

Release Information

Release Type: General Availability

Compatible versions: 9.6.0.78 for al CRs except CR15i; 9.5.8.68 for CR15i

Upgrade prerequisite: 24 x 7 OR 8 x 5 valid Support license

Applicable to: All the Cyberoam Appliance models

Upgrade procedure

Refer Migrate from v9.6.x.x to v10 document.

Compatibility issues

Appliance model-specific firmware and hence firmware of one model will not be applicable on another model. Upgrade will not be successful and error message will be given if your Appliance model is CR100i and you are upgrading it with firmware for model CR500i.

Contents

Release Information	1
Introduction.....	3
Changes from V 9.....	3
1. Logical flow change	3
2. Internet Access control configuration change	3
3. Behavior change	3
4. Redesigned UI - Menu and pages regrouping	4
5. Renamed features	5
6. Functionality moved from CLI to Web Admin Console	5
Discontinued features of version 9.x	5
Features expected in version-10 Stability-1	6
Features expected Post version-10 Stability-1	6
Features availability to be confirmed eventually	7
CLI features	8

Introduction

With version 10, Cyberoam has moved to firmware-based solution with the configuration and behavioral changes as given in the document. Document also lists various functionalities added in version 10. For details on new features added in Version 10, please refer to Version 10 Release Notes.

Changes from V 9

1. Logical flow change

The basic building blocks in Cyberoam are Zones, Interfaces and (Network/Address) objects. This structure is used in defining firewall rules to allow or deny the access.

Zone is the logical grouping of Interface, which includes:

- predefined zones - LAN, WAN, DMZ, LOCAL, VPN
- custom zone

Interface includes:

- actual physical Ethernet interfaces or ports i.e. Port A through Port J depending on the appliance model
- subinterfaces - VLAN
- PPPoE interfaces
- interface aliases and
- WWAN interface if Wireless WAN functionality is enabled

Objects are the logical building blocks of the firewall rule, which includes:

- host - IP and MAC addresses
- services which represent specific protocol and port combination e.g. DNS service for TCP protocol on 53 port
- schedule to control when the rule will be in effect e.g. All Days, Work Hours
- certificates
- file types

2. Internet Access control configuration change

Now Internet access can be controlled by filtering web and application separately. This provides granular control over Internet access. This is achieved by splitting Internet Access policy in two policies – Web filter policy and Application filter policy.

The traffic coming from the web is filtered by various policies and categories through Web filter policy while application filter policy controls user's application access. It specifies which user has access to which applications.

3. Behavior change

1. Wizard behavior change: (Wizard is now deployment wizard)

If wizard is re-run, it will flush following configurations:

- dhcp server/relay configurations
- unicast/multicast routing
- vpn, l2tp, pptp
- static/proxy arp
- VH/ Bypass firewall / firewall rules/ gateway
- pppoe

- custom zones
 - local acls
 - interface based hosts/hostgroup
2. Deleting Interface – Alias and Virtual host will also remove all its dependent configurations including:
 - Interface-Zone binding
 - DHCP Server or Relay
 - Alias based Firewall rules
 - ARP - static and proxy
 - Virtual hosts and VH based firewall rules
 - Interface based Hosts and reference from host groups
 - Routes - Unicast, Multicast
 3. Updating Interface details will also update all its dependent configurations including:
 - Interface-Zone binding
 - DNS
 - Stops the DHCP Server and updates the details. You will have to manually restart the server
 - Gateway
 - Interface based Hosts
 - Disconnects all the tunnels and updates all the VPN policies. You will have to manually reconnect the tunnels.
 - VLAN Interfaces
 - Dynamic DNS Client
 4. Except for WAN zone, Zone-Interface membership can be changed from Manage Interface page as well as Edit Zone page. In previous versions, it was possible only from Edit Zone page. While for WAN zone, it can be changed only from Manage Interface page.
 5. Appliance Access can be configured from Zone as well as from Administration page.
 6. Automatic addition of gateway, no need to add gateway manually. Gateway will be added and removed automatically when any Interface in WAN zone is added or removed.
 7. Deleting VLAN interface will delete its firewall rule also.
 8. Default Administrator user “cyberoam” can be deleted as now Cyberoam is shipped with a global Administrator.
 9. Cyberoam must be rebooted after modifying time zone.
 10. Internet Access policy is divided into two policies
 - Web filter policy – Can be configured to filter HTTP traffic only
 - Application filter policy – Can be configured to filter application traffic
 11. System Health Graphs can be accessed from Web Admin Console using System Graph Page.
 12. Any modifications in user login restriction will be applied on next login.
 13. Service group - PPTP_Group automatically added.
 14. L2TP and PPTP access for the user can be configured through User page as well as L2TP and PPTP Configuration page.
 15. Live Connections Page to display live IPSec connections and live SSL VPN users

