Release Date

Version 10.6.3; 14th October, 2015

Release Information

Release Type: Major Feature Release

Applicable to CyberoamOS Version

V 10.01.0XXX or 10.01.X Build XXX	All the versions
V 10.02.0 Build XXX	047, 174, 176, 192, 206, 224, 227, 409, 473
V 10.04.X Build XXX	0 Build 214, 0 Build 304, 0 Build 311, 0 Build 338, 0 Build 433 1 Build 451 2 Build 527 3 Build 543 4 Build 028 5 Build 007 6 Build 032
V 10.5.3 or V 10.5.4	Common Criteria Certificate (EAL4+) Compliant
V 10.6.X Beta/RC/GA/MR X	0 Beta-1 0 Beta-2 0 Beta-3 1 RC-1, 1 RC-3, 1 RC-4, 1 GA, 1 MR-1, 1 MR-2, 1 MR-3 2 Beta-1, 2 Beta-2, 2 RC-1, 2 GA, 2 MR-1 3 Beta-1, 3 RC-1, 3 RC-2, 3 RC-3, 3 RC-4

Upgrade procedure

To upgrade the existing Cyberoam Appliance follow the procedure below:

- Logon to https://customer.cyberoam.com
- Click “Upgrade” link under Upgrade URL.
- Choose option “Select for Version 10.00.0xxx to current GA Version 10.00.0xxx Firmware”.

For Cyberoam versions prior to 10.01.0472	For Cyberoam version 10.01.0472 or higher
Upgrade Cyberoam to 10.01.0472 selecting option **“Below 10.01.0472”** and follow on-screen instruction. By doing this, the customer will not be able to roll back.	Upgrade Cyberoam to the latest version by selecting option “10.01.0472 or higher” and follow on-screen instruction.

Compatibility Annotations

This version of CyberoamOS is Appliance Model-specific. Hence, firmware of one model will not be applicable on another model and upgrade will not be successful. You will receive an error if you try to upgrade Appliance model CR50iNG with firmware for model CR100iNG.

This release is compatible with all Cyberoam Virtual Appliances.

This Cyberoam version is compatible with the Cyberoam Central Console (CCC) version 02.02.1185 and above. Please check http://docs.cyberoam.com for availability of latest CCC firmware to deal with compatibility issues.

Revision History

Sr. No.	Old Revision Number	New Revision Number	Reference Section	Revision Details
1	1.00-30/03/2015	1.01-29/05/2015	Bugs Solved	Added few bugs: Bug IDs – 19117, 19132, 19142, 19144, 18927, 150, 19178, 19177, 19175, 19047
2	1.00-30/03/2015	1.01-29/05/2015	Features	Added Sophos AP model numbers under "**Centralized Management of Sophos Access Points from Cyberoam**" section
3	1.01-29/05/2015	1.02-02/06/2015	Bugs Solved	Added bug: Bug ID - 18955
4.	1.02-02/06/2015	1.03-17/07/2015	Bugs Solved	Added few bugs: Bug IDs – 17913, 19002, 18920, 19106, 18106, 18923, 6714, 19206, 17796, 13956, 19310, 19332, 19358, 19294, 18983, 18968, 18921, 19268, 19048
5.	1.03-17/07/2015	1.04-21/08/2015	Bugs Solved	Added few bugs: Bug IDs – 19355, 19327, 19379, 19377
6.	1.04-21/08/2015	1.05-14/10/2015	Bugs Solved	Added few bugs: Bug IDs – 19418, 18912, 19281, 19350
6.	1.04-21/08/2015	1.05-14/10/2015	Open Issues	Added one open issue.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Contents

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Introduction

This document contains the release notes for CyberoamOS Version 10.6.3. The following sections describe the release in detail.

This release comes with several new features, enhancements and bug fixes to improve quality, reliability, and performance.

For information about the changes included in any specific version of CyberoamOS, please see the release notes archives.

For detailed information on using any of the CyberoamOS's features, please refer to the Technical Documentation Repository or Online Help.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Features

1. Support to Import/Export Text-based Configuration File

Currently, Cyberoam provides backup-restore feature which allows to create a copy of the appliance configuration and restore it on same or other compatible appliance. However, the contents within the backup file are encrypted and hence cannot be updated before restoring it on the appliance.

