Cyberoam
A SOPHOS Company

Cyberoam High Availability Configuration Guide

Version 10

Document Version 1.0-10.6.1.631-04/06/2014

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

Corporate Headquarters

Cyberoam House,
Saigulshan Complex, Opp. Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad - 380006, GUJARAT, INDIA.
Tel: +91-79-66216666
Fax: +91-79-26407640
Web site: www.cyberoam.com

Contents

Preface

The Appliances use Layer 8 technology to help organizations maintain a state of readiness against today's blended threats and offer real-time protection.

Unified Threat Management Appliances offer identity-based comprehensive security to organizations against blended threats - worms, viruses, malware, data loss, identity theft; threats over applications viz. Instant Messengers; threats over secure protocols viz. HTTPS; and more. They also offer wireless security (WLAN) and 3G wireless broadband. Analog modem support can be used as either Active or Backup WAN connection for business continuity.

The Appliance integrates features like stateful inspection firewall, VPN, Gateway Anti-Virus and Anti-Spyware, Gateway Anti-Spam, Intrusion Prevention System, Content & Application Filtering, Data Leakage Prevention, IM Management and Control, Layer 7 visibility, Web Application Firewall, Bandwidth Management, Multiple Link Management and Comprehensive Reporting over a single platform.

The Appliance has enhanced security by adding an 8th layer (User Identity) to the protocol stack. Advanced inspection provides L8 user-identity and L7 application detail in classifying traffic, enabling Administrators to apply access and bandwidth policies far beyond the controls that traditional UTMs support. It thus offers security to organizations across layer 2 - layer 8, without compromising productivity and connectivity.

The Appliance accelerates unified security by enabling single-point control of all its security features through a Web 2.0-based GUI. An extensible architecture and an 'IPv6 Ready' Gold logo provide Appliance the readiness to deliver on future security requirements.

The Appliances provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

Layer 8 Security:

The Appliance's features are built around its patent pending Layer 8 technology. The Layer 8 technology implements the human layer of networking by allowing organizations control traffic based on users instead of mere IP Addresses. Layer 8 technology keeps organizations a step ahead of conventional security solutions by providing full business flexibility and security in any environment including WI-FI and DHCP.

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
Cyberoam House,
Saigulshan Complex, Opp. Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad - 380006, GUJARAT, INDIA.
Tel: +91-79-66216666
Fax: +91-79-26407640
Web site: www.cyberoam.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-66216565
Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit www.cyberoam.com for the regional and latest contact information.

Introduction

Welcome to Cyberoam's – High Availability Configuration Guide.

This guide describes how the High Availability can be configured among Cyberoam Appliances.

Note

This feature is not available in CR15i, CR15iNG, and all WiFi models.

All the screen shots in the High Availability Configuration User Guides have been taken from NG series of Appliances. The feature and functionalities however remains unchanged across all Cyberoam Appliances

Appliance Administrative Interfaces

Appliance can be accessed and administered through:

1. Web Admin Console
2. Command Line Interface Console
3. Cyberoam Central Console

Administrative Access An administrator can connect and access the Appliance through HTTP, HTTPS, telnet, or SSH services. Depending on the Administrator login account profile used for access, an administrator can access number of Administrative Interfaces and Web Admin Console configuration pages.

Appliance is shipped with two administrator accounts and four administrator profiles.

Administrator Type	Login Credentials	Console Access	Privileges
Super Administrator	admin/admin	Web Admin Console CLI console	Full privileges for both the consoles. It provides read-write permission for all the configuration performed through either of the consoles.
Default	cyberoam/cyber	Web Admin console only	Full privileges. It provides read-write permission for all the configuration pages of Web Admin console.

Note

We recommend that you change the password of both the users immediately on deployment.

Web Admin Console

Web Admin Console is a web-based application that an Administrator can use to configure, monitor, and manage the Appliance.

You can connect to and access Web Admin Console of the Appliance using HTTP or a HTTPS connection from any management computer using web browser:

1. HTTP login: http://<LAN IP Address of the Appliance>
2. HTTPS login: https://<LAN IP Address of the Appliance>

For more details, refer section Web Admin Console.

Command Line Interface (CLI) Console

Appliance CLI console provides a collection of tools to administer, monitor and control certain Appliance component. The Appliance can be accessed remotely using the following connections:

1. Remote login Utility – TELNET login

To access Appliance from command prompt using remote login utility – Telnet, use command TELNET <LAN IP Address of the Appliance>. Use administrator password to login.

Note

Default password of TELNET connection for CLI Console is “admin”.

2. SSH Client (Serial Console)

SSH client securely connects to the Appliance and performs command-line operations. CLI console of the Appliance can be accessed via any of the SSH client using LAN IP Address of the Appliance and providing Administrator credentials for authentication.

Note

Start SSH client and create new Connection with the following parameters:
Host – <LAN IP Address of the Appliance>
Username – admin
Password – admin

Use CLI console for troubleshooting and diagnose network problems in details. For more details, refer version specific Console Guide available on http://docs.cyberoam.com/.

Cyberoam Central Console (CCC)

Distributed Cyberoam Appliances can be centrally managed using a single Cyberoam Central Console (CCC) Appliance, enabling high levels of security for Managed Security Service Provider (MSSPs) and large enterprises. To monitor and manage Cyberoam using CCC Appliance you must:

1. Configure CCC Appliance in Cyberoam
2. Integrate Cyberoam Appliance with CCC using: Auto Discovery, Manually

Once you have added the Appliances and organized them into groups, you can configure single Appliance or groups of Appliances.

For more information, please refer CCC Administrator Guide.

Web Admin Console

CyberoamOS uses a Web 2.0 based easy-to-use graphical interface termed as Web Admin Console to configure and manage the Appliance.

You can access the Appliance for HTTP and HTTPS web browser-based administration from any of the interfaces. Appliance when connected and powered up for the first time, it will have a following default Web Admin Console Access configuration for HTTP and HTTPS services.

Services	Interface/Zones	Default Port
HTTP	LAN, WAN	TCP Port 80
HTTPS	WAN	TCP Port 443

The administrator can update the default ports for HTTP and HTTPS services from **System > Administration > Settings**.

Web Admin Language

The Web Admin Console supports multiple languages, but by default appears in English. To cater to its non-English customers, apart from English, Chinese-Simplified, Chinese-Traditional, Hindi, Japanese and French languages are also supported. Administrator can choose the preferred GUI language at the time of logging on.