4. Redesigned UI - Menu and pages regrouping

To reflect the above changes, GUI pages are reorganized and menus are renamed as:

- System
- Objects
- Network
- Identity
- Firewall
- VPN
- IPS
- Web filter
- Application filter

- QoS
- Anti Virus
- Anti Spam
- Logging & Reporting

5. Renamed features

Old name	New name
Local ACL	Appliance Access
Host	IP host
User	Identity
Bandwidth policy	QoS policy
Surfing quota policy – Allotted hours	Maximum hours
HTTP Proxy	Web Proxy
Web Client	Captive Portal
Full Access (SSL VPN Access mode)	Tunnel Access
Road Warrior	Remote Access
Net-to-Net (IPSec policy)	Site-to-Site

6. Functionality moved from CLI to Web Admin Console

1. Packet capture
2. Unicast and Multicast (can be configured from both the Consoles)
3. Interface speed, MSS and MTU (can be configured and updated from both the Consoles)
4. Live Graphs of CPU usage, Memory usage, Load average and Interface statistics for last hours. Graphs will be refreshed automatically at the interval of 30 seconds.
5. View Access Logs
6. View Audit logs
7. Rollback to Previous version – supported through multiple firmwares

Discontinued features of version 9.x

Following features of V 9.6.x.x will not be supported from V X onwards:

1. Add/Delete Gateway button removed from Manage Gateway page as Gateway will be added/deleted automatically.
2. User Type – Manager. Same as the Admin user with Audit Admin Profile i.e. view reports
3. Shared Policy is removed from Surfing Quota and Data Transfer Policy
4. Surfing quota policy – Cycle hours can be configured in hours only, minutes option is removed
5. Manage HTTP Proxy page is removed but functionality is included in Web proxy
6. Regenerate button has been removed from Update Certificate page as Certificate will be regenerated automatically whenever updated.
7. Data Transfer Limit alerts as on Customize Client Messages page
8. SNMP service start/stop option is removed as it will always be ON once Agent is configured.
9. RMS (Restart Management Services) as now it is now not required for any changes in Network configuration including Alias and Virtual Interface creation.
10. Custom Login messages as it is now included on Captive portal page
11. Antivirus Scan policy (default and custom) for SMTP - now part of Scanning Rule
12. Global and Default Antispam policy
13. Antispam Custom policy - now part of Spam Rule
14. User Migration Utility as Export/Import functionality is added on User page
15. Manual purge of reports. Auto purge will get-in in Stability-1.
16. Service creation – “ICPM Type – Other” will not be available.

17. SNMP Version v3 Protocol support
18. User maximum session timeout option is given globally, however, per group is missing.
19. System Modules Configuration on GUI is not available. It is available on CLI only.
20. DHCP server "Enable Auto Start" Button

Features expected in version-10 Stability-1

1. Traffic discovery – Only live connections will be provided.
2. AV version information is missing - To be made available for all models on update page. Current availability is on 15i and 25i only.
3. AV & AS Quarantine Area – total utilization
4. Web Category - Search URL
5. Corporate Client Download – for all the Cyberoam Clients – Will be available in the form of links in Stability-1. Pre-requisite will be that the download site will need to be allowed for all.
6. Dashboard doclets -
System Resource (CPU, Memory, Disk Usage) Post Stability-1,
Usage Summary (HTTP hits, Search Engine Queries) In Stability-1 ,
User Surfing Pattern Post Stability-1 ,
HTTP Traffic Analysis (Distribution by Hits, Distribution by Data Transfer) – Post Stability-1
7. Backup over Mail
8. IPS Signature details link
9. Editable IP address of Clientless user : Editable IP address will be available as part of Stability-1.
10. "Show All" link on Live Users page – In Stability-1, default 50 live users will be shown.
11. L2TP connection report - User information and data transfer details
12. Web Category – "IPAddress" category
13. Tool tip Firewall rule page for:, host, host group and Identity columns – Except for IPS, tool tip for all others will be available in Stability-1.
14. User search (rather filter for v10) is not available for IP.
15. Reports
 - a. Web Surfing Report
 - i. Category type (by hits)Wise – Will be available post Stability-1.
 - ii. Category type data transfer – Will be available post Stability-1.
 - iii. Group wise Site wise/HTTP data Transfer /HTTP hits by content / HTTP File upload – Will be available post Stability-1.
 - iv. User wise Site wise/HTTP data Transfer /HTTP hits by content type / HTTP File upload
 - b. Gateway wise b/w usage and composite b/w usage graphs on GUI – Will be available post Stability-1.
16. Audit Logs
 - a. GUI Audit logs
 - b. SSL VPN logs – Will be available post Stability-1.
 - c. Appliance Audit logs (RESET/Backup/Restore/Upgradeauto-manual/reboot) .– Will be available in Stability-1 and will be part of GUI audit logs.
 - d. Service Restart Logs – Will be available in Stability-1 and will be part of GUI audit logs
 - e. Firmware apply/bootup logs – Will be available in Stability-1 and will be part of GUI audit logs