To facilitate modification in the backup configuration file, Cyberoam from this version onwards allows exporting and importing appliance configuration to/from a text file respectively. It is useful as the contents of this file are in human readable XML format which makes possible updating the configurations as per the requirements. Administrator can export configuration to a text file and import it on another compatible appliance after updating the configurations. The export and import files are of .tar extension. Example: API-1421656341945133.tar

- Configuration exported from appliance with higher firmware versions cannot be imported on lower versions.
- The destination Cyberoam appliance on which configuration is to be imported must have the same or greater number of ports than the source appliance from which configuration is exported.

This feature will be useful when importing configuration settings on large number of appliances.

To use this feature, go to **System > Maintenance > Import Export**.

Also, it will provide flexibility to the administrators as he/she can choose to export all/few of the appliance configurations. Administrator can use "**Export selective configuration**" option to export selected configuration.

2. TACACS+ External Server Authentication support

From this version onwards, Cyberoam provides Terminal Access Controller Access-Control System Plus (TACACS+) Server Authentication support. It is now possible to authenticate users against TACACS+ Server, if TACACS+ Server is deployed in your network.

TACACS+ is a protocol that provides remote access control to users attempting to gain access to routers or network access servers.

To configure TACACS Server, go to **Identity > Authentication > Authentication Server** and Click 'Add'.

Currently only CHAP & PAP authentication protocols are supported to authenticate L2TP/PPTP users against TACACS+ server.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

3. Cyberoam-iView Reports

a. Grouping of CIPA Reports

From this version, reports related to Children's Internet Protection Act (CIPA) compliance are grouped under Compliance Reports section of Cyberoam-iView. In order to receive E-rate funds for Internet access, it is necessary that Educational Institutes and Libraries comply CIPA requirements.

Cyberoam-iView provides following reports under CIPA:

1. Top Denied Web User
2. Top Denied Categories
3. Top Denied Applications
4. Top Denied Domains
5. Top Denied Protected Contact
6. Search Engine Reports (Google, Yahoo, Bing, Wikipedia, Rediff, eBay and Yandex)

To view the CIPA reports, go to **Compliance Reports > CIPA**.

For more details, please refer On-Appliance iView Help.

b. Grouping of NERC CIP v3 Reports

With this version, CyberoamOS has grouped reports related to NERC CIP v3 as a separate tab under Compliance Reports section that helps organizations with critical infrastructures like ICS, Power Systems etc. to match some of the key cyber security requirements of NERC's CIP v3 standards.

Cyberoam-iView helps to prove compliance to some of the key CIP requirements with the following reports under NERC CIP v3:

1. Top Applications
2. Top Attacks
3. Top Viruses
4. Top Attacked Servers
5. Authentication Events
6. Admin Events

To view the NERC CIP v3 reports, go to **Compliance Reports > NERC CIP v3**.

For more details, please refer On-Appliance iView Help.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

4. IPv6 Supported Features

a. Dynamic IPv6 Address Assignment for WAN Interfaces

From this version onwards, an Interface can be configured to act as DHCPv6 Client. DHCP Server can lease IPv6 Address to WAN interfaces. Till now, WAN Interfaces could only be assigned static IPv6 Address only.

DHCPv6 Client address could be configured in two different ways:

Auto Mode: IPv6 address will be auto-configured based on the Managed and Other flags received in Router Advertisement packet through Stateless Address Auto-Configuration (SLAAC).

Manual Mode: Administrator can select to configure IPv6 address either through SLAAC or DHCPv6 (Stateful Address Assignment).

DHCPv6 Client normally obtains configuration parameters from the Server through four-message exchange (Solicit, Advertise, Request and Reply). To enable quicker client configuration, administrator can select DHCP Rapid Commit" option. Enabling it, will allow the client to obtain configuration parameters through two-message exchange (Solicit and Reply).

To configure IPv6 Interface using DHCPv6, go to **Edit Interface** page under **Network** and select DHCP IP Assignment.