Listed elements of Web Admin Console will be displayed in the configured language:

- Dashboard Doclet contents
- Navigation menu
- Screen elements including field & button labels and tips
- Error messages

Supported Browsers

You can connect to the Web Admin Console of the Appliance using HTTP or a secure HTTPS connection from any management computer using one of the following web browsers:

Browser	Supported Version
Microsoft Internet Explorer	Version 8+
Mozilla Firefox	Version 3+
Google Chrome	All versions
Safari	5.1.2(7534.52.7)+
Opera	15.0.1147.141+

The minimum screen resolution for the management computer is 1024 X 768 and 32-bit true xx-color.

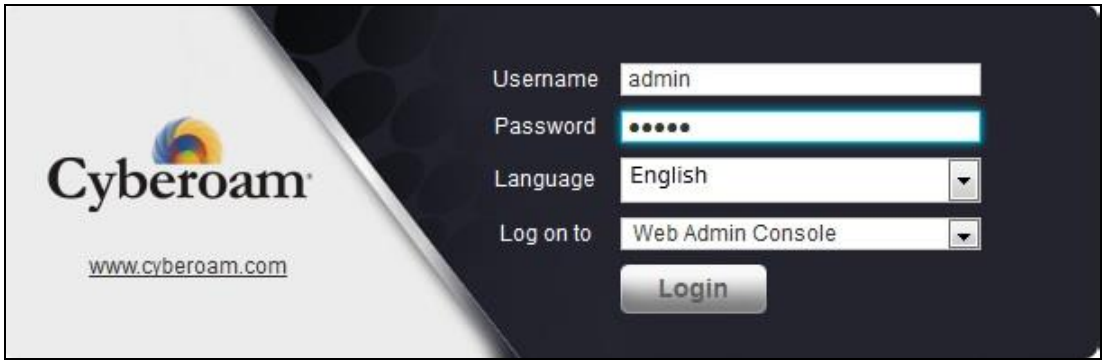
The Administrator can also specify the description for firewall rule, various policies, services and various custom categories in any of the supported languages.

All the configuration done using Web Admin Console takes effect immediately. To assist you in configuring the Appliance, the Appliance includes a detailed context-sensitive online help.

Login procedure

The log on procedure authenticates the user and creates a session with the Appliance until the user logs-off.

To get to the login window, open the browser and type the LAN IP Address of Cyberoam in the browser's URL box. A dialog box appears prompting you to enter username and password.



Screen – Login Screen

Screen Element	Description
Username	Enter user login name. If you are logging on for the first time after installation, use the default username.
Password	Specify user account password. Dots are the placeholders in the password field. If you are logging on for the first time after installation with the default username, use the default password.
Language	Select the language. The available options are Chinese-Simplified, Chinese-Traditional, English, French, and Hindi. Default – English
Log on to	To administer Cyberoam, select 'Web Admin Console' To view logs and reports, select "Reports". To login into your account, select "My Account".
Login button	Click to log on the Web Admin Console.

Screen – Login screen elements

The Dashboard appears as soon as you log on to the Web Admin Console. It provides a quick and fast overview of all the important parameters of your Appliance.

Log out procedure

To avoid un-authorized users from accessing Cyberoam, log off after you have finished working. This will end the session and exit from Cyberoam.

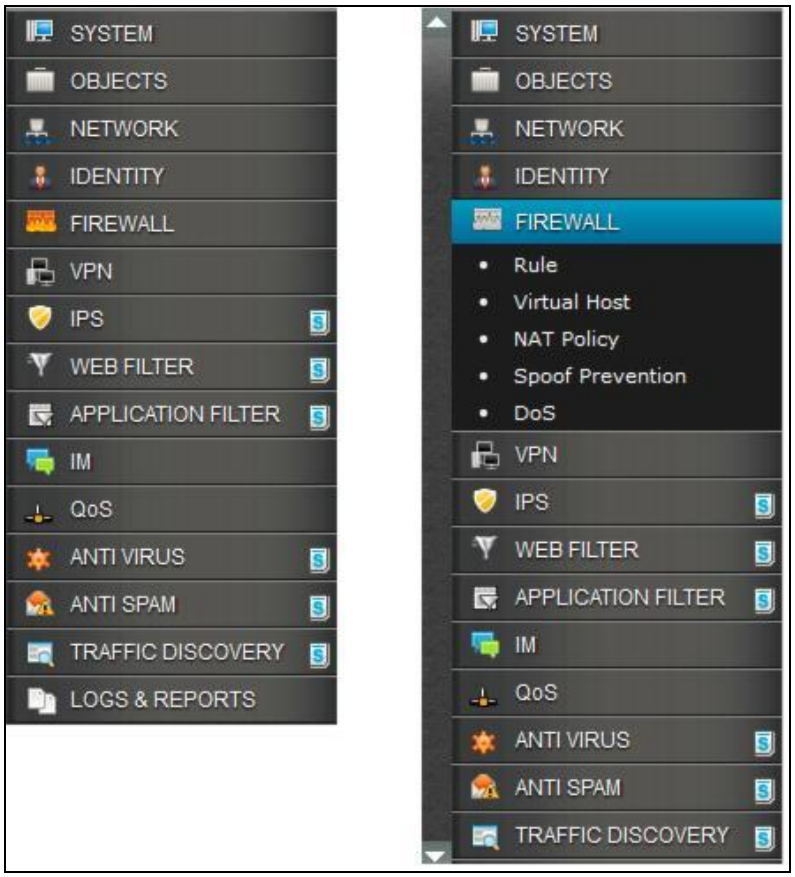
To log off from the Appliance, click the 

button located at the top right of any of the Web Admin Console pages.

Menus and Pages

The Navigation bar on the leftmost side provides access to various configuration pages. This menu consists of sub-menus and tabs. On clicking the menu item in the navigation bar, related management functions are displayed as submenu items in the navigation bar itself. On clicking submenu item, all the associated tabs are displayed as the horizontal menu bar on the top of the page. To view a page associated with the tab, click the required tab.

The left navigation bar expands and contracts dynamically when clicked on without navigating to a submenu. When you click on a top-level heading in the left navigation bar, it automatically expands that heading and contracts the heading for the page you are currently on, but it does not navigate away from the current page. To navigate to a new page, first click on the heading, and then click on the submenu you want navigate to. On hovering the cursor upon the up-scroll icon or the down-scroll icon, automatically scrolls the navigation bar up or down respectively.