Features expected Post version-10 Stability-1

1. Dashboard doclets –

- a. User Surfing Pattern,
- b. HTTP Traffic Analysis (Distribution by Hits, Distribution by Data Transfer)
- c. System Resource (CPU, Memory, Disk Usage)
2. ARP Cache
3. Auto purge
4. Application Filter Logs on the Logging Server
5. Upload Corporate image in Web Filter Category custom messages
6. Bandwidth Usage Graphs
7. Proactive Reports – Category wise Trends, Google Search Keywords – Category wise trends availability to be confirmed eventually. Google Search Keywords will be available post Stability-1.
8. Dashboard alerts
9. Antivirus Engine Information update time
10. Antispam center connectivity status
11. Last upgrade status and timestamp for AV/IPS/Webcat
12. Mail Notification on change of gateway status
13. Language support - Turkish, French
14. Multiple domain support for authentication
15. Zone – Description field, Description field will be removed from manage page
16. Firewall rule – Bandwidth usage (upload and download)
17. IPS Policy - "Select All" for selecting all the Categories
18. Persistent Logs (including VPN logs)
19. Clientless users--> Active and Inactive list cannot be displayed separately: – Will be available post Stability-1 in the form of filter support on “Active/Inactive”.
20. Static route in bridge and IPSEC and http proxy host entry is not there.
21. Console Audit logs
22. Reports
 - a. Web Surfing Report
 - i. Category type (by hits)Wise
 - ii. Category type data transfer
 - iii. Group wise Site wise/HTTP data Transfer /HTTP hits by content / HTTP File upload
 - b. Gateway wise b/w usage and composite b/w usage graphs on GUI
 - c. Internet Usage Report
 - i. User/Group wise Internet Usage Reports
 - ii. User/Group wise Surfing Time Report
 - d. Trend
 - i. Hourly based Trend Reports
 - e. Audit log
 - i. Appliance Audit log

Features availability to be confirmed eventually

1. Customizing Client Preferences - HTTP Client option (Page, Pop-up, None) and default URL & customize Login Message
2. System->Configure->Customize Client Preferences, URL to open a site after client logs on to server.
3. Custom Application Category – Destination IP is not available. Otherwise, service group can be used. Availability of destination IP to be confirmed eventually.
4. Client Login Links from Customize Login Messages page
5. Clientless User – IP address based Sorting and Searching
6. User MyAccount access from Users page
7. Restart Servers option – SMTP, POP3, IMAP, FTP, Cyberoam server from Manage
8. Diagnostic tool
9. Servers page
10. Group wise HTTP keep alive enable/disable

11. User maximum session timeout per group
12. Logon script updation download link in case of SSO. It was available in v9 as part of users | Migrate Users menu:
13. Simultaneous user login option available for user only not for group

CLI features

Menu - System Configuration:

- Trace Route Utility
- Set Module Info
- Bandwidth Graph Settings
- Disable LAN Bypass

Menu - Cyberoam Management:

- Database Utilities
- DHCP Client Settings
- download backup
- restore backup
- View audit logs
- check and upgrade cyberoam new version
- cyberoam auto upgrade status
- webcat auto upgrade status
- rollback to previous version
- HA configuration
- ReBuild firewall rule

Menu Route Configuration

- Configure Unicast Routing {Configure Static-routes/ACLs}

Menu Upgrade version

Menu VPN Management

- View VPN logs
- View connection wise VPN logs
- Advance VPN logs
- PPTP VPN logs

Commands (All the parameters except mentioned here are available)

ping: record-route | numeric | tos | ttl

cyberoam: check_disk | cpu_burn_test | dgd | ips_autoupgrade | repair_disk | service | system_monitor | view | services

httpclient

devicemap

dnslookup: server

ip

ips

route: add | delete

set: advanced-configuration: tcp-window-scaling, cr-traffic-nat

set: cache | usermac

set: bandwidth: guarantee | graph

set: http_proxy: av_sessions | client_sessions | core_dump | debug | deny_unkown_proto | multiple_webcategory | delete | relay_http_invalid_traffic | rw_buffer_size | x_forwarded_for

set: usermac

set: secure-scanning (as included in set service-parameter command)

set: sslvpn: max-clients | max-connections | owa-basic-mode

show: access-log | | antispam | antivirus | firewall-rule-log | ftp | login | mail | monitor | reboot

show: system: logs | devices | dma | filesystems | iomem | ioports | partitions | pci | processes | statistics | modules | uptime

show: http_proxy

show: monitor, ftp, login, access-log

show: system

packet-capture

telnet: tos | source