Administrator could also configure number of solicitation messages that could be sent during Duplicate Address Detection (DAD) process. It will enable the client to determine whether the address is already used by another node. Option to configure DAD Attempts is provided under **Advanced Settings** on Network Edit Interface page.

Further, Cyberoam supports mitigating Router Advertisement (RA) attacks by allowing to configure an Interface to accept RA packets only from specific RA Servers. To configure RA Servers, go to **Edit Interface** page under **Network** and configure MAC Address of Allowed RA Servers under **Advanced Settings**.

b. Anti Virus and Anti Spam scanning over IPv6 Networks

From this version onwards, Cyberoam supports scanning for IPv6-based SMTP/SMTP over SSL/POP3/IMAP/HTTP/HTTPS traffic.

All the Anti Virus and Anti Spam rules are applicable on both IPv4 and IPv6 network.

Points to Note:

One needs to enable AV and AS Scanning for the mail protocol under **Firewall > Rule > IPv6 Rule**.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

c. Security Policies for IPv6

All the security policies applicable on IPv4 traffic can now be applied on IPv6 traffic.

a. All Web Filter policies applicable on IPv4 traffic can be applied on the IPv6 traffic.
b. Application Filter policies could now be attached to the Firewall rule for IPv6 traffic.
c. Intrusion Prevention System (IPS) policies could now be applied on IPv6 traffic.

d. IPv6 Support for IPSec VPN Connection

IPSec VPN connection could now be established between IPv6 end-points/subnets. Till now, it could be established between IPv4 endpoints only. Administrator could configure IPSec Site-to-Site VPN tunnels with mixed IP families as below:

- 4 in 4 (IPv4 subnets with IPv4 gateway)
- 6 in 6 (IPv6 subnets with IPv6 gateway)
- 4 in 6 (IPv4 subnets with IPv6 gateway)
- 6 in 4 (IPv6 subnets with IPv4 gateway)

To facilitate this, a new option "IP Family" has been added on the Connection Page of **VPN > IPSec**.

e. Assign IPv6 address to DNS via DHCP

From this version onwards, it is possible to dynamically obtain IPv6 DNS address from DHCP Server. To facilitate this, a new option "Obtain DNS from DHCP" is added under IPv6 section on **Network > DNS > DNS page**. Till now, only static IPv6 DNS could be configured.

f. Parent Proxy for IPv6

Parent Proxy could be now configured for IPv6 traffic. To configure Parent Proxy, go to **System > Configuration > Parent Proxy**. Separate Parent proxies should be configured for IPv4 and IPv6.

5. Centralized Management of Sophos Access Points from Cyberoam

From this version onwards, Cyberoam can act as Wireless Controller managing Sophos Access Points (AP). Cyberoam administrator can configure and manage multiple Sophos Access Points centrally from Web Admin Console thus easing the task of configuring them individually. Wireless Client traffic is forwarded to Cyberoam and all security policies can be applied on the traffic thus providing wireless clients same level of security as LAN users.

It will be useful in network environments where Sophos APs are deployed to manage internal wireless networks and it is required that Cyberoam behaves both as security appliance and Wireless Controller.

A menu "Wireless Protection" has been added on UI through which Sophos APs could be configured and managed. Administrator could configure Wireless Networks, Mesh Networks, AP and AP groups. The administrator could also view managed APs, SSIDs, connected wireless clients and wireless networks from a single page.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Note:

- This feature is supported for following Sophos AP models: AP 10, AP 15, AP 30, AP 50, AP 55 and AP 100.
- It is not supported in Cyberoam 'wi/wiNG' series appliances and 10iNG/15iNG appliance models.

6. Overriding Organizational Web Filter Policy Restrictions

With this version, Cyberoam allows to provide temporary Web Access for specified domains/websites. Prior to this, Web filtering could be done through statically configured policies. This feature will be useful in educational institutes that require students to access few domains on temporary basis for their Project work. Also, administrator can use this feature in cases where he/she wants the group leader to control Internet access for his/her team.