The navigation menu includes following modules:

- System – System administration and configuration, firmware maintenance, backup - restore
- Objects – Configuration of various policies for hosts, services, schedules and file type
- Networks – Network specific configuration viz., Interface speed, MTU and MSS settings, Gateway, DDNS
- Identity – Configuration and management of User and user groups
- Firewall – Firewall Rule Management
- VPN – VPN and SSL VPN access configuration
- IPS – IPS policies and signature

- Web Filter – Web filtering categories and policies configuration
- Application Filter – Application filtering categories and policies configuration
- WAF – Web Application Filtering policies configuration. Available in all the models except CR15iNG and CR15wiNG.
- IM – IM controls
- QoS – Policy management viz., surfing quota, QoS, access time, data transfer
- Anti Virus – Antivirus filtering policies configuration
- Anti Spam – Anti Spam filtering policies configuration
- Traffic Discovery – Traffic monitoring
- Logs & Reports – Logs and reports configuration

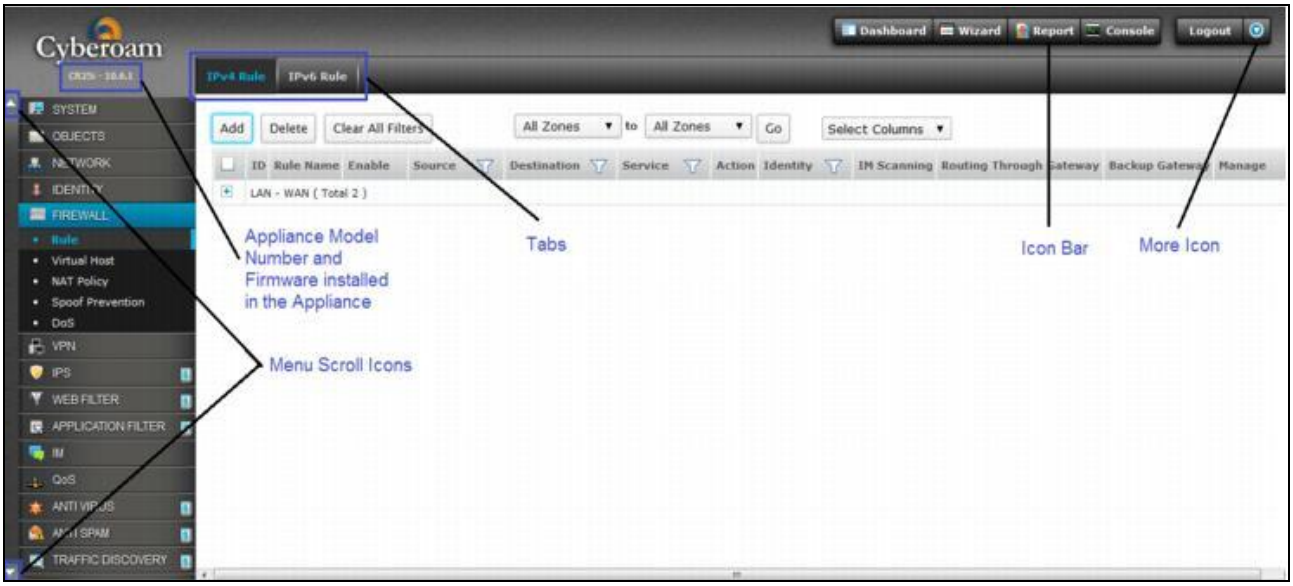
- Note

- Use F1 key for page-specific help.
- Use F10 key to return to Dashboard.

Each section in this guide shows the menu path to the configuration page. For example, to reach the **Zone** page, choose the **Network** menu, then choose **Interface** sub-menu from the navigation bar, and then choose **Zone** tab. Guide mentions this path as **Network > Interface > Zone**.

Page

A typical page looks as shown in the below given image:



Screen – Page

Icon bar

The Icon bar on the upper rightmost corner of every page provides access to several commonly used functions like:

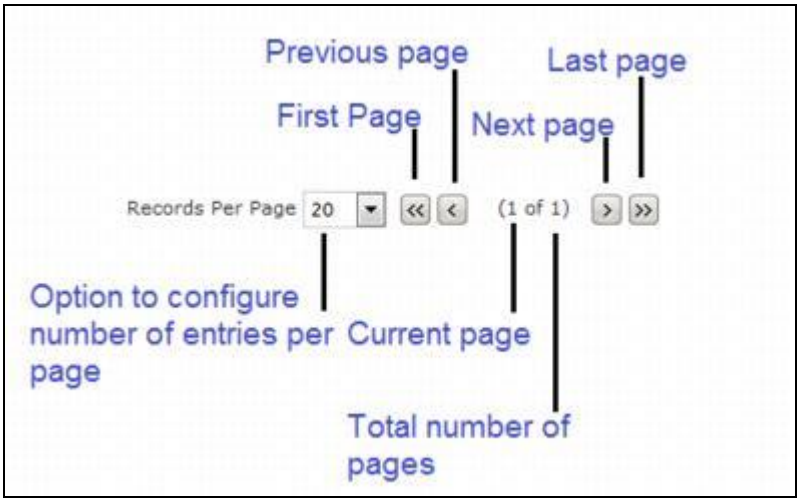
1. **Dashboard –** Click to view the Dashboard
2. **Wizard** – Opens a Network Configuration Wizard for a step-by-step configuration of the network parameters like IP Address, subnet mask and default gateway for your Appliance.
3. **Report** – Opens a Reports page for viewing various usage reports. Integrated Logging and Reporting solution - iView, to offer wide spectrum of 1000+ unique user identity-based reporting across applications and protocols and provide in-depth network visibility to help organizations take corrective and preventive measures.

	This feature is not available for CR15xxxx series of Appliances.

4. **Console** – Provides immediate access to CLI by initiating a telnet connection with CLI without closing Web Admin console.
5. **Logout** – Click to log off from the Web Admin Console.
6. More Options – Provides options for further assistance. The available options are as follows:
   - **Support –** Opens the customer login page for creating a Technical Support Ticket. It is fast, easy and puts your case right into the Technical Support queue.
   - **About Product –** Opens the Appliance registration information page.
   - **Help –** Opens the context – sensitive help page.
   - **Reset Dashboard –** Resets the Dashboard to factory default settings.
   - **Lock –** Locks the Web Admin Console. Web Admin Console is automatically locked if the Appliance is in inactive state for more than 3 minutes. To unlock the Web Admin Console you need to re-login. By default, Lock functionality is disabled. Enable Admin Session Lock from **System > Administration > Settings**.
   - **Reboot Appliance –** Reboots the Appliance.
   - **Shutdown Appliance –** Shut downs the Appliance .

