface based Virtual host is configured, one can delete Alias interface before deleting virtual host.

Virtual Private Network (VPN)

Bug ID – 672

Description – When "*" is configured as remote gateway in Cyberoam and remote host is configured on dynamic IP address, multiple IPSec tunnels cannot be established between remote host and Cyberoam. This happens because Cyberoam does not support mix mode tunnels i.e. one tunnel with Authentication mode as "Main" and another as "Aggressive".

To establish multiple connections it is required that all the tunnels established on the Cyberoam should be either set as "Main" or "Aggressive" mode.

Web Admin console

Bug ID – 215

Description – At the time of adding PPTP users, when one clicks "Show", the list of group users is not displayed.

Bug ID – 270

Description – Format mismatch in advanced firewall configuration parameters when CLI console is accessed through Telnet and HTTP Interface. For example, when CLI is accessed over Telnet, parameters are displayed with special character underscore (_) e.g. source_network, while parameters are displayed without underscore e.g. source network, when CLI is accessed over HTTP Interface.

Bug ID – 708

Description – User is not able to logon to My Account and Diagnostic tool with the password which includes space while user is able to logon to the Web Admin Console with the same password.

Bug ID – 749

Description – If more than one Firewall log is not configured for syslog server from System > Logging > Logs Configuration page, Cyberoam does not send firewall rules log to the syslog server.

Change Log

Revision	Topic	Description
1.0		Initial Release
2.0	Upgrade Requirement and Upgrade Procedure	Added IPS Signature Database information
	Enhancement – IP Reputation	Added more information on subscription and feature usage
3.0	Build 30 Enhancements	Added entire section
	Build 30 Bugs solved	Added entire section
	Build 30 Known Behavior	Root cap behavior
4.0	Build 34 Bugs solved	Section added
5.0	Build 60 Enhancements	Added entire section
	Build 60 Miscellaneous Changes	Added entire section
	Build 60 Bugs solved	Added entire section
5.1	Build 60 Enhancements	Added - Two Factor Authentication for SSL VPN
	Build 60 Bugs solved	Removed Clientless Single Sign On – CTAS, Bug ID – 1538
5.2	Build 62 Bugs solved	Added entire section
6.0	Build 74	Added details of build 74

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 (Toll free)

- APAC/EMEA: +1-877-777- 0368
- Europe: +44-808-120-3958
- India: 1-800-301-00013
- USA: +1-877-777- 0368

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 Commtouch respectively and the performance thereof is under warranty provided by Kaspersky Labs and Commtouch. 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

Document Version – 7.0-24/02/2010