Best use case of this feature is when Teachers need temporary access to a particular website blocked by the School Policy on a daily basis. In such case, they would need to request the administrator to provide access now and then. Hence, to ease administrator's task and prompt resolution, a temporary Access Portal is now provided where in the Teacher can submit list of websites/categories of domains that students need to access temporarily. An access token with limited validity will be generated which can then be used to access the websites. At the end of the validity period, the domains will again be blocked as per the School policy.

To configure Temporary Access Settings navigate to **Web Filter > Settings > Temporary Access Setting** and Enable Portal to use this feature. The settings configured will be applicable for all the Temporary Access requests. Additionally, administrator can also configure domains/categories of domains which would never be granted temporary access.

7. Reducing Administrative Overheads – Support of Route-based VPN

With Route-based VPNs, Routing decides which packets to route through the VPN tunnel. A virtual interface is created on configuring VPN tunnel and all the traffic passing through that interface will be encrypted. Static/Dynamic routes could be added on the virtual tunnel interface that is bound to a specific VPN tunnel.

With Policy-based VPN, IPSec policy determines which packets to route through the VPN tunnel. Due to which, management of large number of VPN sites becomes a burden as administrator needs to update all the VPN Policies when network topology changes. In Route-based VPN, Network configuration is no longer needed hence easing administrator's policy maintenance tasks. In case Static routing is configured, administrator only need to change the static routes rather than changing the Policy configurations.

This feature is more useful when multiple subnets needs to communicate over VPN and dynamic routing is configured on local and remote sites. Administrator needs only one time tunnel configuration thus reducing the overhead to manually configure all the tunnels.

To configure Route-based VPN, navigate to **VPN > IPSec > Add Connection**. Select checkbox "**Bind with An Interface**" for "**Site to Site"** Connection Type. Also, two new parameters "**Local IP Address**" and "**Remote IP Address**" are added on the same page. When configuring dynamic routing on the virtual interface, one needs to configure the above interface details.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Enhancements

1. Support of IPSec VPN Connection on Alias IP Address

IPSec VPN tunnel configuration is now supported on Alias IP created for WAN interfaces thus providing more flexibility in VPN deployment. Till now, Cyberoam supported IPSec VPN tunnel configuration on WAN Physical and VLAN interfaces IP only.

IP Aliases will be listed along with the default WAN interfaces in the Local WAN Port Endpoint details section for IPSec, CISCO VPN and L2TP connections.

2. Totally Configurable Captive Portal page

Till now, limited customization of captive portal could be done. This functionality is further extended to provide full customization. Administrators can now fully brand the page as per their requirement by using custom HMTL template. Dynamic content like banners from external sources/web servers, customizable “Message of the day” box etc. can now be integrated thereby allowing administrator to fully control the look and feel of the page.

To customize Captive Portal, go to **System > Configuration > Captive Portal** and enable option "Use Custom HTML Template" and input HMTL code. Captive Portal will be rendered according to the HTML input.

3. Cyberoam-iView: Support for Yandex Search Engine Reports

With this version onwards, Search Engine reports section of Cyberoam-iView has been enhanced with support of reports for search requests performed using Yandex search engine. Yandex is the largest search engine in Russia with about 60% market share in the country.

To view the report, go to **Reports > Search Engine > Yandex Search.**

4. NTLM Authentication Enhancements

From this version onwards, following are the NTLM Authentication enhancements:

a. Nested Group Support

Cyberoam now supports nested groups for NTLM authentication. With nested groups, the policies configured for parent groups will be automatically applied to the members in subgroups using NTLM authentication. Previously, policy configured for the immediate group could only be applied to the users.

Nested Group Support could be configured from CLI using the commands below:

Command: Cyberoam ntlm_auth nested_group_support on/off

Description: To enable/disable Nested Group support for NTLM Authentication

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Command: Cyberoam ntlm_auth nested_group_support show

Description: Displays whether the nested group support is enabled/disabled.

b. Cascading Trust Using Cross Domain Authentication Support

From this version onwards, NTLM logins from multiple trusted Domains is possible. When a user of a trusted domain logs on and is a member of any group which is a member of group defined in the domain added in Cyberoam then the group policy can be applied on that user. Previously, in such scenario, for applying group policy, administrator had to add and select all the domains or else the default group policy will get applied on the user. You need to add only one trusted domain now thus easing the administrative task of adding all the domains and importing the respective groups.