List Navigation Controls

The Web Admin Console pages display information in the form of lists that are spread across the multiple pages. Page Navigation Control Bar on the upper right top corner of the list provides navigation buttons for moving through the list of pages with a large number of entries. It also includes an option to specify the number entries/records displayed per page.

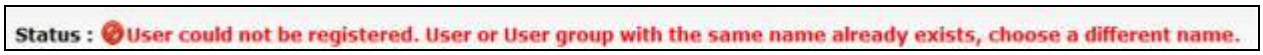


Tool Tips

To view the additional configuration information use tool tip. Tool tip is provided for many configurable fields. Move the pointer over the icon  to view the brief configuration summary.

Status Bar

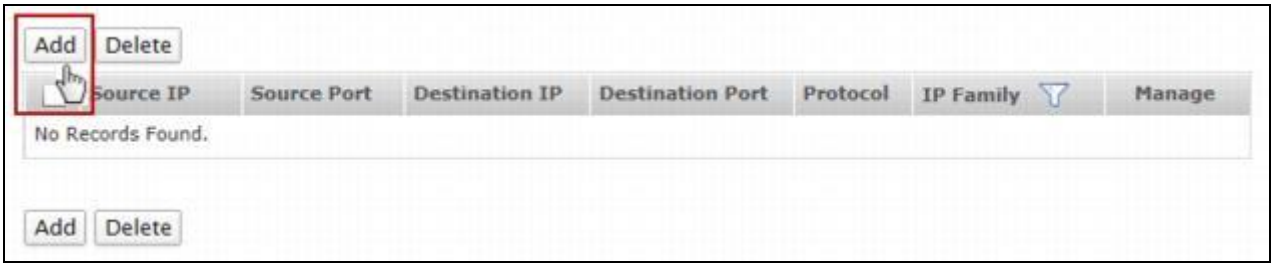
The Status bar at the bottom of the page displays the action status.



Common Operations

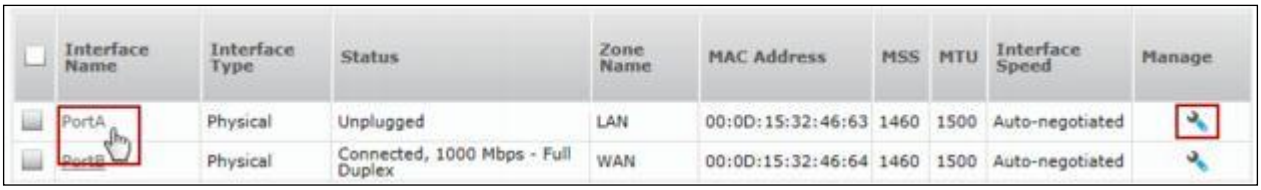
Adding an Entity

You can add a new entity like policy, group, user, rule, ir host by clicking the Add button available on most of the configuration pages. Clicking this button either opens a new page or a pop-up window.



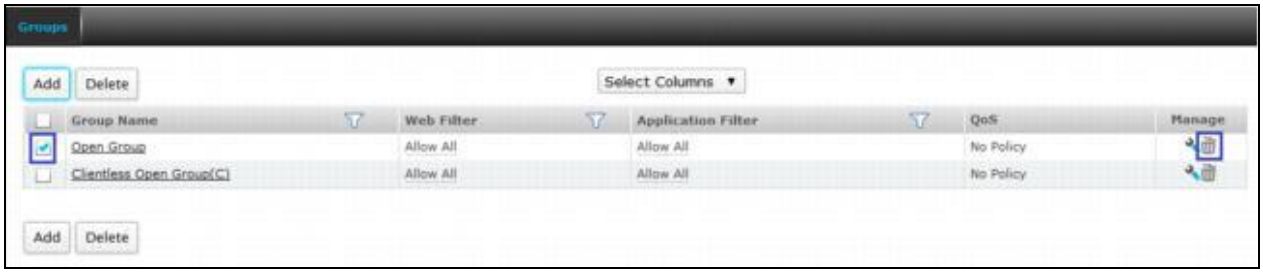
Editing an Entity

All the editable entities are hyperlinked. You can edit any entity by clicking either the hyperlink or the Edit icon under the Manage column.

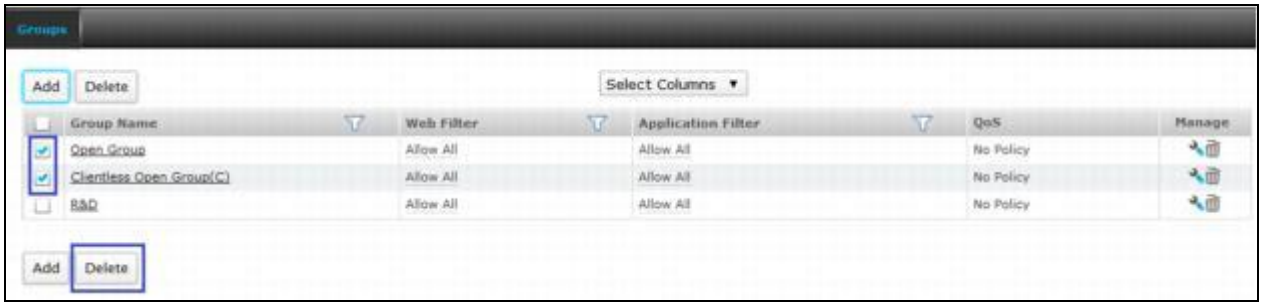


Deleting an Entity

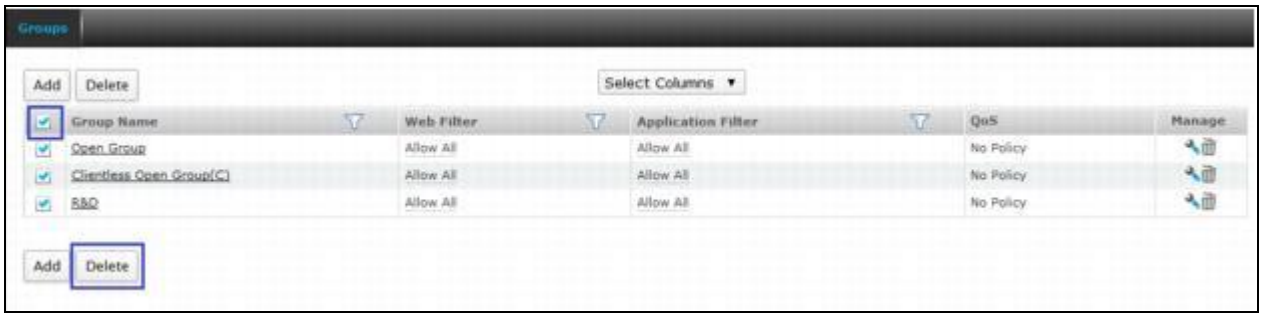
You can delete an entity by selecting the checkbox and clicking the Delete button or Delete icon.



To delete multiple entities, select individual entity and click the Delete button.



To delete all the entities, select in the heading column and click the Delete button.



Sorting Lists

To organize a list spread over multiple pages, sort the list in ascending or descending order of a column attribute. You can sort a list by clicking a column heading.

- Ascending Order icon  in a column heading indicates that the list is sorted in ascending order of the column attribute.
- Descending Order icon  in a column heading indicates that the list is sorted descending order of the column attribute.

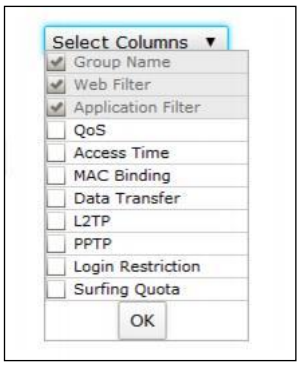
Filtering Lists

To search specific information within the long list spread over multiple pages, filter the lists. Filtering criteria vary depending on a column data and can be a number or an IP address or part of an address, or any text string combination.

To create filter, click the Filter  icon in a column heading. When a filter is applied to a column, the Filter icon changes to  .

Configuring Column Settings

By default on every page all columnar information is displayed but on certain pages where a large number of columnar information is available, all the columns cannot be displayed. It is also possible that some content may not be of use to everyone. Using column settings, you can configure to display only those numbers of columns which are important to you.



To configure column settings, click Select Column Settings and select the checkbox against the columns you want to display and clear the checkbox against the columns which you do not want to display. All the default columns are greyed and not selectable.

High Availability

Hardware failure such as a failure of the power supply, hard disk, or processor is the main reason behind the failure of Internet security system and/or a Firewall. To provide a reliable and continuous connection to the Internet and to provide security services such as Firewall, VPN, Intrusion Detection and Prevention, Virus Scanning, Web Filtering, and Spam Filtering services, two Appliances can be configured to function as a single Appliance and provide High Availability.

Clustering Technology is used to ensure the High Availability. In a cluster, two Appliances are grouped together and instructed to work as a single entity.

HA Terminology

1. HA Cluster

It is a group of two Appliances instructed to work as a single entity. Every HA Cluster has one Primary Appliance and one Auxiliary Appliance. The Primary Appliance controls how the cluster operates. The roles that the Primary and Auxiliary Appliances play in the cluster depends on the configuration mode.

2. HA Configuration Modes

Active-Active

A configuration of HA cluster consists of a Primary Appliance and one Auxiliary Appliance. In this mode, both the Primary Appliance and Auxiliary Appliance process traffic. While the primary unit is in charge of balancing the traffic. Decision of load balancing is taken by the Primary Appliance. Auxiliary Appliance can take over only in case of a primary unit failure.

Active-Passive

A configuration of HA cluster consists of a Primary Appliance and an Auxiliary Appliance. In this mode, only the Primary Appliance processes traffic while Auxiliary Appliance remains in stand-by mode, ready to take over if a Primary Appliance failure occurs.

3. Primary Appliance

The Primary Appliance also tracks the status of all cluster Appliances. In an Active-Active cluster, the Primary Appliance receives the entire network traffic and acts as the load balancer to redirect traffic to Auxiliary Appliance. In an Active-Passive cluster, the Primary Appliance processes the network traffic while the Auxiliary Appliance does not process any traffic but remains ready to take over if Primary Appliance fails.

4. Auxiliary Appliance

The Auxiliary Appliance is always waits to become the Primary Appliance.

In an Active-Active cluster, Auxiliary Appliance processes the network traffic assigned to it by the Primary Appliance. In case the Primary Appliance fails, the Auxiliary Appliance becomes the Primary Appliance. In an Active-Passive cluster, the Auxiliary Appliance does not process network traffic and is in stand-by. It becomes active only when the Primary Appliance is not available to process the traffic.

5. Dedicated HA Link Port

A Dedicated HA link is a direct physical link between the Appliances participating in HA cluster.

6. Load Balancing

An ability of HA cluster to balance the traffic between nodes in the HA cluster.

7. Monitored Interface

A set of interfaces are selected to be monitored. Each Appliance monitors its own interface and if any one of them goes down, the Appliance will remove itself from the cluster and failover occurs.

8. Virtual MAC

It is a MAC Address associated with the HA cluster. This address is sent in response when any of the machines make an ARP request to HA cluster. It is not the actual MAC Address and is not assigned to the interface of any unit in the cluster.

The Primary Appliance owns the MAC Address and is used for routing network traffic. All external clients use this address to communicate with the HA cluster. In case of failover, the new Primary Appliance will have the same MAC Address as the failed Primary Appliance. The cluster Appliance which has a Virtual MAC Address acts as a Primary Appliance.

9. Primary state

In Active-Active mode, the Appliance that is in charge of receiving all the traffic and load balancing is said to be in "Primary" state. An Appliance can be in "Primary" state only when the other Appliance is in "Auxiliary" state.

In Active-Passive mode, the Appliance in charge of processing all the traffic is said to be in the "Primary" state. An Appliance can be in "Primary" state only when the other Appliance is in "Auxiliary" state.

10. Auxiliary state

In Active-Active mode, the Appliance that receives the traffic to be processed by it from the Primary Appliance is termed to be in "Auxiliary" state. An Appliance can be in "Auxiliary" state only when the other Appliance is in "Primary" state.

In Active-Passive mode, the Appliance which is not processing the traffic is called to be in "Auxiliary" state. An Appliance can be in "Auxiliary" state only when the other Appliance is in "Primary" state.