5. Mail Notifications using CRAM-MD5 Authentication

With this version onwards, Cyberoam supports Encrypted authentication for the Mail Servers configured for Email Alert Notification. Cyberoam now supports CRAM-MD5 Authentication method in lieu of just Plain Text Authentication method supported in the earlier versions.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Miscellaneous

CyberoamOS has the following miscellaneous change:

- Two new icons "Renew IP" and "Release IP" will be displayed on the Manage Interface page of Network, if IPv6 configuration is done through DHCP.
- On Migration to firmware version 10.6.3 RC-2:

  If you have previously created Site-to-Site IPSec Connection with Amazon VPC, you need to edit the VPN Policy used for the connection and disable the option "**Pass Data In Compressed Format**" under **VPN > Policy**.

  When you create Site-to-Site IPSec Connection with Amazon VPC, make sure that the option "**Pass Data In Compressed Format**" under **VPN > Policy** is disabled.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Bugs Solved

Access Server

Bug ID - 18920

Description - Multiple users are created in Appliance even if a single username is entered in different formats while logging into domain.

For example, userhu.sic.local\toth.szilveszter enters his username in Three (3) formats: "toth.szilveszter@hu.sic.local", "HU\toth.szilveszter" and "HU.SIC.LOCAL\toth.szilveszter".

Anti Spam

Bug ID – 19268

Description – Anti Spam service taking high CPU usage in Firmware version 10.6.3 RC-2.

Bug ID – 19206

Description – The transferred values of the Rule column in Quarantine Area appear NULL when Appliance is upgraded from firmware version 10.4.6 Build 032 to 10.6.2 MR-1.

Bug ID – 17913

Description – Mail Servers with Private IP from the subnet 10.0.0.0/8 get incorrectly submitted for IP Reputation check**.**

Bug ID – 6714

Description – Mails from the quarantine are not released as mail server accepts a hostname that is fully qualified domain name.

Anti Virus

Bug ID – 19048

Description – Appliance does not show Auto/Manual AV update successful logs for incremental AV updates in log viewer. This is observed in Firmware version 10.6.2 onwards.

Bug ID - 19047

Description - Emails sent over STARTTLS pass through unscanned, if only **SMTP** is enabled and **SMTPS** is not enabled against **AV & AS Scanning** in Firewall Rule.

Bug ID - 19002

Description - Cyberoam Appliance is unable to block the .exe file type of attachments while sending or receiving emails if the file contains non-English characters.

CLI

Bug ID – 18650

Description – Multiple custom ports cannot be added to the SIP Module under system_modules. This is observed in firmware version 10.6.2 RC-1.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Firewall

Bug ID – 19178

Description – Cannot access Virtual Host from Appliance's WAN Interface, if the External IP is set as the Interface IP of the WAN Interface.

Bug ID – 19310

Description – Thin Client users are not able to access Internet even after being authenticated. This is observed in firmware version 10.6.3 RC-2 onwards.

Bug ID – 19332

Description – Cyberoam does not NAT the LAN IP Address of a user to Public IP Address if WAF is configured on Appliance and user accesses the Web Server. This is observed in firmware version 10.6.3 RC2 onwards.

Bug ID – 19358

Description – On Appliance reboot, expired Firewall Rule with One-Time Schedule becomes active again.

Firmware

Bug ID - 19418

Description - Appliance cannot be accessed when 15wing-AM03 appliance is upgraded to firmware version 10.6.3 RC3.

Bug ID – 18927

Description **–** In **System > Maintenance > Firmware,** Cyberoam allows uploading of the same firmware image in firmware slot 1, as the active firmware in slot 2.

Guest User

Bug ID – 18338

Description – Guest Users are created with status as 'Expired', the Expiry Date the same as the Created Date and Validity as a random number, if Multiple Guest Users are created from Identity > Guest Users > Guest Users using the Add Multiple button in which the 'Validity Start' parameter is set as 'Immediately'.

Bug ID – 17126

Description – "You must select Country Code" error is displayed when a guest user tries to register at the Guest User registration page. This error occurs when the Default Country Code field on the General Settings page is left blank and the Cell Number Format - Use Country Code with Cell Number is enabled on the SMS Gateway page of Identity > Guest Users.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

GUI

Bug ID – 19281

Description – User cannot login into My Account without mentioning domain name as part of username. This is observed in firmware version 10.6.3 RC-2.

Bug ID - 18555

Description - The error message “You must enter valid value for Mail Server IPv4 Address / FQDN” is displayed and Email Server is not configured if an FQDN with more than 45 characters is specified for the parameter Mail Server IPv4 Address / FQDN in **System > Configuration > Notification**.

High Availability

Bug ID – 19355

Description – When HA is configured, admin is able to access Appliance using SSH and Telnet even if Appliance Access is disabled for those services. This is observed in firmware version 10.6.3 onwards.

Bug ID – 19327

Description - Traffic load balancing is not working when Cyberoam is configured as Direct Proxy.

IPS

Bug ID - 19377

Description - IPS consumes high memory for appliances running on firmware version 10.6.3 RC-3.

Bug ID – 19175

Description – Upstream DHCP Server cannot lease IP Address to Appliance WAN Interface, if the Interface is part of a Bridge and the associated LAN to WAN Firewall Rule contains IPS policy configuration. This is observed in firmware version 10.6.2 onwards.

Bug ID – 18687

Description – RAM usage exponentially increases when IPS policy is applied on Firewall Rule.

Bug ID - 17967

Description - User is unable to browse the Internet through Internet Explorer 9 when an IPS Policy is applied on a Firewall Rule for Appliances running on firmware version 10.6.1 MR-1.

Logs & Reports

Bug ID – 18106

Description – Logs and Reports are not generated if “Secure Communication” is enabled on the Central Management page of System > Administration.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Network

Bug ID - 19350

Description - Administrator is unable to add alias on PPPoE interface. This is observed in firmware version 10.6.3 RC-2.

Bug ID - 19177

Description - Appliance is unable to integrate with ConnectWise if user accesses HTTPS based website. This is observed in all versions of 10.6.2.

Bug ID - 19106

Description - In Appliance Models CR1000iNG-XP, CR1500iNG-XP and CR2500iNG-XP, if you set the zone of any port, say Port1, as “None”, the VLAN and Alias configuration on ports that start with “1”, that is ports 10-19, get removed.

Bug ID - 18917

Description - Cannot access and update interface configuration, and error “<Interface> cannot be updated” is displayed if that Interface is specified against ‘Interface’ parameter in any Unicast Static Route. This is observed in firmware version 10.6.2 GA.

Proxy

Bug ID - 19132

Description - Captive portal cannot be accessed over HTTPS when appliance is upgraded to firmware version 10.6.3 RC-1.

Bug ID – 18983

Description – High memory utilization is observed in Firmware version 10.6.3 RC-2 when AV & AS Scanning for POP3/IMAP is enabled.

Bug ID - 18955

Description - While browsing an HTTPS website before user authentication, Captive Portal is not redirected over HTTPS if Cyberoam acts as a direct proxy. This is observed in firmware version 10.6.2 GA onwards.

Bug ID – 18983

Description – High memory utilization is observed in Firmware version 10.6.3 RC-2 when AV & AS Scanning for POP3/IMAP is enabled.

Bug ID – 18968

Description – Slow browsing issue is observed randomly in Firmware version 10.6.2 due to high load on Web Proxy.

Bug ID – 18921

Description – When web based Gmail is blocked, mails through Google Hosted servers also gets blocked even though host name is configured through: set service-param HTTPS google-hosted.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Bug ID – 18311

Description – HTTPS traffic is dropped by Cyberoam if an upstream Parent Proxy is configured with NTLM authentication method.

Reports

Bug ID - 18864

Description - "Top Web Users" report, exported in PDF format is incorrectly named as "Web---" when Japanese is selected as the User Interface language at the time of login.

Bug ID – 18249

Description – Custom View Reports cannot be exported in PDF format.