11. Standalone state

An Appliance is called to be in Standalone state when it can still process network traffic and when the other Appliance is not in a position to process network traffic (is either "Fault" state or is Shut Down).

12. Fault state

An Appliance is in fault state when it cannot process network traffic if a device or link fails.

13. Peer

Once the HA cluster is configured, the cluster Appliances are termed as Peers. This means that for the Primary Appliance, the Auxiliary Appliance is its peer Appliance and vice versa.

14. Synchronization

Synchronization is the process of sharing the various cluster configurations, between the Cluster Appliances (HA peers). Reports generated are not synchronized.

15. Device failover

If an Appliance does not receive any communication within the predetermined period of time from the HA peer, the peer Appliance is considered to have failed. This process is termed as Device Failover as when this occurs, the peer Appliance is taken over.

16. Link Failover

Both the Appliances in an HA cluster continuously monitor the dedicated HA link and the interfaces configured to be monitored. If any of them fails, it is called link failure.

17. Session failover

Whether a device or link failover is observed, session failover occurs for forwarded TCP traffic except for the virus scanned sessions that are in progress, VPN sessions, UDP, ICMP, multicast, and broadcast sessions and Proxy traffic.

The Appliance normally maintains session information for TCP traffic which is not passing through the proxy service. Hence, in case of failover, the Appliance which takes over will take care of all the sessions (TCP session not passing through the proxy application). The entire process is transparent for the end users.

How the Cluster works

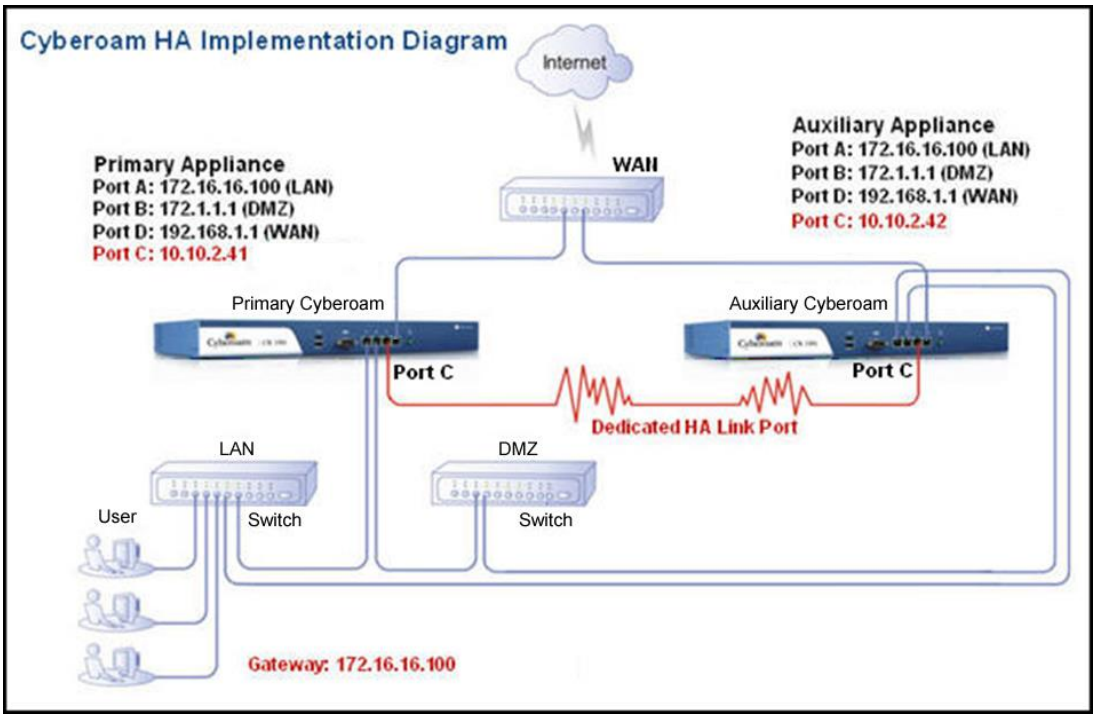
The Appliance offers High Availability by using a Virtual MAC Address shared between a Primary Appliance and an Auxiliary linked together as a “cluster”.

The Appliances - Primary and Auxiliary Appliance, are physically connected over a dedicated HA link port.

Typically, traffic enters your network by passing through a network switch. In an HA solution, one of the Appliances in the cluster has a Virtual MAC Address and traffic is forwarded to that cluster Appliance which has the virtual MAC Address. The Appliance which has virtual MAC Address is the Primary Appliance and other peer is the Auxiliary Appliance. The Primary Appliance acts as a load balancer and forwards the traffic to the Auxiliary Appliance for processing. The Auxiliary Appliance can process traffic only if the cluster is operating in the Active-Active mode.

If configured in the Active-Passive mode, the Primary Appliance processes the entire traffic and Auxiliary Appliance waits in a ready mode to operate as the Primary Appliance, in case Primary Appliance or any of the monitored links fail.

The Auxiliary Appliance monitors the Primary Appliance through the dedicated HA link and if it does not receive any communication within the pre-configured time, the Primary Appliance is considered to have failed. In this case, the Auxiliary Appliance takes ownership of the virtual MAC Address from the Primary Appliance, and temporarily becomes the Primary Appliance. The actual Primary Appliance automatically takes over from the Auxiliary Appliance once it starts functioning.



Screen – Cyberoam HA Implementation

Configure HA

Use to

- Configure Primary Appliance for HA
- Disable HA
- Switch Appliance to standby mode
- Synchronize HA peers

Points to be noted

Behavior

- **DHCP, PPPoE, WWAN, WLAN** – High Availability (HA) cluster cannot be configured if any one of the Interfaces is dynamically configured using DHCP and PPPoE protocols or WWAN or WLAN is configured.

- Session Failover is not possible for AV Scanned sessions or any other forwarded traffic like ICMP, UDP, multicast and broadcast traffic, traffic passing through Proxy Subsystem - transparent, direct and parent proxy traffic, and VPN traffic.

- **Masqueraded Connections** – In case of the manual synchronization event from any of the HA cluster Appliances, all the masqueraded connections will be dropped.

- **HA Load balancing** – An Active-Active HA cluster do not load balance the VPN sessions, UDP, ICMP, multicast and broadcast sessions and scanned FTP traffic. TCP traffic for Web Admin Console or Telnet Console, H323 traffic sessions are also not load balanced between the cluster Appliances.

- **HA Load balancing** – An Active-Active HA cluster will load balance the Normal Forwarded TCP Traffic, NATed (both SNAT & Virtual Host) Forwarded TCP Traffic, and TCP Traffic passing through Proxy Subsystem - Transparent Proxy, Direct Proxy and Parent Proxy and VLAN Traffic.

- HA can be disabled from either of the Appliance. If disabled from the Primary Appliance, HA will be disabled on both the Appliance. If disabled from the Auxiliary Appliance, HA will not be disabled on the Primary Appliance and Appliance will act as a stand-alone Appliance.

- After disabling HA, the Primary Appliance IP schema will not change.

- After disabling HA for Auxiliary Appliance, all the ports except the dedicated HA link port and Peer Administration port will be disabled. The Peer HA Link IP will be assigned IP address assigned to the Dedicated HA Link Port while Peer Aministration IP will be assigned IP Address assigned to the Peer Administration Port.

- If HA is disabled from stand-alone machine, the IP schema will not change.

- Super Administrator privileges are required to access the Auxiliary Appliance Web Admin Console and therefore it can be accessed by “admin” user only. Live users/DHCP leases/IPSec live connections pages will not be displayed.

- After disabling HA, in case of the Auxiliary Appliance, all the administrative services – HTTP, HTTPS, Telnet, SSH are allowed for LAN zone while for DMZ zone only HTTPS and SSH are allowed.

- For the Auxiliary Appliance, Deployment Wizard will not be accessible.

- Dedicated HA link port should be from any of the DMZ interface only. Make sure that the IP Address of the HA link port of Primary and Auxiliary Appliances are in same subnet.

- After enabling HA, if backup without HA configuration is restored then HA will be disabled and Primary Appliance will be accessible as per the backup configuration while the Auxiliary Appliance will be accessible with the Auxiliary Admin IP Address.

- In Active-Active mode, mails will be quarantined separately on both the appliances as SMTP Proxy traffic is load balanced in round robin manner.

- In Active-Passive mode, mails will be quarantined on Primary Appliance only.

- If Quarantine Digest is configured, both the appliances in the cluster will receive Quarantine Digest.

- Administrator can release quarantined mails of all the users from both the appliances.

- User can release quarantined mails from My Account. My Account displays mails quarantined only on Primary Appliance. Also, user can release them from the Quarantine Digest mailed from the Primary Appliance.

Note

HA will get disabled if you run Deployment Wizard.

Before configuring HA

Before attempting to configure two Appliances as an HA pair to prevent single point of hardware failure, check the following requirements:

- Both the Appliances in the HA cluster, the Primary Appliance and the Auxiliary Appliance must be registered and must have same number of interfaces. Both the member Appliances should be of the same model.

Note
If XP Appliances are used in HA cluster, both the Appliances must be of same model number and must be registered

- Both Appliances in the HA cluster must have the same firmware version installed on them.

- Two separate licenses are required, one for the Primary Appliance and the other for the Auxiliary Appliance.

- On both the Appliances, same subscription modules should be enabled, else these modules will not be supported in the event of a failure of the Primary Appliance. For example, if an IPS module is enabled on the Primary Appliance and not enabled on Auxiliary Appliance then on failover when the Auxiliary Appliance becomes Active, IPS policies will not be applicable.

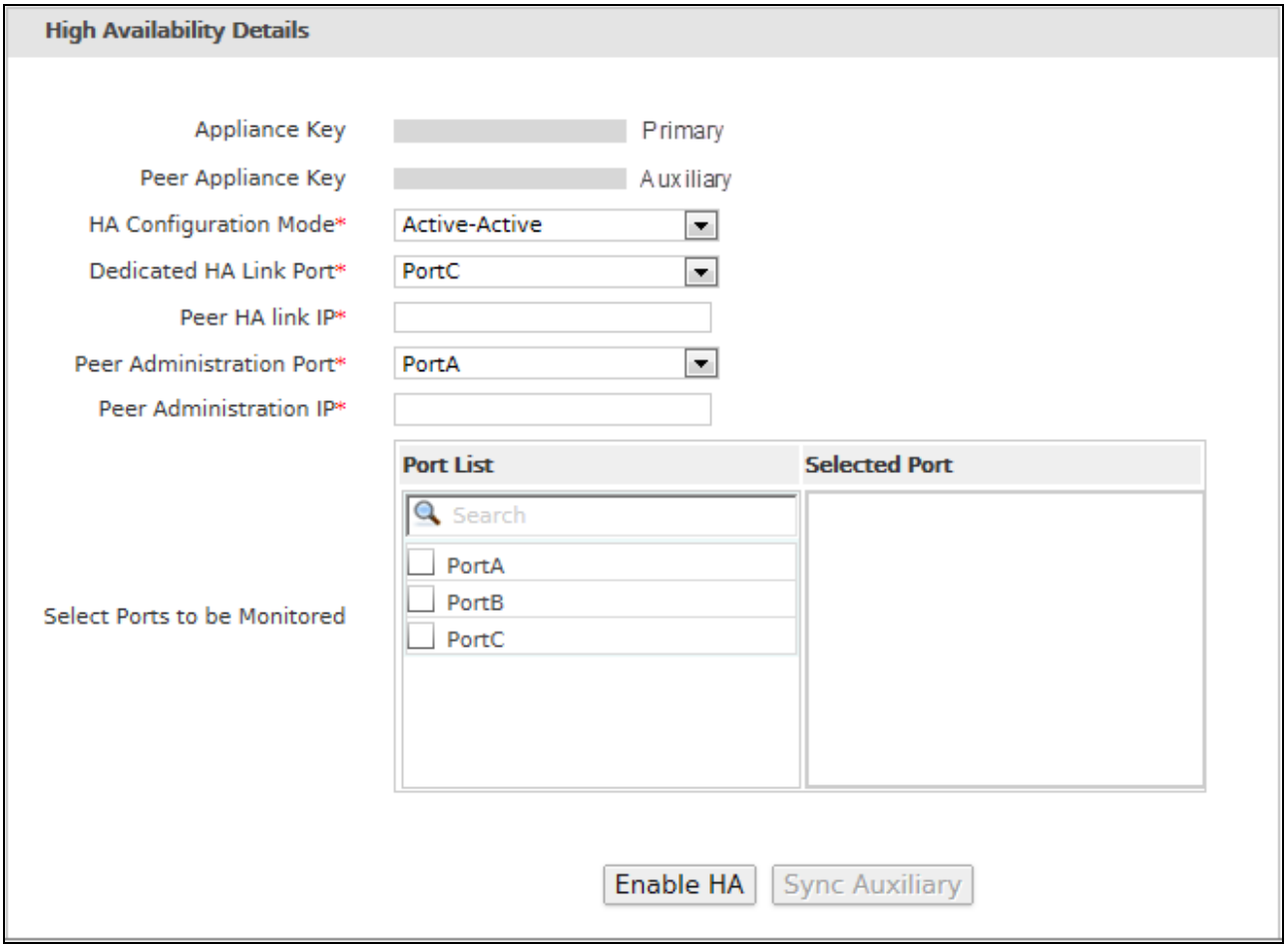
- Cables to all the monitored ports on the Appliance to be configured as Primary must be properly connected. Connect the dedicated HA link port of both the Appliances with a crossover cable.