Bug ID – 18352

Description – In a Custom View in On-Appliance iView, reports included in a previously deleted Custom View are displayed in addition to currently selected reports.

Bug ID – 15748

Description – On-Appliance iView Reports do not get displayed at random instances in the Appliance with Firmware Version 10.04.5 Build 007, if "French" language is selected while logging into Reports.

SNMP

Bug ID - 18923

Description - Appliance goes into Failsafe Mode and error “Unable to start logging Daemon” is displayed on upgrading Appliance to firmware version 10.6.3.076, if SNMP is configured before the upgrade.

System

Bug ID – 150 (Applicable only for Cyberoam Virtual Security Appliances)

Description - Virtual Cyberoam Security Appliance does not work with Firmware version 10.6.3 RC-1 and keeps on rebooting after installation.

Virtual Host

Bug ID - 19142

Description - Cannot access Virtual Host placed behind a Bridged Interface from WAN Interface. This is observed in firmware version 10.6.3 RC-1 onwards.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

VPN

Bug ID – 13956

Description – VPN auto reconnect fails, if the Fully Qualified Domain Name configured under VPN does not get resolved.

Bug ID - 19117

Description - Not able to establish IPSec VPN tunnel if Local End Point is a PPPoE WAN Interface. This is observed in Firmware Version 10.6.3. RC-1 onwards.

Bug ID - 19144

Description - Appliance is unable to establish Site to Site IPSec Tunnel mode connection when appliance is upgraded to firmware version 10.6.3 RC-1.

Bug ID - 18912

Description - IPSec connection is not established if, under **VPN > Policy > Policy**, the “PFS Group (DH Group)” under Phase 2 is set as None and PFS is enabled at the remote VPN peer.

Bug ID - 18582

Description - Data is not transferred over VPN connections established between Cyberoam and a third party device, where the other device acts as an initiator while Cyberoam acts as a responder, and compression is enabled at both ends. This is observed in firmware version 10.6.2 onwards.

Bug ID- 17796

Description - Traffic does not flow through configured static route in IPSec Connection even if it is visible when viewed using command “cyberoam ipsec-route show”, if the connection has multiple tunnels.

Bug ID – 19294

Description – On Appliance reboot, IPSec tunnels are NOT re-established if the tunnels are configured on a PPPoE WAN Link.

Bug ID - 19379

Description – IPSec VPN tunnel cannot connect if Remote Endpoint is set as "Any" and "Local ID" & "Remote ID" is FQDN. This is observed when appliance is upgraded from Firmware Version 10.6.2 MR-1 to Version 10.6.3 RC-3.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Open Issues

- In IPv6 Networks, FTP over HTTP is not supported when Cyberoam is configured as Direct Proxy.
- Anti Virus definitions, IPS Signatures and Web Category databases can be upgraded only through IPv4 Gateway.
- After upgrading to this firmware, it will not be possible to establish SSL VPN Connection over a UDP Port.

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

General Information

Technical Assistance

If you have problems with your system, contact customer support using one of the following methods:

E-mail 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

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

Important Notice

Cyberoam Technologies Pvt. Ltd. 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. Cyberoam Technologies Pvt. Ltd. assumes no responsibility for any errors that may appear in this document. Cyberoam Technologies Pvt. Ltd. reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

Use of this product and document is subject to acceptance of the terms and conditions of Cyberoam End User License Agreement (EULA) and Warranty Policy for Cyberoam UTM Appliances.
You will find the copy of the EULA at http://www.cyberoam.com/documents/EULA.html and the Warranty Policy for Cyberoam UTM Appliances at http://kb.cyberoam.com.

RESTRICTED RIGHTS

Copyright 1999 - 2015 Cyberoam Technologies Private Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Cyberoam Technologies Pvt. Ltd.

Corporate Headquarters

Cyberoam Technologies Pvt. Ltd.
Cyberoam House,
Saigulshan Complex, Opp, Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad – 380006, INDIA
Phone: +91-79-66065606
Fax: +91-79-26407640
Website: www.cyberoam.com

Cyberoam www.cyberoam.com © Copyright 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.