- The dedicated HA link port must be from the DMZ interface only and must have an unique IP Address on both the Appliance. SSH should be enabled for both the Appliances on DMZ.

- The Interfaces on which DHCP or PPPoE is enabled, WWAN or WLAN interfaces must be disabled before HA configuration.

Configuring the Primary Appliance

- No changes in the firewall configuration. Only need to enable SSH on the dedicated DMZ interface.
- Allow SSH traffic for the dedicated HA link port on both the ApplianceAppliances through the Firewall Rule or by Appliance Access.
- Select **System > HA > HA**



Screen – Configuration Screen (Primary Appliance)

Screen Elements	Description
High Availability Details	
Appliance Key	Displays the Appliance key only after HA is configured.
Peer Appliance Key	Displays the peer's Appliance Key. In case of the Primary Appliance, it displays the Auxiliary Appliance Key and vice versa.
HA Configuration Mode	Select HA Configuration mode for cluster. **Active-Active** – Select to configure a cluster for load balancing and failover HA. In the Active-Active mode both, the the Primary Appliance and the Auxiliary Appliance process the traffic and monitor the status of the other cluster Appliance. The Primary Appliance controls load balancing among both the cluster Appliances. **Active-Passive –** Select to configure a cluster for failover HA. In Active-Passive mode, the Primary Appliance processes all connections. Auxiliary Appliance passively monitors the cluster status and remains synchronized with the Primary Appliance.
Dedicated HA Link Port	Specify the dedicated HA link port. Dedicated HA link port must be from any of the DMZ interface only. HA peers are physically connected using a crossover cable through this port. The same port must be used as an HA link port on peer Appliance also. For example, if port E is configured as the HA link port on the Primary Appliance then use only port E as HA link port on Auxiliary ApplianceAppliance. Make sure that the IP Address of HA link port for both, the Primary Appliance and Auxiliary Appliances are in same subnet. Cluster Appliances use this link to communicate cluster information and to synchronize with each other.
Peer HA link IP	Specify the IP Address configured on the HA link port of the peer Appliance.
Peer Administration Port	Specify the Administration Port for the Auxiliary Appliance. This port can be used for administration purpose.
Peer Administration IP	Specify the Administration IP Address for Auxiliary Appliance. With this IP Address, the Admin Console of the Auxiliary Appliance can be accessed. Any user accessing the Web Admin Console of Auxiliary Appliance will be logged-in with HA Profile and have read-only rights.
Select Ports to be Monitored	Select the ports to be monitored. Both the Appliances will monitor their own ports and if any of the monitored port goes down, the Appliance will leave the

	cluster and failover will occur.
Enable/Disable HA	Click to enable/disable HA.
Sync Auxiliary	Click to synchronize the Auxiliary Appliance with the Primary Appliance.

Table – Configuration screen elements

Note

The Appliance from which HA is enabled, acts as a Primary Appliance while the peer Appliance acts as Auxiliary Appliance.

If everything is cabled and configured properly and HA is enabled successfully:

- Both the Appliances will have the same configuration except the HA link port IP Address.
- Additional options made available after HA is enabled:
  Primary Appliance – Put on Standby (for Active-Passive mode), Disable HA, Sync Auxiliary (use to synchronize Auxiliary Appliance and Primary Appliance configurations)

  Auxiliary Appliance – Disable HA, Sync with Primary (use to synchronize the Auxiliary Appliance and Primary Appliance configurations)
- By default, as soon as HA is enabled successfully, both the Appliances will synchronize automatically.
- As soon as the Active-Active mode is configured, traffic load balancing is enabled. If required, it can be disabled from CLI console using **"cyberoam ha load-balancing on/off"** command.

Disable HA

HA can be disabled from HA configuration page (**System > HA > HA**) from the Primary Appliance.

- HA can be disabled from either of the Appliances. If disabled from the Primary Appliance, HA will be disabled on both the Appliances. If disabled from Auxiliary Appliance, HA will not be disabled on Primary Appliance and will act as stand-alone Appliance.
- After disabling HA, the Primary Appliance IP schema will not change.
- After disabling HA, the Auxiliary Appliance will reboot, all the ports except the dedicated HA link port and Peer Administration port will be disabled. The dedicated HA link port will be assigned Peer HA link IP Address and Peer Administration port will be assigned Peer Administration IP Address.
- If HA is disabled from stand-alone machine, the IP schema will not change.

Switch Appliance to standby mode

Standby mode for the Appliance can be configured only if the cluster is operating in Active-Passive

mode. Auxiliary Appliance takes over as Primary Appliance.

Synchronize HA peers

In normal conditions, the Auxiliary Appliance is always synchronized with the Primary Appliance. However, if need arises, the Auxiliary Appliance can also be manually synchronized with the Primary Appliance by clicking Sync Auxiliary.

Manual synchronization gets data and configuration updates except reports from the Primary Appliance.

Manual Synchronization will reboot the Auxiliary Appliance.

Manual synchronization process can be initiated from either of the peers from **System > HA > HA** page.

If synchronized from the Primary Appliance, Primary Appliance will push updates and if synchronized from the Auxiliary Appliance, Auxiliary Appliance will pull the updates from Primary Appliance.

From/To	Standalone	Primary	Auxiliary**	Fault
Standalone	No	Yes	Yes*	No
Primary	Yes	No	No	Yes
Auxiliary**	Yes	No	No	Yes
Fault	No	No	Yes	No

Table – State Transition Matrix

Note:
* Possible when a dedicated link goes down and comes up again.
** When the Appliance transits into Backup mode, it will soft boot.